CYBER DEFENSE MAGAZINE

eMAGAZINE

OCTOBER 2024

In This Edition

Navigating Advanced Threat Landscapes

The GenAI Scam Revolution

Bridging The Manufacturing Security "Air Gap"

...and much more...

MORE INSIDE!

`

CONTENTS

@MILIEFSKY

From the

Publisher…

As we publish the October issue of Cyber Defense Magazine, I'm pleased to note that we continue to receive positive responses to new and valuable initiatives we offer for the benefit of our readers and followers.

For example, you can find many new "Spotlight" articles on the magazine's home page, under the "Spotlight" nav bar: https://www.cyberdefensemagazine.com/spotlight/ Note they are identified as "Publisher's Spotlight" and "Innovator's Spotlight," depending on which of our professionals submitted the article.

We are approaching the last weeks of registration for the upcoming Cyber Defense Conference. Please see detailed information at the Conference and Awards website:

https://cyberdefenseconferences.com/top-infosec-innovator-awards-2024-apply-today/

The virtual red carpet is already set up, with the incredible high traffic website and social media marketing, and much more to help bolster the good news around our winners during our 2nd half of 2024, 12th anniversary and 12th annual awards during CyberDefenseCon 2024.

We continue on our principal mission - to share cutting-edge knowledge, real-world stories and awards on the best ideas, products, and services in the information security industry to help you on this journey.

Warmest regards,

Gary S. Miliefsky

Gary S. Miliefsky, fmDHS, CISSP®
CEO/Publisher/Radio/TV Host

P.S. When you share a story or an article or information about CDM, please use #CDM and @CyberDefenseMag and @Miliefsky – it helps spread the word about our free resources even more quickly

@CYBERDEFENSEMA

CYBER DEFENSE eMAGAZINE

Published monthly by the team at Cyber Defense Media Group and distributed electronically via opt-in Email, HTML, PDF and Online Flipbook formats.

EDITOR-IN-CHIEF
Yan Ross, JD
yan.ross@cyberdefensemagazine.com

ADVERTISING
Marketing Team
marketing@cyberdefensemagazine.com

CONTACT US:
Cyber Defense Magazine
Toll Free: 1-833-844-9468
International: +1-603-280-4451

https://www.cyberdefensemagazine.com

PUBLISHER
Gary S. Miliefsky, CISSP®

Learn more about our founder & publisher at:
https://www.cyberdefensemagazine.com/about-our-founder/

12 YEARS OF EXCELLENCE!

Providing free information, best practices, tips, and techniques on cybersecurity since 2012, Cyber Defense Magazine is your go-to-source for Information Security. We're a proud division of Cyber Defense Media Group:

CYBERDEFENSEMEDIAGROUP.COM

MAGAZINE TV RADIO AWARDS

PROFESSIONALS WIRE WEBINARS

CYBERDEFENSECONFERENCES

Welcome to CDM's October 2024 Issue

From the Editor-in-Chief

In my capacity as Editor-in-Chief of Cyber Defense Magazine, and on behalf of our entire team, we would like to take this opportunity to extend our appreciation to our many dozens of authors, and the many PR professionals who represent them.

The October 2024 issue of Cyber Defense Magazine includes over 50 articles of vital importance to our readers. We are pleased to provide quality as well as quantity as we continue to broaden our base of authors and readers.

We believe that the scope of our articles reflects the increasing number and breadth of cyber attacks (both successfully and unsuccessfully defended) against important sectors of our critical infrastructure. We cannot emphasize too much that the protection of critical infrastructure is not at all new. The most surprising aspect is that the 16 sectors have been recognized and discussed for over 25 years – but the official responses to the obvious vulnerabilities are still reactive, not pro-active.

We are also pleased to note that our authors write predictively as well as in response to cyber threats already experienced. We might call it "Zero Day Prevention" as a term of art. Not only do our authors serve the needs of CISOs and other cyber security professionals, but also provide valuable information to a growing cadre of vendors and suppliers and clientele of the entire range of cyber rick management providers.

As always, we strive to be the best and most actionable set of resources for the CISO community in publishing Cyber Defense Magazine and broadening the activities of Cyber Defense Media Group.

Wishing you all success in your cybersecurity endeavors,

Yan Ross
Editor-in-Chief
Cyber Defense Magazine

About the US Editor-in-Chief

Yan Ross, J.D., is a Cybersecurity Journalist & U.S. Editor-in-Chief of Cyber Defense Magazine. He is an accredited author and educator and has provided editorial services for award-winning best-selling books on a variety of topics. He also serves as ICFE's Director of Special Projects, and the author of the Certified Identity Theft Risk Management Specialist ® XV CITRMS® course. As an accredited educator for over 20 years, Yan addresses risk management in the areas of identity theft, privacy, and cyber security for consumers and organizations holding sensitive personal information. You can reach him by e-mail at yan.ross@cyberdefensemagazine.com


SPONSORS

NIGHTDRAGON

***"NightDragon** Security is not looking to invest in 'yet another endpoint' solution or falling for the hype of 'yet another a.i. solution', it's creating a unique platform for tomorrow's solutions to come to market faster, to breathe new life into a stale cyber defense economy"*

-David DeWalt

Managing Director and Founder NightDragon Security

ADVISE

WE DELIVER SOUND ADVICE AS YOUR FINANCIAL PARTNERS

INVEST

WE ARE FLEXIBLE INVESTORS ACROSS ALL STAGES OF GROWTH TO PRE-IPO

ACCELERATE

WE HELP OUR COMPANIES ACCELERATE THEIR GROWTH THROUGH STRATEGY TUNING AND RELATIONSHIP BUILDING

www.nightdragon.com

UNKNOWN CYBER

"70% of Malware Infections Go Undetected by Antivirus..."

Not by us. We detect the unknowns.

www.unknowncyber.com


2001
2024
ALLEGIS CYBER CAPITAL
The first dedicated cybersecurity venture firm in the world.
AN INTEGRATED GLOBAL, STAGE-AGNOSTIC CYBERSECURITY INVESTMENT PLATFORM SPANNING SEED THROUGH GROWTH.
For 20 years, AllegisCyber Capital has offered a proven investment platform that actively engages with the most promising entrepreneurs in cyber and delivers the market access, team building, and operating experience essential to their success.
BUILDING AND FUNDING THE MOST INNOVATIVE COMPANIES IN CYBER
Signifyd
SAFEGUARD CYBER
ELISITY
panaseer
Synack
SkyHive
cyber GRX
DRAGOS
CONCEAL
vArmour
ALLEGISCYBER CAPITAL
www.allegiscyber.com

Partner to Close Gaps.

NSA's no-cost **vulnerability assessment** quickly finds issues before they become compromises.

GET STARTED TODAY WITH THIS AND OTHER SERVICES

nsa.gov/ccc

NATIONAL SECURITY AGENCY · UNITED STATES OF AMERICA

CYBERSECURITY COLLABORATION CENTER

Spin.ai

SaaS Security Platform for Mission-Critical SaaS Apps

Enhance Cyber Resilience, Security Operations, and Cost Efficiency

Schedule a Demo Today

www.spin.ai/demo


ARTICLES

Navigating Advanced Threat Landscapes

Approaches for CISOs in Complex Defense Environments

By Daniel Baiz Cabal, CEO, OneAxiom (previously ELK Analytics)

In today's era, marked by rapid digital transformations and an increase in sophisticated cyber threats, the role of Chief Information Security Officers is more crucial than ever. CISOs face the daunting task of navigating through complex cyber threats, developing advanced defensive strategies, and leveraging critical data and trends to craft a dynamic cybersecurity framework. Essential to this role is the formation of a highly knowledgeable team—both internal staff and outsourced experts—equipped with the necessary tools to proactively anticipate, respond to, and effectively neutralize sophisticated cyber threats. This approach ensures that CISOs not only defend but also strengthen their organizations' security posture in this volatile cyber landscape.

Understanding the Advanced Cyber Threat Landscape

Today's cyber threat landscape is marked not only by an increase in the number of threats but also by their growing sophistication. AI-driven attacks have seen a significant uptick, now being incorporated into roughly one-quarter of new software and applications, leading to an increase in AI-exploited vulnerabilities. The financial toll is equally concerning, with the 2024 IBM Cost of a Data Breach Report

revealing that the average cost of a data breach has surged to a record $4.88 million, covering both immediate expenses and extensive long-term reputational damage. This escalation in cybercrime costs, projected to reach a staggering $23.84 trillion by 2027 from $8.44 trillion in 2022 according to the World Economic Forum, underscores the enormous financial and operational stakes at play, highlighting the urgent need for robust cybersecurity measures to mitigate these advanced threats.

Emerging Cybersecurity Trends

The cybersecurity landscape is witnessing rapid evolutions, fueled by advancements in technology and shifts in attacker tactics:

1. **Quantum Computing's Dual-Edged Sword**: While quantum computing promises to revolutionize data processing and encryption, it also poses significant threats to existing cryptographic standards, necessitating the development of quantum-resistant encryption methods.
2. **Sophistication in Phishing Attacks**: Phishing attacks are becoming more intricate, with attackers now utilizing advanced techniques that bypass traditional security measures. This underscores the need for robust multi-factor authentication and sophisticated detection systems.
3. **Rise in Identity-Based Threats**: With a surge in identity theft and credential abuse, cybercriminals are increasingly exploiting personal data to facilitate breaches. The use of generative AI by adversaries to enhance social engineering tactics is particularly concerning.

Investment in an Enhanced Security Posture

The rising costs associated with cyber threats have necessitated increased investment in cybersecurity. According to Gartner, the global security market is expected to grow substantially, reaching an estimated $215 billion by 2024, reflecting the critical need and significant capital being directed towards mitigating cyber risks. Investing in comprehensive cybersecurity infrastructure not only protects against financial losses but also preserves brand integrity and customer trust.

Proactive Cybersecurity Measures

A reactive stance in cybersecurity is obsolete. CISOs must adopt a proactive approach, characterized by ongoing risk assessments, real-time threat monitoring, and predictive analytics. This forward-thinking posture enables security teams to stay one step ahead of potential threats. Some strategies include:

1. **AI-Enhanced Cybersecurity Frameworks**: Leverage AI to bolster threat detection and response. AI's ability to process vast datasets quickly can identify threats before they manifest, providing a critical edge in threat management.
2. **Zero Trust Architecture**: Implement Zero Trust principles throughout the organizational network. This approach ensures rigorous verification and minimal access rights, significantly enhancing security posture.

3. **Comprehensive Endpoint Protection with EDR**: Implementing an EDR solution is crucial for maintaining the security of network endpoints. They offer continuous monitoring and real-time response capabilities that are vital for addressing the threats that originate at endpoints, which account for approximately 70% of all successful cyber attacks.
4. **Vulnerability Scanning and Patching:** Regularly scheduled updates and patching are essential for defending against prevalent cyber threats. This routine maintenance is critical to identifying and closing security gaps or loopholes, thereby strengthening your systems against potential intrusions.
5. **Advanced SIEM Integration:** SIEM technology offers deeper insights into security events and potential breaches through comprehensive data analysis and real-time monitoring. This integration allows businesses to detect subtle anomalies that might indicate complex cyber threats, facilitating more informed and timely decision-making in cybersecurity operations.
6. **Penetration Testing and Red Teaming**: Regularly conduct penetration testing and red team exercises to simulate cyber attacks and test your organization's defenses. This proactive approach helps identify vulnerabilities before they can be exploited.
7. **Robust DDoS Mitigation Techniques**: Deploy advanced DDoS protection strategies as these attacks increase in frequency and intensity. Effective DDoS mitigation tools and practices can help maintain service availability even under attack.
8. **Education and Training**: Regularly update training programs to include the latest cybersecurity practices and threat awareness. This helps in building a resilient organizational culture prepared to handle emerging cyber challenges.
9. **Post-Quantum Cryptography**: Prepare for the quantum computing era by integrating quantum-resistant encryption methods into your security infrastructure to protect against future cryptographic challenges.

Building a Robust Cybersecurity Team

The human element is essential in crafting an effective cybersecurity defense strategy. While advanced tools are crucial, they must be managed by skilled professionals who can optimize their effectiveness. Given the scarcity and high cost of such talent, CISOs should focus on assembling a balanced team of both in-house and outsourced security experts who can seamlessly integrate into their operations and become an extension of their team. These professionals are not just proficient in utilizing sophisticated cybersecurity technologies but are also continuously trained on the latest threats and mitigation techniques. It is vital for these specialists to have a deep understanding of the specific business needs and infrastructure to tailor security measures effectively and ensure the best ROI.

Final Notes: In the face of rapidly evolving cyber threats, CISOs must elevate their cybersecurity strategies from merely defensive to strategically anticipatory. The integration of cutting-edge technologies, skilled personnel, and a proactive security posture will be pivotal in protecting against the next generation of cyber threats.

Some of the trends and data presented here underscore the critical nature of cybersecurity investments and the strategic enhancements needed to safeguard an organization's digital assets. As cybersecurity threats grow both in sophistication and impact, the role of the CISO becomes ever more challenging—but also more crucial to the organization's resilience and success.

By implementing advanced strategies and staying informed, CISOs can ensure their organizations are well-prepared to face the cyber challenges of tomorrow, safeguarding their operational integrity and maintaining trust with stakeholders.

About the Author

Daniel Baiz is an Engineer from Purdue University and holds a Master's Degree from Harvard Business School (2019-2021). Daniel is the CEO of OneAxiom, a leading company in cybersecurity solutions and advanced defense systems. OneAxiom offers a variety of managed cybersecurity solutions designed to meet the specific needs of various industries and clients around the world. OneAxiom has been recognized with several awards, including being part of the Inc 5000 list of the fastest-growing companies in the U.S., Best MSSP by the Global Infosec Award and Cybersecurity Excellence Awards, and ranked among the top 250 managed security service providers in the world. Daniel can be reached by email at daniel@oneaxiom.com, LinkedIn (https://www.linkedin.com/in/daniel-baiz/) and at OneAxiom's website https://www.oneaxiom.com/.

The GenAI Scam Revolution

Producing Hyper-Targeted Scams at Scale

By Julio Casal, CIO and Founder, Constella Intelligence

Introduction

The intersection of cutting-edge artificial intelligence technologies and the extensive exposure of personal data has opened a Pandora's box of potential misuse, including hyper-targeted scams. Large language models (LLMs), with their ability to generate hyper-targeted context-aware, personalized content, are at the forefront of this concern, especially when armed with detailed personal information harvested from the dark web.

Capabilities of Large GenAI Language Models

LLMs, powered by extensive datasets and sophisticated algorithms, excel in generating human-like text that is relevant and engaging at a very low cost. Their ability to parse and utilize vast amounts of information enables them to produce content that is not only convincing but also highly customized to infinite topics. These models can adapt their responses based on the context provided to them, making their applications versatile—from writing novels to simulating conversations.

Exploitation of Exposed Personal Information

With hundreds of billions of personal identities available on the dark web, often as a result of data breaches, scammers have a vast repository of detailed personal data at their disposal. This information can include everything from names and addresses to more sensitive financial and health information. When combined with the generative capabilities of LLMs, scammers can create scams that are specifically designed to manipulate individual targets. These scams are not only personalized but also crafted to resonate with the victim's personal circumstances, leveraging known facts and real situations to bypass skepticism.

Enhanced Scam Techniques

Utilizing LLMs, scammers can dynamically generate content that reacts to a victim's responses, maintaining a believable and interactive dialogue. For example, if a scammer knows from a data breach that a person has recently applied for a loan, the LLM can craft and adapt a scam narrative from the specific loan bank around supposed loan offers or issues, using industry-specific language and pressure tactics that are known to elicit responses.

GenAI models are adept at engaging in natural language conversations with an advanced understanding of context and nuance. They can maintain coherence throughout extended dialogues by retaining and recalling context from earlier in the conversation. This ability enables them to adapt responses to the flow of dialogue, adjusting tone and style as needed. In real-time applications, such as voice interactions or instant messaging, LLMs process and respond promptly, facilitating smooth and believable exchanges. Their scalability allows them to manage numerous interactions simultaneously, and their multilingual capabilities support conversations across different languages, enhancing their utility in diverse settings.

Ethical and Security Challenges

The misuse of AI for such scams highlights the ethical challenges and security issues surrounding AI development and data privacy. It is crucial to establish comprehensive ethical standards and robust security measures to prevent the misuse of both AI technologies and personal data. This includes regulating the use of personal information, securing data against breaches, and monitoring the development and deployment of AI systems.

Proactive Defense: Educating Users with AI-Simulated Scam Awareness Training

To safeguard users against the sophisticated threats posed by generative AI-powered scams, proactive education strategies are essential. By informing individuals of their exposed personal information and potential attack surfaces, they can better understand and recognize their vulnerabilities. One innovative approach involves using generative AI to simulate targeted scams that exploit specific pieces of a user's exposed information.

By experiencing these simulated scams in a controlled environment, users can learn firsthand how scammers might manipulate their personal data. This educational method not only highlights the realistic nature of AI-generated threats but also empowers users to identify and respond effectively to actual scam attempts in the future. This proactive defense strategy is crucial in building resilience against the increasingly personalized and deceptive scams crafted by criminals using advanced AI technologies.

About the Author

Julio Casal, Founder and CIO at Constella Intelligence, is originally from Madrid and has lived in Silicon Valley for 14 years. He has founded and co-founded startups with a combined exit value over $1 billion.

Casal studied Physics at Universidad Complutense in Madrid and began his career by selling video games at the age of 13. In 1995, he launched Cybered, an early email service provider. He then worked as Chief Security Officer for pioneering Spanish ISPs before founding Spain's first dedicated cybersecurity company, IP6 Seguridad, in 1997. In 2003, Casal invented the OSSIM open-source SIEM project and founded AlienVault in 2007. Under his leadership as CEO until 2012, AlienVault raised $110M and was acquired by AT&T in 2018.

He co-founded Constella in 2014, a leading cyber intelligence firm, and has been a founding investor in Wazuh, Stratio, and Playgiga (sold to Facebook in 2019). He advises venture capital firms and invests in Spanish and Hispanic entrepreneurs aiming for global success.

Julio can be reached online at jcasal@constellaintelligence.com and at Constella's website: https://constella.ai/.

Bridging The Manufacturing Security “Air Gap”

By Erik Gross, Deputy CISO at QAD

In the world of manufacturing, one security measure has stood out above all others: the "air gap." This technique, which isolates technology from the outside world, once provided a reasonable shield against cyber threats. However, as our reliance on digital connectivity grows, this once-reliable defense has become as outdated as floppy disks and serial connections.

Integrating operational technology (OT) with information technology (IT) has blurred the lines between previously isolated systems, creating a more complex security landscape. The *air gap* typically refers to technical processes, but the technique has also been applied to the workforce. Many workers are employed without an identity, an email address, or *any* technology. Manufacturers, as the backbone of our industry, who fail to connect their people, their processes, or their technology are at a competitive disadvantage. But that's not to say it's easy.

This challenge is not unique to manufacturing. It's a shared struggle across industries. Healthcare workers navigate the need for quick, often chaotic access to shared devices while the education sector grapples with issuing digital identities to elementary school children who lack email addresses. The demand for secure, efficient, and inclusive technology solutions is universal, underscoring the necessity for innovative, adaptive, and often creative approaches to cybersecurity.

People-Centric Challenges

1. One of the most pressing challenges is managing employees' identities who require access to cloud-based or external applications. Ensuring these identities are managed adequately without overburdening the IT department is critical. For example, a user on a plant floor may need an email address or a secondary device to reset their password efficiently. This problem is exacerbated by the need to ensure security while maintaining productivity. Solutions must be found that balance ease of use with robust security measures to prevent unauthorized access.
2. In many manufacturing environments, shared devices are an everyday necessity. These devices must be accessible to multiple users while maintaining secure and individualized access controls. Managing access to shared devices can be challenging, particularly when preventing unauthorized access and ensuring that all activity on the device is tracked correctly and attributed.
3. The manufacturing sector often relies on temporary workers or experiences high employee turnover. This high rate of onboarding and offboarding employees creates a unique challenge in maintaining cybersecurity standards. Temporary employees may require immediate access to systems and data, but providing individual credentials can be time-consuming and risky. Additionally, high turnover rates mean that credentials need to be constantly updated and deactivated, which can strain IT resources.

Strategies for Robust Cybersecurity

Businesses must address technology and human factors to tackle cybersecurity challenges comprehensively. Here are some key strategies:

1. Access control is built on three pillars: something you know (like a password), something you are (biometric data), and something you have (a security token). In manufacturing environments, where gloves, hairnets, and safety gear are standard, relying on biometric data (something you are) can be tricky. Similarly, issuing physical tokens (something you have) might add excessive costs. Therefore, exploring flexible access solutions, such as temporary or time-based access controls, is crucial to ensure effective and practical security in these unique settings.
2. As technology advances, Multi-Factor Authentication (MFA) is becoming both more accessible and more essential. Now is the time for businesses to start planning for MFA implementation. Companies can ensure a smooth transition by laying the groundwork for MFA, including educating employees about its benefits and preparing the necessary infrastructure. Adaptive MFA offers many promising options for manufacturing.
3. You've automated your production line to boost efficiency and productivity—now it's time to apply that same strategy to digital access. Automating digital access management streamlines the process, reduces the burden on IT departments, and ensures that employees have the access they need when they need it. Automating onboarding, access control, and credential management tasks allows you to maintain a secure environment while freeing up resources to focus on other critical areas. Be sure to dedicate resources and time to your IT team for a future-proof design.

The Path Forward

In conclusion, the evolution of cybersecurity in the manufacturing sector highlights a broader truth: adaptation is critical. Just as the air gap has transitioned from a robust safeguard to a quaint relic, our approach to securing digital identities and access must evolve. Integrating IT and OT presents challenges but offers unprecedented opportunities to rethink and redesign our security frameworks. By embracing flexible access solutions, planning for MFA, and automating digital access management, manufacturers and all industries can stay ahead in the ever-shifting landscape of cyber threats.

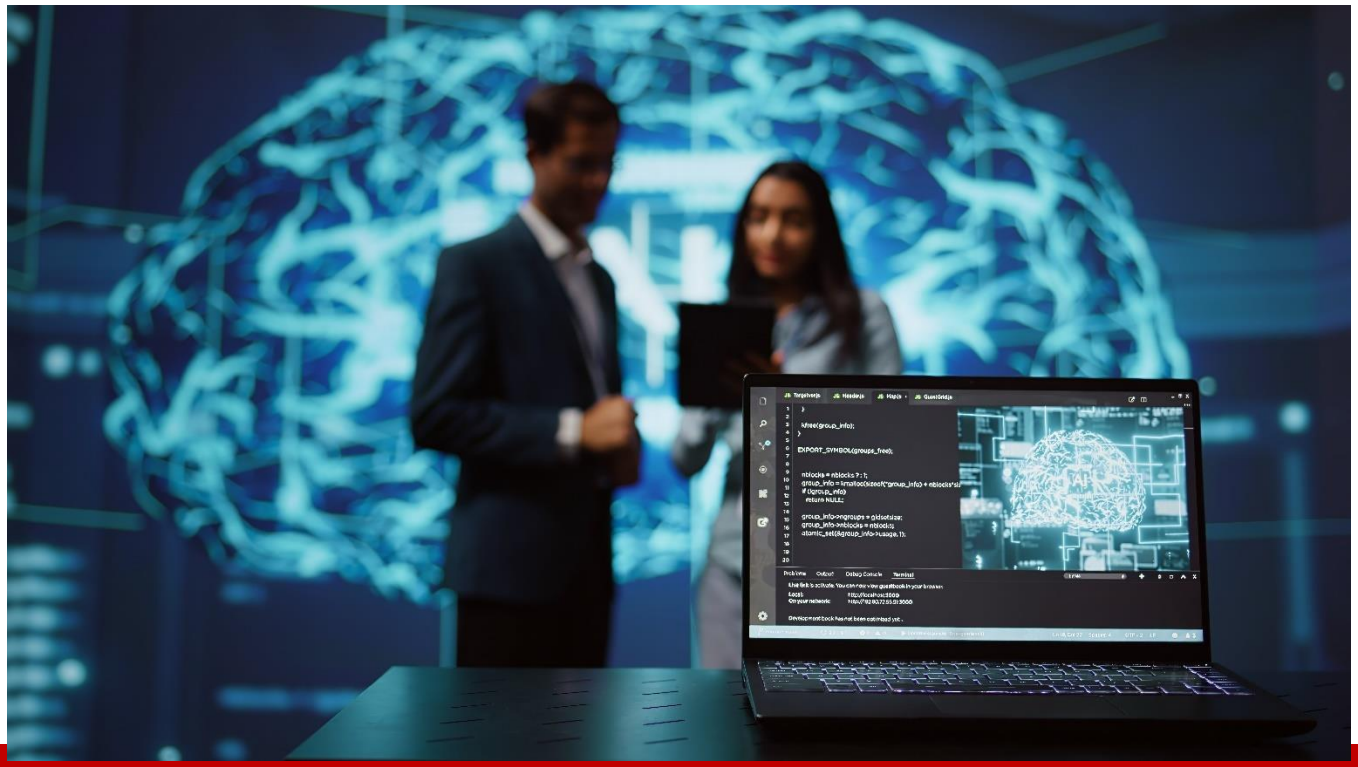
The road to robust cybersecurity is paved with both technological innovation and human-centric strategies. It's about balancing convenience and security, ensuring every employee—from the plant floor to the executive suite—has seamless, secure access without compromising productivity.

Stay vigilant, stay secure, and keep pushing forward.

About the Author

Erik Gross is the Deputy Chief Information Security Officer (CISO) at QAD. Erik leads cybersecurity initiatives, blending his rich experience with a leadership ethos that encourages collaboration and adaptability. At Redzone, Erik was the Vice President of Security, where he was instrumental in developing the security program from the ground up. His professional roots in operational technology (OT) provided a firm understanding of industrial security challenges. His leadership emphasizes the essential role of people in cybersecurity, fostering a culture where teamwork and agility are crucial, thereby enhancing problem-solving and organizational responsiveness. His 15+ years of experience highlights a commitment to strengthening security practices while creating an environment where every team member's input is key to the collective cybersecurity effort.

Erik can be reached online at https://www.linkedin.com/in/erikgross1/ and at our company website https://www.qad.com/.



How vCISOs Can Enhance an Organization's Cybersecurity Posture with Cyber Insurance

By Pete Green, vCISO, Cybersecurity Consultant and Reporter for CDM

In today's digital age, where cyber threats loom large and data breaches are increasingly common, many organizations are turning to **Virtual Chief Information Security Officers (vCISOs)** to bolster their cybersecurity frameworks. These outsourced experts bring specialized knowledge and insights, guiding companies in creating robust security policies and procedures.

But there's another crucial layer of protection that vCISOs can help implement: **Cyber Insurance**. By integrating Cyber Insurance into a company's risk management strategy, vCISOs can offer organizations an additional safety net to deal with financial repercussions after a cyberattack.

Let's break down how vCISOs can leverage Cyber Insurance to enhance an organization's cybersecurity posture, focusing on the current state of cybersecurity insurance, how it is acquired, ways to lower premiums, and how to ensure adequate coverage.

The Current State of Cyber Insurance

Cyber Insurance is no longer a “nice-to-have” for modern businesses—it’s becoming a must-have. With the rise in high-profile breaches like those affecting Equifax, Marriott, and Target, companies are beginning to recognize the devastating financial impact of cyber incidents. These costs can include legal fees, regulatory fines, customer notification expenses, and even lost business due to reputational damage.

Cyber Insurance policies have evolved significantly in recent years, moving from basic coverage of data breaches to more comprehensive offerings that address ransomware, business interruption, and liability. The demand for these policies has skyrocketed, and insurance providers are adjusting their offerings to cater to different business sizes, industries, and risk levels.

For vCISOs, staying up-to-date on the latest Cyber Insurance trends is crucial. Not only can they help organizations identify coverage gaps, but they can also guide them in selecting policies that align with their specific risk profiles. Many businesses are still unclear about what exactly their Cyber Insurance covers, which is where the expertise of a vCISO becomes invaluable.

How Cyber Insurance is Acquired

Acquiring Cyber Insurance is relatively straightforward, but organizations need to prepare. Insurers typically require businesses to undergo an in-depth assessment to determine their risk level before issuing a policy. This assessment often examines factors such as:

- **Existing Security Controls**: Insurers will look at the organization’s cybersecurity framework, including firewalls, endpoint detection, and security awareness training.
- **Compliance Standards:** Companies adhering to industry-specific standards like GDPR, HIPAA, or PCI-DSS may qualify for lower premiums.
- **Incident Response Plans**: Having a well-defined incident response plan can positively impact an organization’s insurability.

vCISOs play a pivotal role in helping organizations prepare for this assessment. They can evaluate current cybersecurity measures, identify areas of improvement, and implement new policies that align with insurers' requirements. In some cases, vCISOs can even help negotiate on behalf of the company, ensuring that the organization receives the best possible coverage at a competitive rate.

How to Lower Your Insurance Rates

For many businesses, the cost of Cyber Insurance can be a major deterrent. However, vCISOs can help companies lower their premiums by optimizing their cybersecurity practices. Insurers reward organizations that demonstrate strong cyber hygiene, and vCISOs can lead the charge in implementing the following strategies:

1. **Adopt a Zero Trust Architecture:** By segmenting networks and ensuring that users only have access to the resources they need, companies can reduce their exposure to cyber threats. Many insurers offer lower rates for businesses that have adopted this model.

2. **Regular Vulnerability Assessments:** Proactively identifying and addressing vulnerabilities can drastically reduce the likelihood of a breach. Insurers view regular vulnerability assessments as a sign that the organization is committed to maintaining its security posture.

3. **Employee Training:** Human error, including insider threats, is often the weakest link in cybersecurity. Offering regular security awareness training to employees reduces the risk of phishing attacks and other social engineering tactics, which in turn can help lower insurance premiums.

4. **Incident Response Drills (Tabletop Exercises):** Insurers prefer companies that are prepared to respond to an attack. Conducting regular incident response drills not only strengthens the organization's preparedness but can also signal to insurers that the business is less likely to suffer prolonged disruptions in the event of an attack.

By ensuring these measures are in place, vCISOs can help companies present a lower risk to insurers, which often leads to reduced premiums.

How to Ensure You Have the Right Coverage

It's one thing to have Cyber Insurance, but ensuring the policy provides adequate protection is another challenge entirely. Many companies fall into the trap of assuming their policy covers every possible cyber threat, only to find out post-incident that they are underinsured or lack coverage for specific scenarios.

vCISOs are instrumental in reviewing policies and ensuring that businesses have the right coverage. Here are key coverage areas that vCISOs should verify:

1. **First-Party Coverage:** This includes the costs directly incurred by the organization during a cyberattack, such as data restoration, customer notification, and legal fees. vCISOs should ensure that the policy offers adequate protection for these expenses.

2. **Third-Party Coverage:** If a cyber incident affects external parties, such as customers or partners, third-party coverage helps with liability claims and legal expenses. vCISOs should assess the scope of this coverage, especially for third-parties that handle sensitive customer data.

3. **Business Interruption:** Many cyberattacks can lead to prolonged business disruptions. vCISOs need to ensure that the Cyber Insurance policy covers lost income and additional operational costs resulting from downtime. This option can typically be the most expensive coverage in a Cyber Insurance policy and should be "right-sized" to cover a 2–3-week period of downtime and the associated daily operating costs of an organization to keep the cost of appropriate coverage as low as possible.

4. **Ransomware & Extortion:** With ransomware attacks becoming increasingly common, having specific coverage for ransom payments and associated costs is essential. vCISOs should verify that policies include this, as well as coverage for negotiating with threat actors. It is rarely recommended that an

organization make extortion payments, but ransomware coverage can help defray those costs in the uncommon case that an extortion payment would be cheaper than an extended business disruption.

By meticulously reviewing policies, vCISOs can ensure that organizations are not only protected but also positioned to recover from cyberattacks with minimal financial strain.

The vCISO's Expanding Role in Cyber Insurance

Just like other insurance types, Cyber Insurance policies need to be renewed regularly, often annually. However, the renewal process is not always straightforward. If a company has experienced a breach or incident, it may face increased premiums or reduced coverage. A vCISO helps organizations navigate the renewal process by addressing any gaps in security that were exposed in the previous coverage period. By proactively improving the company's cybersecurity posture, the vCISO can negotiate better rates and ensure continued coverage. Additionally, they can provide the necessary documentation and reporting to insurers to demonstrate the organization's efforts in reducing cyber risks.

"Silent cyber" refers to cyber risks that are not explicitly covered under standard insurance policies but may still affect an organization. These risks might include physical damage caused by a cyberattack, such as damage to a manufacturing line or office equipment, business interruptions, or liabilities that arise from non-compliance with data privacy laws. vCISOs are increasingly being tasked with identifying these "silent cyber" risks and working with both internal teams and insurance providers to close coverage gaps. By addressing these hidden risks, a vCISO ensures that the company is fully protected, even against indirect or unforeseen consequences of cyberattacks.

Certain industries or types of businesses face unique cyber risks that may not be adequately covered under a typical Cyber Insurance policy. For example, a healthcare organization might require coverage for HIPAA violations, while a financial services company could need additional protection against fraudulent transactions. A vCISO's industry-specific knowledge is invaluable in negotiating customized Cyber Insurance policies. They can work directly with brokers to ensure that the organization's specific risks are covered, often securing tailored policies that offer more comprehensive protection than generic plans.

Filing a Cyber Insurance claim can be a complex process, particularly when it comes to proving the extent of damages and losses. vCISOs are essential in this process, as they can provide detailed documentation of the incident, including timelines, affected systems, remediation efforts, and ongoing risks. Their expertise can also expedite the claim process, ensuring that the organization receives the financial support it needs to recover quickly. Furthermore, vCISOs can assist in quantifying the long-term impact of a cyberattack, such as business interruption losses or reputational damage, which are often required for claims involving complex or high-value incidents.

Lesser-Known Facts About Cyber Insurance

Cyber Insurance Policies Can Vary Dramatically

While Cyber Insurance policies have become more common, many organizations are unaware of how different policies can be in terms of coverage. Some policies may only cover specific types of cyber incidents (like data breaches), while others might include more comprehensive protection, such as coverage for intellectual property theft, damage to digital assets, and even defamation.

vCISOs play a critical role in helping organizations understand the differences in policies. They analyze the fine print, identify exclusions, and ensure that the organization isn't left vulnerable due to overlooked coverage gaps.

Post-Breach Assistance

One often-overlooked benefit of Cyber Insurance is the post-breach assistance provided by insurers. Many policies offer access to a network of expert services, such as forensics teams, breach response coordinators, legal counsel, and public relations specialists. These services can be invaluable in containing and mitigating the damage caused by a breach.

A vCISO can help an organization fully leverage these services by coordinating with the insurance provider after an incident and ensuring that the company gets the appropriate support. This is especially important in the chaotic aftermath of a cyberattack, where quick decisions and effective communication are critical.

Cyber Insurance is Becoming a Business Requirement

As cyber threats evolve, more companies (especially those in highly regulated industries) are making Cyber Insurance a contractual requirement. This means that businesses seeking to partner with certain organizations may need to have adequate Cyber Insurance coverage in place to even be considered.

vCISOs help organizations navigate these contractual obligations and ensure they meet the Cyber Insurance requirements of potential clients or partners. This not only helps in securing business deals but also strengthens the company’s overall risk management posture.

Evolving Ransomware Clauses

With the rise of ransomware attacks, many Cyber Insurance policies now include specific clauses that outline how the insurer will handle ransom payments. However, these clauses can be complex. Some insurers may cover the ransom itself but not the negotiation process, while others might have strict requirements before making payments, such as using a pre-approved forensics firm to verify the attack.

A vCISO can help ensure that the organization complies with these requirements in the event of a ransomware attack. They also provide strategic advice on when and how to involve law enforcement and whether paying the ransom is advisable based on the company's specific situation.

Conclusion

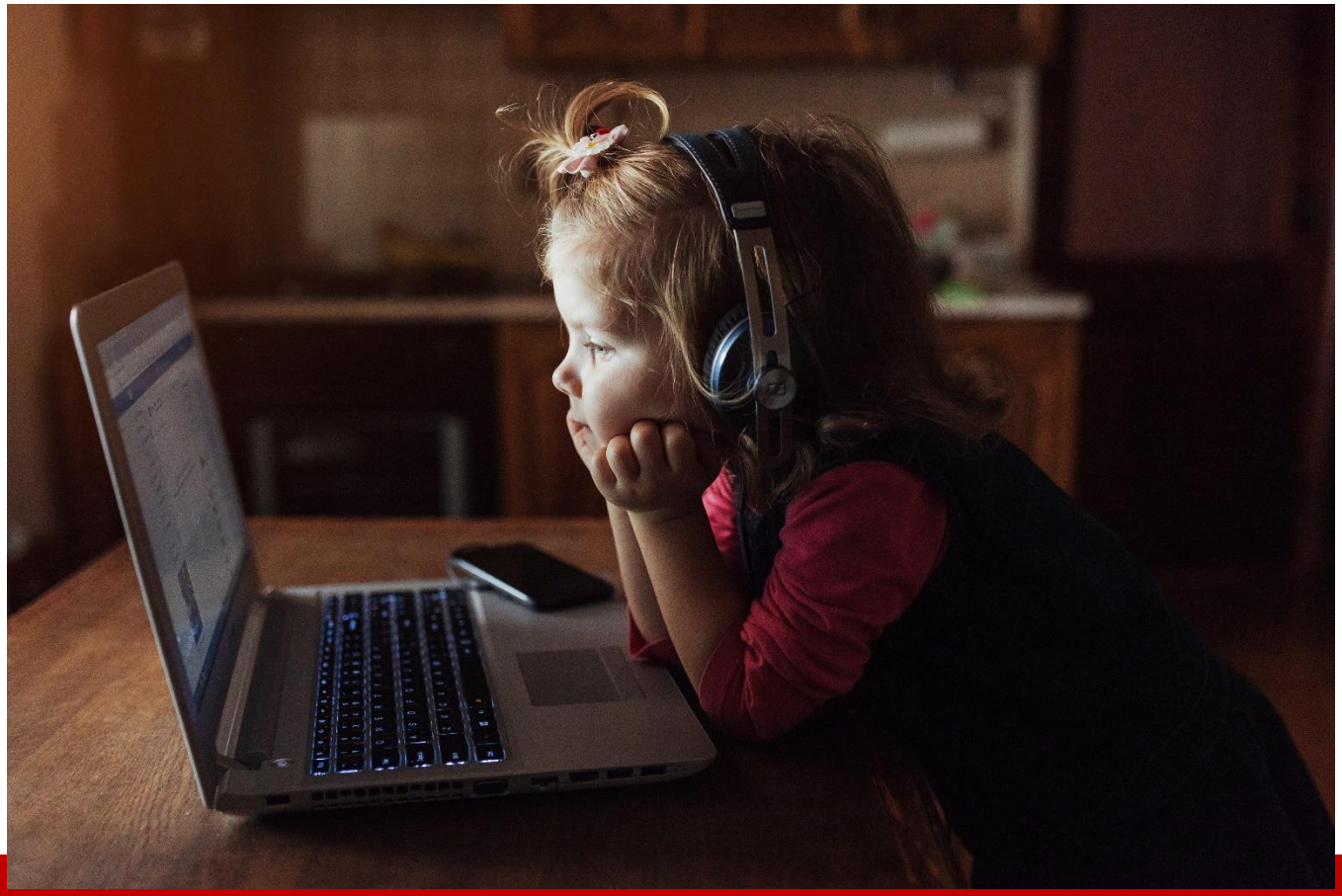
The role of a vCISO extends far beyond simply improving an organization's cybersecurity practices. When paired with the right Cyber Insurance policy, a vCISO becomes a strategic asset in protecting the organization both from the immediate threats posed by cyberattacks and the long-term financial consequences that can arise. By understanding the intricacies of Cyber Insurance and ensuring that the company is both well-covered and actively mitigating risk, a vCISO can help safeguard the organization's future in an increasingly hostile digital environment.

About the Author

Pete Green, vCISO, Cybersecurity Consultant and Reporter for CDM. Pete Green has over 20 years of experience in Information Technology related fields and is an accomplished practitioner of Information Security. He has held a variety of security operations positions including LAN / WLAN Engineer, Threat Analyst / Engineer, Security Project Manager, Security Architect, Cloud Security Architect, Principal Security Consultant, Manager / Director of IT, CTO, CEO, and Virtual CISO. Pete has worked with clients in a wide variety of industries including federal, state and local government, financial services, healthcare, food services, manufacturing, technology, transportation, and hospitality.

Pete holds a Master of Computer Information Systems in Information Security from Boston University, an NSA / DHS National Center of Academic Excellence in Information Assurance / Cyber Defense (CAE IA / CD), and a Master of Business Administration in Informatics.

Pete can be reached online at greenish@gmail.com, @petegreen, https://linkedin.com/in/petegreen and at our company website http://www.guidepointsecurity.com/.



To Combat Cyberbullying and Online Fraud, We Must Do More to Protect Minors

Research Shows That Cyberbullying and Extortion Go Hand in Hand. The Kids Online Safety Act (Kosa) Is A Promising First Step Toward Addressing a Growing Threat

By Tracy Kitten, Director, Fraud & Security, Javelin Strategy & Research

The last 20 years have fundamentally redefined how consumers behave online. The emergence of sites such as YouTube, Meta, and X has reshaped how we share and consume media. Online gaming platforms have exploded in popularity, and messaging applications like WhatsApp have made it easier to stay in touch. But there is a dark side to this evolution.

While the digital landscape has transformed, little has been done to shield minors from the adverse effects of online exposure, such as cyberbullying and extortion. Meanwhile, cybercriminals have adopted increasingly sophisticated methods to target users — with few or no consequences on the platforms where these individuals operate.

Data indicate that the scope and seriousness of online threats are only rising. The last time lawmakers passed legislation to address this issue was in 1998, when the Children's Online Privacy Protection Act (COPPA) was enacted. Now, a landmark bill could begin the process of holding digital platforms accountable for harm posed to minors.

A 'Duty of Care' for Children Online

The Kids Online Safety Act (KOSA), which passed the Senate with bipartisan support in July, would require social media sites to create safeguards to protect minors from potentially harmful content, such as violence, pornography, hate speech, and misinformation. The bill would mandate that sites automatically enable the highest privacy and safety settings for children and allow younger users to opt out of features like personalized recommendations. It would also enforce a "duty of care" for digital platforms, including gaming and messaging sites, requiring them to take reasonable steps to prevent harm to minors.

KOSA, which has been paired with an updated version of the Children and Teens' Online Privacy Protection Act (COPPA 2.0), represents the most significant congressional action to protect children online in decades. However, while this is a welcomed development for child safety advocates, evidence suggests it is only scratching the surface of a pervasive and growing problem.

Addressing an Escalating Threat

According to Javelin Strategy & Research, 73% of U.S. households are concerned about cyberbullying. However, less attention is given to the ways these behaviors can repeat and escalate, leading to instances of identity fraud and phishing. Javelin finds that cyberbullying is most prevalent among children aged 10 to 12 — a vulnerable group of users that often have little understanding of how to protect themselves online. Minors are most at risk of being cyberbullied on YouTube, Snapchat, TikTok, and Facebook, although digital gaming and messaging platforms also pose a threat.

Online and social media engagement among children has increased dramatically since the COVID-19 pandemic, which prompted a surge in the use of digital technologies among users of all ages. Security.org reports that 79% of children active on YouTube have been cyberbullied since the pandemic. Meanwhile, only 11% of teenage victims of cyberbullying told their parents or caregivers, suggesting that, in many cases, adults are unlikely to be in a position to intervene.

Perhaps most disturbing, Javelin's most recent "Child ID Theft: Social Cyber Risks and the Persistent Threat to Families" report finds that minors who are cyberbullied at a young age are more likely to be cyberbullied and victimized by identity fraud as they get older. Almost three-quarters (71%) of households that reported having a minor victimized by fraud noted that their child had previously been bullied, with 31% specifically cyberbullied.

The Correlation between Cyberbullying and Fraud

The compounding nature of cyberbullying, scams, and fraud emphasizes the need for proactive intervention. Rather than adapting their behavior based on early and negative experiences, research indicates that children who are targeted online in their youth are more likely to be vulnerable to socially engineered deceptive lures like phishing and romance scams as teenagers and adults.

Cyberbullying and online extortion are closely linked. Both occur on digital platforms such as social media, gaming, and messaging sites. Cyber attackers commonly use social engineering techniques to build trust before psychologically manipulating their targets into providing sensitive or confidential information. Similarly, cyberbullies make use of the growing volume of personal data available online to identify and exploit users' vulnerabilities.

Caregivers can play a role in addressing the threat of cybercrime by educating children about the perils of sharing information online, monitoring digital activity, and investing in identity protection services (IDPS). However, after years of escalating risk, it is clear that federal action is necessary.

Holding Social Media Platforms to Account

As it stands, there are limited legal guardrails in place to protect minors online. There are few controls around how content is marketed and how accounts are vetted, and children signing up for social media platforms can often circumvent age restrictions simply by lying. KOSA represents a promising step in the right direction. But even if the bill successfully clears the House of Representatives, more must be done to ensure robust protections are established for children using the web.

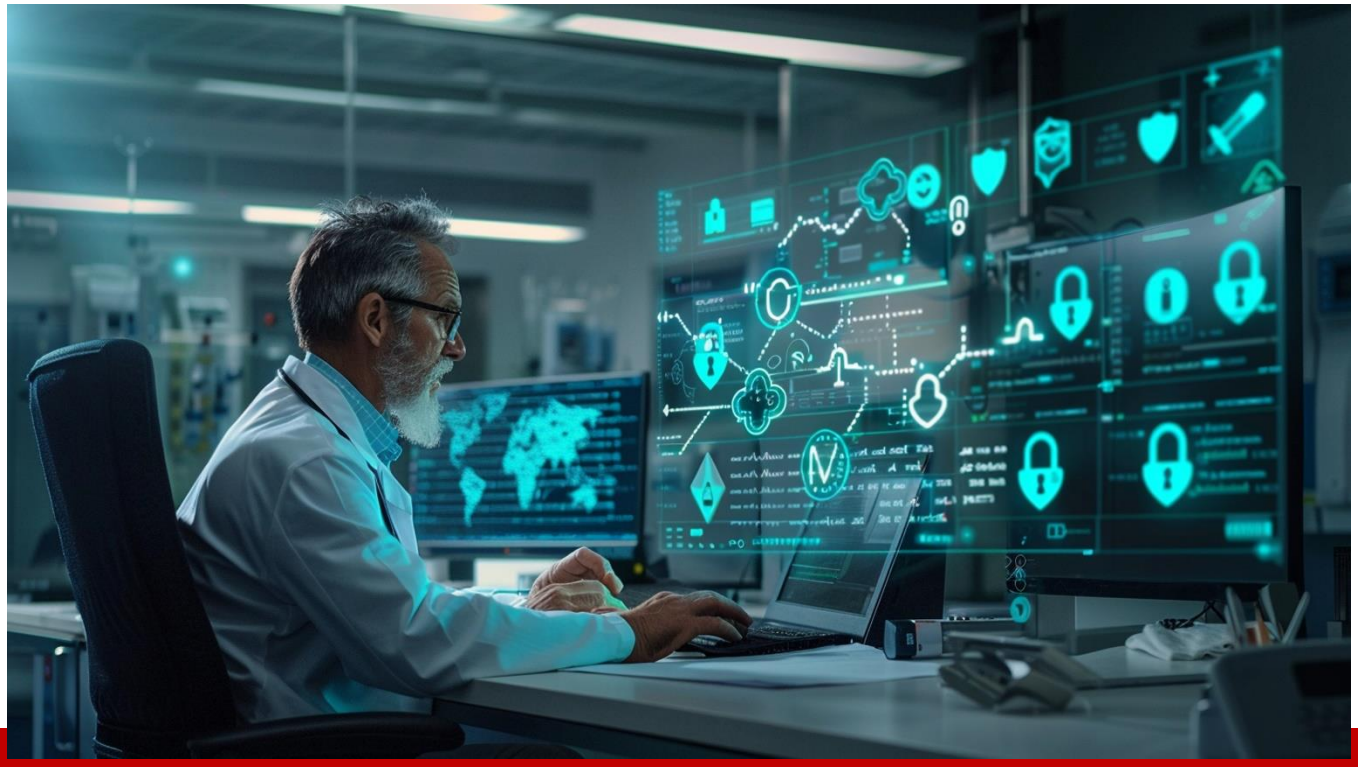
For starters, consumers and lawmakers need to embrace a more expansive definition of social media, something for which KOSA lays the foundation. While many are familiar with high-profile cases of cyberbullying and abuse on platforms such as Meta and X, parents and guardians are less aware of the dangers posed by gaming sites. Javelin found in 2022 that 41% of children who fell prey to online scams were targeted after downloading a game or mobile application.

Online social, gaming, and messaging sites are unregulated, unpredictable, and risky. These platforms must be held accountable for monitoring the content they host, enforcing age restrictions, and complying with established models of parental consent. Until these sites face tangible consequences for the misconduct they play a role in facilitating, they will have no impetus to tighten their security measures to address the very real threats that minors encounter online.

About the Author

Tracy Kitten is the Director of Fraud and Security at Javelin Strategy & Research. Tracy is a recognized fraud and cybersecurity subject matter expert within the financial services community. A veteran journalist who has covered fraud, payments, financial technology, and cybersecurity for the last 20 years, Tracy has watched attacks and cyberthreats evolve, having spoken with countless industry experts, practitioners, and sometimes even hackers to anticipate what's coming next.

As the Director of Fraud and Security at Javelin Strategy & Research, Tracy brings her years of experience to help her practices and their clients grow and strengthen resiliency. Tracy can be reached online at tracy.kitten@javelinstrategy.com and at https://javelinstrategy.com/.



How The Right Application Server Can Protect Healthcare and Public Institutions from Cyber Attacks

A look at the current status of cybersecurity in the healthcare and public sectors and how organizations can boost the robustness and resilience of their software.

By Louise Castens, Senior Product Manager at Payara, and Chiara Civardi, Marketing Coordinator at Payara

Cybersecurity in the public and healthcare sectors is a growing concern as cyberattacks become increasingly sophisticated and frequent. However, many existing vulnerabilities can be easily addressed to deliver more robust and resilient systems. Selecting a fully supported and patched application runtime eliminates possible vulnerabilities that can be exploited. This strengthens the security protections for healthcare and public infrastructures. Organizations can thus protect their businesses, patients and citizens while improving their reputation and cost-effectiveness.

The engineering team behind the Payara Platform closely monitors incidents of cyberattacks on public and healthcare systems globally, particularly focusing on how to protect the mission-critical application infrastructure in order to support end users with a robust solution. Current trends indicate that the number of data breaches and cybersecurity attacks targeted to healthcare and public bodies' systems is increasing. In particular, the Center for Internet Security found that malware attacks in 023 increased by

148% compared to the previous year. According to the report, 2023 also saw a 313% rise in endpoint security services incidents, such as data breaches, unauthorized access and insider threats.[1]

Whenever these issues occur, a cascade of issues take place. For healthcare providers, delivery of care can be delayed, compromising patients' lives. When it comes to state and local public offices, such issues can threaten citizen privacy, disrupt government functions, undermining confidence in governance.

In both cases, data safety is affected and organizations incur unpredictable expenses. While public sector expenses for data breaches are relatively low, at USD 2.60 million per incident, healthcare reported the highest costs of all industries. The average expenditure to address a healthcare data breach is estimated at USD 10.93 million, with such figure increasing of 53.3% over the past three years. [3]

The U.S. government's Health Insurance Portability and Accountability Act (HIPAA) reported on the causes and costs of security breaches in healthcare. It also offered an insight into why healthcare systems are particularly exposed to cyberthreats.

It states: "The healthcare industry is struggling to deal with increasingly sophisticated cyberattacks, although in many incidents cyber threat actors have exploited vulnerabilities that should have been identified and addressed long before they were found and exploited by hackers. Many healthcare organizations are failing at basic security measures and are not consistently adhering to cybersecurity best practices due to budgetary pressures, difficulty recruiting and retaining skilled IT security professionals, and confusion about the most effective steps to take to improve resilience to cyber threats." [2]

Similarly, when it comes to the United States' nation's state, local, tribal, and territorial (SLTT) governments, "SLTT organizations reported not performing a number of cybersecurity activities or doing so only in an informal or partial manner", according to the Nationwide Cybersecurity Review: 2022 Summary Report. [1]

State-of-the-art technology to ensure cyber resilience

Cyberattacks on public and healthcare systems occur simply because state and local governments, public offices, medical trusts, hospitals, clinical, and patient data provide valuable targets and can be lucrative if ransom demands are met. Besides, healthcare providers and government bodies are typically viewed by hackers as an easy target for cyberattacks, since they can take advantage of a number of vulnerabilities in their system infrastructures. For example, when looking at application runtimes, a number of production systems in these sectors often rely on legacy, unsupported or outdated solutions. A typical example is companies running production systems on the GlassFish Project or open source technologies that lack commercial support and are not designed for mission-critical business applications and production environments.

In effect, neither offer the high level of protection that can reduce vulnerabilities. This leaves a broad attack surface and opportunity for such vulnerabilities to be exploited by malicious actors.

While the current situation may seem dire, there are a number of existing solutions that healthcare organizations and public bodies can already leverage to enhance the security and regulatory compliance of their application servers and digital systems. Firstly, companies should migrate to a commercially supported and up-to-date application runtime.

The ideal solution should offer a variety of tools that support advanced encryption, authentication, authorization, verification, segmentation and compartmentalization. In addition, it should quickly deliver security reports with critical security vulnerabilities as Common Vulnerabilities and Exposures (CVE) to users and public security databases, as well as making the relevant public disclosures. These activities help to swiftly identify and address exploits.

Partnering with a security-oriented expert

By establishing a solid relationship with an application server provider and its support team, healthcare organizations and government bodies can better protect their systems, data, citizens and patients against the evolving threat landscape. Even more, such a partnership can help streamline the application server migration process, slashing the associated time, cost and resources while ensuring performance and effectiveness of the software applications.

When looking for a suitable vendor, it is important to favor a provider with a strong security policy and that releases frequent security fixes and upgrades for their products. For example, the Payara Platform Enterprise benefits from monthly releases. In addition, partnering with a specialist that adheres to key standards and specifications while contributing to cyber resilience technical working groups and taskforces is highly beneficial.

Finally, protecting systems and businesses through a comprehensive service level agreement (SLA) is key to minimizing downtime and its associated costs. This agreement not only outlines the responsibilities and expectations for both parties but also includes provisions for regular maintenance, incident management and penalties for non-compliance. By establishing these guidelines, organizations can ensure continuous operation, mitigate risks and protect patients' safety.

At Payara, we are dedicated to helping organizations deliver world class applications through our fully supported Jakarta EE runtimes. We offer standard-based APIs and advanced security tools that are designed to protect application resources accessed by multiple users and data traveling across unprotected networks, such as the internet. In addition, we align with the National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) and adhere to guidelines set by the Open Web Application Security Project (OWASP). Payara is also part of the Eclipse Foundation's Open Regulatory Compliance Working Group to help develop specifications that enable the Enterprise Java software development industry to meet regulatory requirements, such as those outlined in the EU Cyber Resilient Act (CRA).

Finally, transparency and quick resolution of security issues are paramount to us. We report CVEs to The Mitre Corporation and other public security databases. Also, as a CVE Numbering Authority (CNA), we help control the information published on the CVE Index, ensuring quick identification, resolution and transparent communication of security vulnerabilities.

References

[1] Multi-State Information Sharing and Analysis Center® (MS-ISAC®), Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®). (2023). Nationwide Cybersecurity Review: 2022 Summary Report. Available at: https://learn.cisecurity.org/NCSR-2022-Summary-Report [Accessed: 24 July 2024].

[2] Alder, S. (2024). Security Breaches in Healthcare. The HIPAA Journal. Available at: https://www.hipaajournal.com/security-breaches-in-healthcare/ [Accessed: 19 July 2024].

[3] IBM. (2023). Cost of a Data Breach Report 2023. Available at: https://www.ibm.com/reports/data-breach [Accessed: 24 July 2024].

About the Authors

Louise Castens is a Senior Product Manager and Product Lead at Payara, and she is committed to helping shape technology solutions that deliver value to end users. Louise has more than 15 years of experience in Product Management - identifying opportunities, delivering quality solutions, sustained results and effective change for businesses and clients across a wide range of B2B and SaaS products and industries. With a business background, some of her specialties and certifications include Agile frameworks, Business Analysis and Process optimization. Louise can be reached online at louise.castens@payara.fish and at our company website www.payara.fish.

Chiara Civardi is a Marketing Coordinator with over 10 years of experience in producing content on anything technological, from industrial automation and networking technology to developer tools, Cloud and Edge computing as well as AI. She has a passion for sharing insights that are technically accurate and engaging. Chiara holds a PhD from ETH Zurich and a MSc from the University of Southampton. Chiara can be reached online at chiara.civardi@payara.fish and at our company website www.payara.fish.

Win or Lose: Using CMMC 2.0 Proposed Rule to Position Yourself for DOD Contracts

By Isaias "Cy" Alba, IV, Partner, Daniel Figuenick, III, Associate PilieroMazza PLLC

The Cybersecurity Maturity Model Certification (CMMC) Program has been a headache for many defense contractors since the idea was first introduced in 2019. The program seeks to protect unclassified information, including federal contract information (FCI) and controlled unclassified information (CUI) not intended for public release, shared by the Department of Defense (DOD) with its contractors and subcontractors. In December 2023, the DOD proposed a rule to formally codify the CMMC Program in a phased rollout. The DOD has now released a proposed rule (Proposed Rule) relevant to Phase 1, another step towards the ultimate goal of requiring certain DOD contractors handling sensitive information to achieve a particular CMMC level as a condition of contract award. DOD contractors that process, store, or transmit FCI or CUI (or plan to do so in the future) must become familiar with the CMMC Program as it could 'make-or-break' winning or losing major government contracts.

General Overview of CMMC

DOD procuring activities will assign solicitations and contracts a certain CMMC level depending on the type and sensitivity of the information being shared with or developed by the awarded contractor (or its subcontractors). There are three CMMC levels. CMMC Level 1 requires a contractor to self-assess and attest to compliance with all 15 basic safeguarding requirements to protect FCI currently listed in Federal Acquisition Regulation (FAR) clause 52.204-21. CMMC Level 2 can require a self-assessment or a certification depending on the solicitation/contract. For the self-assessment, contractors will need to verify that all applicable security requirements, as listed in National Institute of Standards and Technology (NIST) Special Publication (SP) 800–171, have been implemented for any relevant assets, as is already required by Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204–7012. For the certification, one of the major differences is that an authorized or accredited C3PAO[1] is required to validate the implementation of the NIST SP 800-171 security requirements. Finally, CMMC Level 3 requires that the DOD assess a contractor's implementation of all CMMC Level 2 requirements as well as those additional, enhanced security requirements from NIST SP 800-172. For CMMC Levels 2 and 3, contractors that do not have a high enough total assessment score may need to create and implement a Plan of Action and Milestones (POA&M) that must be closed out within 180 days to achieve the requisite level.

Phased Rollout of CMMC

DOD initially (and ambitiously) expected CMMC to be fully implemented by October 2026. The December 2023 proposed rule regarding the implementation of CMMC into Title 32 of the Code of Federal Regulations was significant but did not address the implementation of the program's requirements into solicitations. The phased rollout of CMMC is as follows:

- Phase 1 begins once the DFARS 252.204-7021 rulemaking becomes effective. CMMC Level 1 and Level 2 Self-Assessment requirements will be included as conditions to contract award in all applicable solicitations.
- Phase 2 starts six months following the beginning of Phase 1. CMMC Level 2 Certification requirements will be included as conditions to contract award in all applicable solicitations.
- Phase 3 proceeds one year after the start of Phase 2. CMMC Level 2 Certification requirements will be included as a condition of exercising an option period. Also, CMMC Level 3 Certification requirements will be included in all solicitations as a condition of contract award.
- Phase 4 initiates one year after Phase 3 begins and requires full implementation of the CMMC Program. All three level requirements must be included as (1) conditions to contract award in all solicitations and (2) conditions to exercise option periods in all contracts.

This Proposed Rule addresses how DOD plans to implement the CMMC Program into solicitations moving forward. Once the Proposed Rule goes through appropriate notice-and-comment rulemaking, a subsequent final rule is published, and the DFARS revisions made effective, then Phase 1 will have officially begun.

Proposed DFARS Revisions

Two notable revisions are described in the Proposed Rule:

First, DFARS 252.204-7021 – Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirements, will be included in all solicitations, contracts, and task/delivery orders that require contractors to have a CMMC certificate or CMMC self-assessment at a specific level, except for acquisitions of solely commercially available off-the-shelf items. The clause will have a placeholder for the Contracting Officer (CO) to assign the applicable CMMC Level to the solicitation/contract. The requisite CMMC Level must be maintained for the entire life of the contract for all applicable information systems and contractors will need to notify the CO within 72 hours if there is a lapse or change in a CMMC certificate/self-assessment level during performance. In addition, contractors and subcontractors will need to complete and maintain annually (or when a change to CMMC compliance status occurs) an affirmation of continuous compliance in the Supplier Performance Risk System (SPRS) for the relevant security requirements depending on the CMMC level.

Second, a new clause DFARS 252.204-7YYY – Notice of Cybersecurity Maturity Model Certification Level Requirements will be implemented to, like above, notify contractors of the applicable CMMC certificate or self-assessment level. It expressly provides that apparently successful offerors will be ineligible for contract award if they do not have *current* results for their CMMC certificates/self-assessments, at the minimum level required by the solicitation, uploaded into SPRS. *Current* means:

1. for CMMC Level 1 Self-Assessments, not older than 1 year with no changes in CMMC compliance since the date of the assessment;
2. for CMMC Level 2, not older than 3 years with no changes in CMMC compliance since the date of the assessment;
3. for CMMC Level 3, not older than 3 years for Level 3 certificates with no changes in CMMC compliance since the date of the assessment; and
4. for affirmations of continuous compliance with 32 C.F.R. part 170, not older than 1 year with no changes in CMMC compliance since the date of the affirmation.

Key Takeaways

1. Application to Contracts. Phase 1 of the Rollout does not begin until the effective date of the Final Rule implementing CMMC into the DFARS. Of course, COs do have the *discretion* to bilaterally incorporate the clause in contracts in effect prior to the effective date of the clause with appropriate consideration.
2. Current Certifications/Self-Assessments in SPRS. Understanding when certifications/self-assessments expire will be crucial to winning contract awards. Having a certification or self-assessment expire even one day prior to contract award will cost contractors major contract opportunities.
3. Flow-downs to Subcontractors. Contractors must flow down CMMC's requirements to applicable subcontractors. While no tool exists that would allow subcontractors to electronically share the results of their assessments with their prime contractors, the prime contractor is expected to work

with its suppliers to conduct verifications as it would under any other clause requirement that applies to subcontractors.

4. Joint Venture Compliance. In the previous interim rule applicable to CMMC 1.0, many commenters asked how to handle CMMC certifications and CMMC self-assessments for joint ventures. DOD has explained that each individual venturer that has a requirement for CMMC would be required to comply with the requirements related to the individual entity's information systems that process, store, or transmit FCI or CUI during contract performance.
5. Protesting CMMC-Related Issues. The potential protest grounds for CMMC requirements are numerous. For example, in the post-award context, if an agency removes an offeror from consideration of award for failing to have the requisite CMMC Level at the time of proposal submission as opposed to at the time of award, the agency's conduct in this regard could be considered "unreasonable" and/or "arbitrary and capricious" depending on the protest forum the offeror selects.

Comments on the Proposed Rule are due by October 15, 2024, and can be submitted here. PilieroMazza's attorneys are monitoring any new developments related to the Proposed Rule and will provide an update when the rule becomes final.

[1] A C3PAO is a service provider organization that the CMMC Accreditation Body (CMMC-AB) has accredited and authorized to conduct CMMC assessments and submits findings and certify that Organizations Seeking Certification (OSCs) comply with the relevant CMMC 2.0 maturity level.

About the Author

Isaias “Cy” Alba, IV, Partner. PilieroMazza PLLC. Cy Alba is a Partner at PilieroMazza. He counsels clients in a broad range of government contracting matters before government agencies and federal courts that include overall regulatory compliance with FAR and DFARS requirements, as well as other procurement laws and regulations. Cy also represents companies of all sizes with compliant corporate structuring, mergers and acquisitions, and small business rules and regulations. He handles the prosecution and defense of small business size and status protests and appeals, as well as bid protests and claims before administrative agencies and federal courts.

Cy can be reached at ialba@pilieromazza.com and on our website at https://www.pilieromazza.com/people/isaias-cy-alba-iv/.

Daniel Figuenick, III, Associate. PilieroMazza PLLC. As an Associate in PilieroMazza’s Government Contracts Group, Daniel’s practice centers on providing legal support to businesses operating in the federal procurement space. He works with clients on all matters relating to government contracts law, including handling the bid protest process, navigating the Small Business Administration’s small business programs, and assisting in requests for equitable adjustment (REAs), claims, and appeals.

Daniel can be reached at dfiguenick@pilieromazza.com and on our website at https://www.pilieromazza.com/people/daniel-figuenick-iii/.

Cyber Score, OSINT, and the Transformation of Horiens Risk Advisors in Latin America

By Ronaldo Andrade CISO – Horiens Risk Advisors

Introduction

The cybersecurity landscape is constantly evolving, and organizations face increasing challenges in protecting their digital assets, often referred to as the “Crown Jewels.” In this context, the use of Open-Source Intelligence (OSINT) and the development of a cyber score have become essential strategies for assessing risks and making informed decisions, particularly regarding risk transfer and cyber insurance.

Cyber Insurance in Brazil: • Global Perspective:

The demand for cyber insurance is growing as cyberattacks become more frequent. Recent reports indicate that cyber insurance premiums increased from $4.7 billion in 2018 to $9.2 billion in 2021, with projections to reach $22.1 billion by the end of 2025.

Brazil:

A survey by SUSEP (Superintendência de Seguros Privados) revealed that cyber risk insurance premiums collected a total of R$ 98.12 million in the first half of 2023, representing a 27.2% increase compared to the same period last year. The topic remains relevant in 2024 due to the significant financial impacts and operational disruptions caused by cyber incidents. Additionally, potential reputational damage is severe, as it erodes people's trust in the affected company.

What is a cyber score?

It is a metric that assesses an organization's security posture. It considers factors such as vulnerabilities, exposure to threats, incident history, and implemented protection measures. An effective cyber score allows companies to identify areas for improvement and prioritize investments in security. Horiens partners with Security Scorecard for this process and has a successful track record using the tool for its own monitoring before applying the solution to its clients.

Use of OSINT for monitoring

OSINT (Open Source Intelligence) is the process of collecting and analyzing publicly available information to assess threats. It involves searching sources such as internet search engines, print media, social networks, online forums, and public records. Horiens Risk Advisors uses OSINT techniques to monitor threats, identify vulnerabilities, and anticipate potential attacks. This process aims to assess leaked credentials that are constantly used for targeted attacks on executives and decision-makers. The infostealer market is vast in the deep and dark web, and this is a measured risk portrayed to Horiens' clients through excellence in risk analysis.

Risk forms for insurers

The completion and submission of risk forms are crucial for the cyber insurance sector. Horiens has developed efficient processes to collect relevant information from clients and assess associated risks. These forms allow insurers to make informed decisions and o9er adequate coverage.

This process has been repeatedly highlighted in specific insurance forums, and we see slow progress on this topic from insurers. We believe that we should be the solution to the risk, not part of it. Therefore,

using encryption and appropriate tools for handling this traffic has set Horiens apart from its direct competitors and is changing the game, especially in critical infrastructure and large industries

Threat intelligence and Horiens

Horiens Risk Advisors is at the forefront of threat intelligence usage in Latin America for the Cyber market. Their team of experts analyzes OSINT data, develops customized cyber scores, and provides actionable insights for clients. With real statistics from the Brazilian cyber insurance market, Horiens is offering innovative solutions and protecting companies against digital threats.

We believe our main differentiator is having technical leaders who can directly engage with risk stakeholders in each business. That's why we have a CISO (Chief Information Security Officer) speaking directly with the CIO/CTO/CISO of each client. This goes beyond being a mere differentiator it's a technical relationship of trust that makes perfect sense in such a sensitive area as cyber posture and resilience.

In summary, our approach and the development of a specific framework for Cyber Risk analysis are as follows:

Conclusion

Cybersecurity is fundamental, that is indisputable. And Cyber Insurance is no longer discretionary, it's a latent necessity that aims to protect assets, companies, and their business continuity. Horiens Risk Advisors demonstrates how the combination of cyber score, OSINT (Open Source Intelligence), and threat intelligence can transform digital protection in Latin America. The company not only keeps up with trends but also sets them, ensuring a safer environment for its clients.

About the Author

Ronaldo Andrade is a CISO at Horiens Risk Advisors, responsible for Cyber Insurance in the market. His background is in computer networks, with a specialization in business from NOVA Business School in Portugal. Ronaldo holds over 56 certifications in Cyber Security, Data Privacy, Critical Infrastructure, Technology Investigation, and Regulations. He serves as CISO at Horiens and as Director of Cyber Security at the Institute for Combating Cyber Crime (INCC). He is also a frequent speaker, having delivered over 40 lectures in Brazil, Latin America and the USA.

The Five Steps to vCISO Success

By David Primor, Co-Founder and CEO of Cynomi

The demand for vCISO services is on the rise as companies are seeking cost-effective solutions for reliable cybersecurity surveillance. In fact, 61% of mid-sized businesses do not have in-house cybersecurity staff providing proof that there is more room for growth for MSPs and MSSPs and their services. To fully capitalize on these opportunities, outlined are five steps MSPs should follow within the first 100 days when engaging with a new vCISO client to ensure that they provide reliable vCISO services. The five steps act like a waterfall as each step flows into one another and cannot be completed without starting the next step.

Step 1: Research (Days 0 – 30)

To fully understand the client's needs and security gaps, you must perform thorough research and discuss with the board of directors to acknowledge your client's specific wants and needs regarding their

security requirements and desires. Management should also be encouraged to comprehend this material and acknowledge the importance of cybersecurity as it may aid in its implementation of essential measures.

This first step involves five tasks that are crucial for vCISO's success:

1. Meet with stakeholders and management: This is where the discussion begins in identifying the client's pivotal assets.
2. Identify Critical Assets: Establish the key aspects of the business including identifying which line-of-business applications are in use. This is essential for efficiency and productivity, cost management, risk management, strategic planning, as well as training and support.
3. Assess Data Storage: Perform audits regarding the allocation of data and where the data is stored.
4. Evaluate the Impact of Downtime: Review the implications of key systems being down over various time frames such as 7 days, 14 days, etc.
5. Understand Business Impact: Discuss the opportunity cost resulting from these potential downtimes or data losses and what effect they have on the business.

Gaining knowledge at this stage is critical for the success of the plan. It is important to meet with all departments, stakeholders, management, IT, relevant teams and associates to effectively identify and obtain access to the corresponding tools and systems. At this time, review vulnerability management reports and conduct threat intelligence research pertaining to the client's industry and the threats targeting them. Also, analyze all past security incident reports and how they were processed as well as review vendor management processes and identify any third-party risks.

Effectively performing these tasks and gathering the data will allow the current security environment to come to light for your respective client.

Understand (Days 0 – 45)

This is the step that helps you clearly see the client's security position, identify potential risks, and determine the necessary precautions and measures to eradicate them. Once you have identified the client's current security status, the findings from the risk assessment can help determine the appropriate security needs.

It's recommended that this procedure includes a formal gap analysis to emphasize the differences between the current status and the security position. You should also utilize established cybersecurity frameworks like NIST to gauge the organization's security measures against industry regulations.

Your findings should be presented from three points of view:

- Risk Without Services: Display the client's risk levels without any security procedures.
- Risk With Basic Services: Demonstrate how basic security services reduce risk.
- Customized Risk Mitigation: Provide the client with a customized plan created for them to achieve a desirable level of security while outlining steps to further reduce risk.

Prioritize (Days 15 – 60)

In this step, use a framework that prioritizes the most critical security issues above all, ensuring the client's most vulnerable areas are promptly taken care of. Identify the SMART goals (specific, measurable, achievable, relevant, and time) for the organization and create a detailed plan that specifies the necessary steps, timelines, responsible parties, and expected outcomes along with documenting identified risks, probability, and impact on security and budget.

Key points to include:

a. **Immediate High-Impact Wins:** Direct the focus toward the top three actions to improve security immediately.
b. **Long-Term Improvement Plan:** To avoid overwhelming clients, you must create a year-long improvement plan highlighting any additional necessary actions.

Once the goals and long-term plan are completed, they should be shared with management, ensuring transparency from the top of the organization to the bottom.

Execute and Monitor (Days 30 – 80)

In this step, the overall goal is to execute your strategic plan as well as establish your vCISO credibility and set a standard for ongoing security management. You must earn stakeholder and management buy-in by explaining the strategic plan, its plans, and its overall impact on the organization. Once they acknowledge and back the plan, you must implement automated systems to handle everyday tasks such as automated password reset and report generation, accounting systems that require dual approval for money transfers and a state-of-the-art vCISO platform.

You must focus on impactful wins that can help build momentum and demonstrate early successes. You should regularly perform updates and policy refinements to ensure you have the knowledge and access to the latest security services provided. Setting a cadence for external scanning and reporting is also recommended to demonstrate improvement and risk reduction over time. By constantly reviewing the management and adjustments made for your remediation plans, you're ensuring the security remains effective and responsive.

Report (Days 45 – 100)

In the final phase of this plan, validate the strategy's effectiveness and ensure ongoing support from the board of directors and management as well as underline the importance of comprehensive reporting for MSPs and their respective clients. It is important to note that when delivering a report always start with the good news to build confidence and then address the areas that need improvement. Measure success by collecting and analyzing data that reflects the success of the completed plan such as reduced incident response times, a decrease in the number of phishing incidents or the security improvements and compliance postures.

Ensuring that security measures align with business needs and showing value to the board of directors is the ultimate goal when creating a continuous improvement cycle. Doing so will help MSPs position themselves not only as trusted advisors but also help develop strong and profitable client relationships.

vCISO services hold significant potential for expanding the capabilities of MSPs and MSSPs, enabling them to deliver CISO-level security expertise to organizations of all sizes. Offering vCISO services is well within reach for many MSPs and MSSPs; they just need to follow these key steps while leveraging the right tools to define and streamline the process effectively. This approach not only enhances their service portfolio but also meets the growing demand for comprehensive security solutions in today's digital landscape.

About the Author

David Primor, Co-Founder and CEO of Cynomi. He is a Lt. Colonel (ret) in IDF unit 8200, and previously technology director of Israel's cyber authority, David spent decades dealing with state-level cyber threats. David leads the Cynomi team and runs the occasional marathon in his free time. David holds a BSc. In electrical engineering from the Technion, Israel and completed his PhD at CERN.

David can be reached online at https://www.linkedin.com/in/david-primor-b2165582/ and our company website https://cynomi.com.

From Door Locks to Data Locks - How Securing Your Health Info is Like Home Security

By Jim Ducharme, Chief Technology Officer, ClearDATA

Healthcare organizations are increasingly moving Protected Health Information (PHI) to the cloud. This shift brings significant benefits in terms of efficiency and accessibility, but it also introduces new challenges in ensuring the security of sensitive data. As more healthcare companies, including payers, providers, and health tech firms, transition to cloud-based operations, they face mounting pressures to protect PHI from breaches and vulnerabilities.

To understand how to protect PHI in healthcare, let's look at an easy way to understand it and the parallels that exist between healthcare security and home security.

Understanding the Importance of PHI Security

The healthcare industry is a prime target for cyberattacks due to the valuable nature of Protected Health Information (PHI). Examples of recent cyberattacks include the Universal Health Services (UHS) Attack in 2020. UHS, a major healthcare provider in the US, experienced a ransomware attack that forced its systems offline, causing significant disruptions in patient care and hospital operations. The Anthem Inc. Data Breach nearly 10 years ago where hackers accessed the personal information of nearly 80 million Anthem customers, including names, birthdays, medical IDs, Social Security numbers, and addresses. This was one of the largest healthcare breaches in history. A more recent example is the Change Healthcare breach that happened back in Feb. of 2024 because of unauthorized access to their systems due to stolen or compromised credentials.

These examples underscore the critical need for robust cybersecurity measures in the healthcare sector to protect sensitive patient information and ensure the continuity of essential medical services. And these kinds of breaches can lead to severe regulatory penalties, reputational damage, and operational disruptions.

For these reasons (and many more) healthcare organizations must adopt a comprehensive approach to security. This involves understanding where PHI resides, implementing robust access controls, continuously monitoring security measures, and adapting to changes in the digital landscape.

The Home Security Analogy

To grasp the complexities of healthcare security, let's draw an analogy to securing a home. Just as homeowners take steps to protect their valuables, healthcare organizations must implement similar measures to safeguard PHI in the cloud.

1. **Know Where Your Valuables Are**

In a home, you wouldn't leave your passports, wills, and heirlooms scattered around. Instead, you'd designate a secure place, like a safe, to store these important items. Similarly, healthcare organizations need to know where their PHI is stored in the cloud. Identifying the locations of sensitive data is the first step in protecting it. This involves mapping out where PHI resides across various systems and ensuring that it is stored in secure, designated areas.

2. **Implement Access Controls**

Once you've identified where your valuables are, the next step is to control access to them. In a home, this means having strong locks on doors and windows. For healthcare organizations, this translates to implementing robust access controls for PHI. Access control measures determine who can access sensitive data, under what conditions, and what actions they can perform. This includes using strong authentication methods, such as multi-factor authentication, to verify the identities of users accessing PHI.

3. Continuous Monitoring: The Security Cameras of the Digital World

In a home, security cameras provide real-time monitoring of activities, alerting homeowners to suspicious behavior. In the digital realm, continuous monitoring plays a similar role. Healthcare organizations need to continuously monitor their systems for signs of unauthorized access or unusual activities. This involves logging access events, analyzing patterns, and detecting anomalies that could indicate a security breach. Continuous monitoring ensures that any suspicious activity is promptly identified and addressed.

4. Adapt to Changes: Handling the Unexpected

Homes are dynamic environments where changes occur regularly, such as new family members moving in or renovations taking place. Similarly, healthcare organizations must adapt to changes in their digital environments. This includes managing changes in personnel, applications, and infrastructure. For instance, when new employees join, their access to PHI must be carefully managed, and when they leave, their access should be promptly revoked. Regular reviews of access controls and permissions help ensure that only authorized individuals have access to sensitive data.

5. Protecting Against Broken and Unlocked Windows

Just as burglars constantly devise new methods to break into homes, such as searching for broken or unlocked windows, cyber attackers continuously evolve their tactics to breach healthcare systems. Healthcare organizations must stay informed about emerging threats and adapt their security measures accordingly. This involves leveraging threat intelligence to understand the latest attack vectors and vulnerabilities. By staying ahead of cyber attackers, healthcare organizations can proactively strengthen their defenses.

Several high-profile breaches in the healthcare industry highlight the importance of robust security measures. For example, in 2020, a ransomware attack on a major healthcare provider resulted in the compromise of over 300,000 patient records. This incident underscores the need for comprehensive security strategies that encompass prevention, detection, and response.

In addition, according to a recent report by the Ponemon Institute, the average cost of a healthcare data breach is $9.42 million, the highest of any industry. This staggering figure reflects the severe consequences of inadequate security measures. Furthermore, the report found that 44% of healthcare breaches were caused by malicious attacks, emphasizing the need for proactive defense mechanisms.

To enhance security and protect PHI, healthcare organizations can follow these practical steps based on home security - and make sure you are implementing these simple steps that are best practices.

Identify and Classify PHI: Conduct a thorough assessment to identify where PHI resides and classify it based on its sensitivity. This helps prioritize security efforts and allocate resources effectively.

Implement Strong Access Controls: Use multi-factor authentication and role-based access controls to limit access to PHI. Regularly review and update access permissions to ensure they align with current roles and responsibilities.

Continuous Monitoring and Incident Response: Deploy advanced monitoring tools to detect and respond to suspicious activities in real-time. Develop a robust incident response plan to mitigate the impact of potential breaches.

Regular Security Risk Assessments: Conduct regular security assessments by leveraging CSPM technology that gives visibility into the compliance and security posture of your cloud environments and helps to prioritize and remediate risks present in your environment.

Employee Training and Awareness: Educate employees about security best practices and the importance of protecting PHI. Regular training sessions can help build a security-conscious culture within the organization.

Leverage Threat Intelligence: Stay informed about the latest threats and vulnerabilities by leveraging threat intelligence feeds. Use this information to proactively strengthen security measures and stay ahead of cyber attackers.

Protecting PHI in the cloud requires a multifaceted approach that parallels the strategies used to secure a home. By knowing where PHI resides, implementing robust access controls, continuously monitoring security measures, adapting to changes, and staying informed about emerging threats, healthcare organizations can effectively safeguard their sensitive data.

Healthcare organizations must prioritize security to protect patient data and maintain trust. By adopting a proactive and comprehensive security strategy, they can navigate the complexities of cloud-based operations and safeguard their most valuable assets—just as they would protect their homes and the valuables within them.

About the Author

Jim leads ClearDATA's Engineering, Product Management, and IT teams. He has more than 25 years leading product organizations in the identity, integrated risk, and fraud management markets. Prior to joining ClearDATA, Jim served as Chief Operating Officer of Outseer, an RSA Company, where he served over 10 years in executive leadership roles. Prior to RSA in 2012, he served in executive leadership roles for Aveksa, CA and Netegrity. Ducharme frequently speaks at industry events and regularly contributes articles to trade publications.

Jim also holds several patents and a Bachelor of Science in Computer Science degree from the University of New Hampshire. He and his wife live in Maine in their dream log home, which was featured in Log and Timber Home Living magazine.

Jim can be reached online at https://www.linkedin.com/in/jimducharme/ and at our company website http://www.cleardata.com.

The Foundation of Data Security: Why Data Discovery Is the Critical First Step

Understanding the Pivotal Role of Data Discovery in Building Robust Security Strategies

By Missi Carmen, Chief Marketing Officer, Spirion

In the complex world of cybersecurity, one fundamental truth remains constant: you can't protect what you don't know exists. This is why data discovery stands as the cornerstone of any effective data security strategy. For Chief Information Security Officers (CISOs) and security professionals, understanding the critical importance of comprehensive data discovery can mean the difference between a robust, responsive security posture and a vulnerable one.

Data discovery is not just a preliminary step; it's the foundation upon which all other security measures are built. Here's why data discovery should be at the forefront of every security professional's mind:

1. **Comprehensive Risk Assessment**

Without knowing what data exists, where it resides, and who has access to it, it's impossible to accurately assess risk. Comprehensive data discovery provides a complete picture of an organization's data landscape, allowing security teams to identify vulnerabilities and prioritize security efforts effectively.

2. **Regulatory Compliance**

With regulations like GDPR, CCPA, and HIPAA imposing strict requirements on data handling, knowing exactly what data you have is crucial. Robust discovery capabilities ensure that organizations can quickly locate and categorize sensitive information, making compliance efforts more manageable and effective.

3. **Incident Response Preparedness**

In the event of a security breach, rapid response is critical. Comprehensive data discovery enables organizations to quickly identify what data may have been compromised, facilitating faster and more effective incident response.

4. **Resource Optimization**

By understanding where sensitive data resides, security teams can allocate resources more efficiently, focusing efforts on protecting the most critical assets rather than applying a one-size-fits-all approach.

5. **Data Minimization**

Effective data discovery allows organizations to identify and eliminate unnecessary data, reducing the attack surface and simplifying data management.

Key Aspects of Effective Data Discovery

To truly leverage the power of data discovery, organizations should focus on several key aspects:

1. Automated Scanning: Utilizing advanced algorithms to automatically scan and identify sensitive data across an organization's entire infrastructure, from on-premises systems to cloud storage.
2. Deep Content Inspection: Looking beyond file names or metadata to dive deep into the content of files, identifying sensitive information that might otherwise be overlooked.
3. Broad Data Coverage: Identifying all types of sensitive data, from personally identifiable information (PII) to intellectual property, across structured and unstructured data sources.
4. Real-time Discovery: Monitoring for new or changed data in real-time, ensuring that newly created or modified sensitive information is quickly identified and protected.
5. Scalability: Ensuring that discovery capabilities can scale to meet the needs of organizations of all sizes, handling large volumes of data efficiently.

Implementing Effective Data Discovery: Best Practices

To leverage the full power of data discovery, security professionals should consider the following best practices:

1. Establish a comprehensive data inventory as a baseline for your security strategy.
2. Implement continuous discovery processes to keep up with dynamic data environments.
3. Integrate discovery results with other security tools and processes for a holistic approach.

4. Use discovery insights to inform data governance policies and procedures.
5. Regularly audit and update discovery processes to ensure they remain effective as your data landscape evolves.

In today's data-driven world, the importance of robust data discovery cannot be overstated. It's not just about finding sensitive information; it's about gaining a deep understanding of your data ecosystem to inform every aspect of your security strategy.

By starting with a solid foundation of comprehensive data discovery, organizations can not only enhance their security posture but also position themselves to more effectively meet the data protection challenges of today and tomorrow. As we continue to navigate an increasingly complex digital landscape, data discovery will remain a critical tool in the cybersecurity arsenal, enabling organizations to stay one step ahead of potential threats and maintain the trust of their customers, stakeholders, and the broader community.

About the Author

Missi Carmen is Spirion's Chief Marketing Officer with over two decades of experience driving growth in B2B SaaS and enterprise organizations like ion interactive, OPSWAT, and M&T Bank, as well as BPO giants like Concentrix and Foundever. Specializing in demand generation, MarTech, and revenue operations, Missi is passionate about making marketing smarter, more agile, and efficient while supporting Spirion's mission to protect sensitive data. She holds an MS in Information Technology: E-Commerce from UMGC and a BS in Marketing Communications from the University of Baltimore. Missi resides in Boca Raton with her husband, daughter, and two dogs. Missi can be reached online at https://www.linkedin.com/in/missicarmen/ and at our company website https://www.spirion.com/contact.

A Step-by-Step Guide to the NIST Risk Management Framework (RMF): Simplifying Risk Management for Small Enterprises

By Zoe Lindsey, Security Strategist at Blumira

As the decade nears its halfway mark, ransomware attacks continue to dominate headlines across newspapers and website homepages. The relentless uptick in attacks shows no signs of slowing down, and small and mid-sized businesses (SMBs) are increasingly finding themselves in the crosshairs.

Thankfully, there's a silver lining: the National Institute of Standards and Technology (NIST) and its risk management framework (RMF). Growing businesses can reference this RMF to arm themselves with practical strategies to fend off attackers.

Let's dive into why ransomware actors are doubling back on mid-market companies and break down the key takeaways from NIST's latest guidance.

A Change in The Tide

Small enterprises have always been prime targets for ransomware, but their share of the pie decreased in recent years as cybercriminals set their sights on bigger, juicier targets—think massive enterprises like manufacturers and healthcare providers. These were high-stakes heists, requiring coordinated efforts and serious investment from the attackers, but the potential payout was worth the investment.

Instead of the typical shotgun approach, hackers started performing surgical strikes on high-value targets, often using double extortion tactics (or as the clever folks at Verizon's DBIR call it, "ranstortion"). Here, the attackers encrypt the data, exfiltrate it and then demand a second ransom to avoid leaking sensitive information.

But times are changing. SMBs are now making up nearly 80% of all ransomware targets as of the first half of 2023, a trend that has only solidified since. So, what's driving this shift?

First off, law enforcement is cracking down on big organized attack forces, scattering their members and pushing many of them to go solo. Second, the rise of affordable ransomware-as-a-service (RaaS) toolkits is making it easier than ever for these lone wolves to launch attacks. These tools, designed for ease of use and automation, enable even low-skill attackers to launch a high volume of attacks, focusing on smaller businesses that can't afford the same defense level as larger enterprises. Smaller payouts are just fine for solo operators because they don't have to split the take.

With a new wave of cyber skiddies on the loose, how can IT admins at SMBs protect their turf?

NIST to the Rescue: An RMF for SMBs

Services in the security market flood the industry, often seeming out of reach for SMBs with tight budgets. Recognizing this gap, NIST stepped in with a structured, systematic approach tailored for smaller organizations. NIST recently published a quick start guide to its RMF called SP 1314. While the full RMF can feel overwhelming, this new guide offers nine pages of actionable tips, along with resources for individuals interested in digging deeper.

Unlike compliance standards that pile on requirements, NIST's RMF is all about creating a repeatable cycle for framing, assessing, responding to and monitoring risk, making it adaptable to any organization, no matter the size or industry.

Here's a brief breakdown of the seven steps NIST recommends:

1. **Prepare:** The first step is to lay the groundwork for your risk management activities. This step involves designating a project leader and identifying the assets that are most valuable to your business—such as customer data, financial information or intellectual property. You'll also need to determine what expertise is necessary to make informed decisions throughout the process. This preparation ensures that your efforts are focused and that you have the right resources in place from the start.
2. **Categorize:** Once you've identified your key assets, categorize them based on their importance to your business operations. This process helps prioritize your security efforts, ensuring that the

most critical systems and data receive the most attention. For example, you might focus first on protecting your customer database, then move on to less critical systems. This step is crucial for efficient resource allocation, especially in organizations with limited budgets.

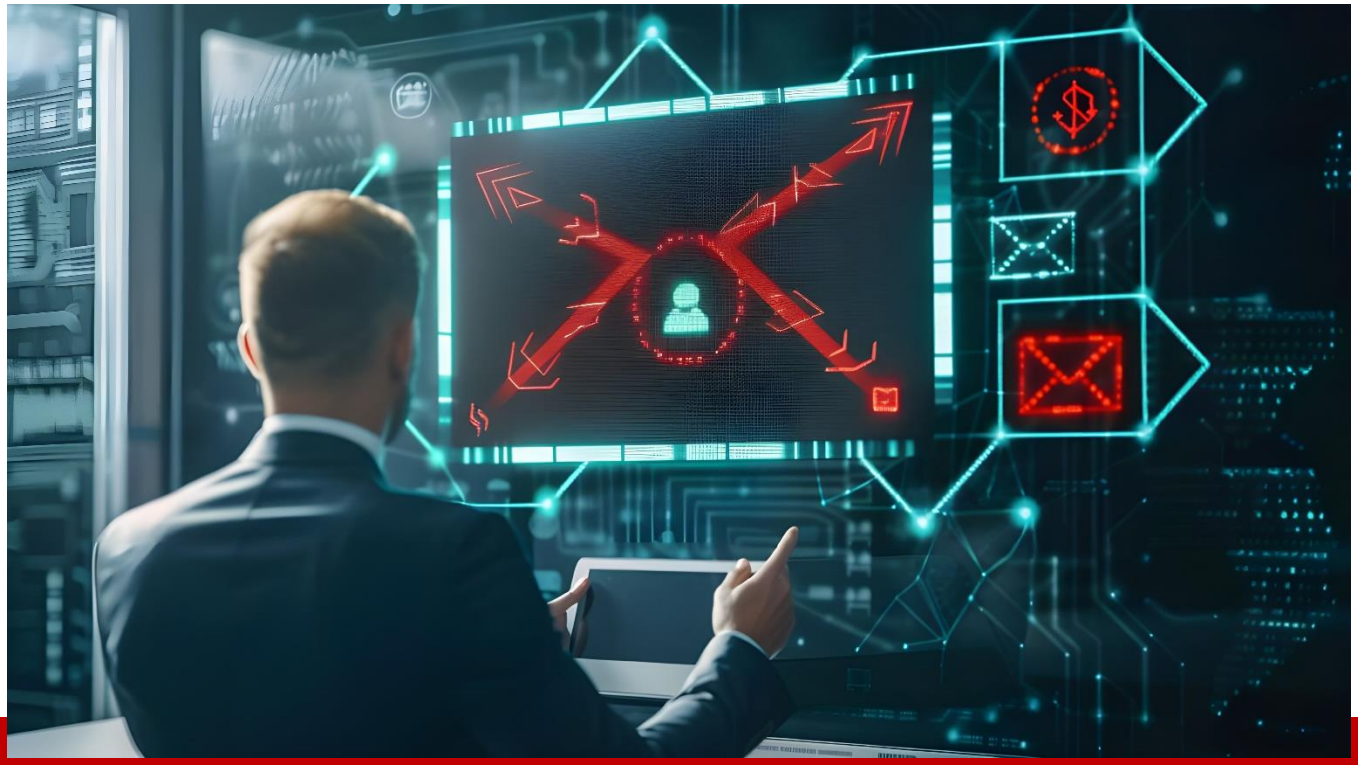
3. **Select:** After categorizing your assets, compare them against NIST's recommended security controls (detailed in NIST SP 800-53) to choose the ones that best fit your organization's needs and budget. This process isn't about applying every control available; it's about selecting the ones that provide the best protection for your most valuable assets. You can achieve more effective security without overspending by tailoring your controls to your specific risk profile.
4. **Implement:** Implementation involves putting the selected controls into practice, which might include installing security software, training employees on new procedures or updating business processes. The key here is to start somewhere, even if it's small, and build on that foundation over time. NIST's RMF acknowledges that perfection isn't necessary out of the gate—what matters is making progress and continually improving.
5. **Assess:** Regular assessment is necessary to ensure that the controls you've established are working as intended. This step involves checking your controls against the metrics of success you established earlier. Simple tools like checklists can be incredibly effective in identifying gaps or areas that need adjustment. The assessment process also provides valuable insights that inform the next cycle of risk management activities.
6. **Authorize:** Once you've assessed the effectiveness of your controls, the next step is to formally authorize them. This step involves defining a clear chain of command for decision-making, ensuring that everyone understands who has the final say on whether a system is adequately protected. Authorization provides accountability and helps streamline decision-making, especially in high-pressure situations requiring quick action.
7. **Monitor:** The final step in the RMF is ongoing monitoring. This process involves continuously keeping an eye on your security posture, watching for new threats and tracking any changes in your business that might affect your risk profile. Regularly update leadership on your security status to maintain awareness and readiness. Identify new risks and re-enter the RMF cycle to address them, ensuring your security strategy remains effective over time.

Remember: These steps aren't a one-time deal—they're part of an ongoing cycle of improvement. Every time you go through the process, you strengthen your defenses.

Implementing a formal risk management strategy might seem daunting, but NIST's guide is a great place to start. It's all about making security more accessible, no matter the size of your business. Remind yourself that perfection isn't the goal—progress is. Each iteration of the cycle enhances your defenses and ensures your security plan continuously evolves.

About the Author

Zoe Lindsey is a Security Strategist at Blumira with over a decade of experience in Information Security. She began her infosec career at Duo Security in 2012 with a background in medical and cellular technology. Throughout her career, Zoe has advised organizations of all sizes on strong security tactics and strategies. As a sought-after speaker, she has shared best practices and recommendations at industry-leading events including RSA Conference, SecureWorld, and Cisco Live.



Cybersecurity's Broken Model: The Cost of Overcomplication and Underperformance

The cybersecurity industry's reliance on rigid, complex solutions is wasting budgets and increasing security risks

By Guy Flechter, CEO and Founder of Sola Security

Cybersecurity is in need of a reckoning.

Global cybersecurity spend reached a record $79.2 billion in 2023 and is expected to grow by almost 10% this year – a reflection of the evolving, and increasingly nefarious threats in our hyper-digital world. On paper, that's a good thing. More investment should mean better protection, right?

Yes, it should.

But, despite the rise in spending, in the first half of 2024 alone there was still a 14% increase in reports of compromised data compared to the same period last year, impacting around 1.07 billion victims.

When increased investment fails to improve security outcomes, the conclusion can only be that there are fundamental flaws in how we approach cybersecurity. These failures are the result of an industry that has over-complicated its solutions. Companies today either employ a multitude of rigid, decentralized, independently managed tools, each serving a too-narrow function, or opt for purposely "all-

encompassing" solutions that are costly, and too broad to address specific organizational needs. Choosing the lesser of two evils means that evil wins either way.

Two things are now clear – detrimental cyberattacks will continue to proliferate, and traditional approaches to cybersecurity infrastructure are increasingly proving to be insufficient.

One-Trick Ponies

The "one-trick-ponies" are a common class of cybersecurity tools, each built for a niche application. They're treated like patches in a quilt — their purposed appeal is that organizations can adopt exactly the solution they need for any given vulnerability and piece together a cybersecurity posture that suits their needs perfectly.

It's convenient in theory, but truthfully, it's too good to be true.

To adequately address today's security threats, organizations are forced to deploy upwards of 50 independently managed systems just to stay secure. The average enterprise security toolset includes 60-80 distinct solutions, with some enterprises reaching as many as 140.

With the cybersecurity landscape rapidly growing and evolving, new tools must be constantly adopted and deployed just to keep up, which is why there's been a59% increase in cyber budgets year-over-year.

While each of these tools serves a distinct purpose, deploying a large stack of such tools is complex. As every tool is configured separately – each accompanied by its own dashboard and alert system – managing this type of security infrastructure becomes dangerously difficult and costly, requiring extensive manpower and expertise.

The lack of synergy between these tools also creates inefficiencies and increases the risk of misconfiguration. Each tool is managed independently, so settings may be incorrectly selected, misconfigured, or misaligned with other operating tools, leading to security gaps. On top of all this, teams are having to manually manage multiple security tools – each with its own system of notification and alerts – so responding to every incident becomes highly challenging, making it easy to overlook critical alerts and vulnerabilities.

Ultimately, a suite of individual tools only provides a partial view of an organization's security landscape, resulting in fragmented visibility and unnecessarily challenging conditions for security teams to construct a comprehensive understanding of their organization's defensive posture.

The "Panacea"

An alternative to the one-trick-ponies is the "cure-all solution" approach. Why patchwork together your own quilt when you could just buy a full-coverage blanket?

Indeed, these solutions are designed to offer a broad range of features across various aspects of cybersecurity, all in one neat package, promising to streamline security management by consolidating it into a single platform.

While they somewhat alleviate the issue of complexity, sometimes they can be overwhelming, like a huge, heavy-duty duvet when all you need is a light throw. Additionally, because of all of the extra material included, the cost of all-in-one services can be significantly higher than targeted solutions, and they come with their own set of limitations.

Comprehensive packages often bundle solutions that might not actually be relevant to the needs of a specific organization. Companies will purchase these packages anyway because they include tools that the organization's current security posture requires – but they also end up paying a hefty price for features they don't actually need.

These packages are also designed to serve a broad range of industries, meaning they aren't optimized for the unique needs of an organization in a particular sector. These solutions tend to be inflexible and continue to be so as organizations evolve and their security needs change, limiting the effectiveness of the solution as new vulnerabilities emerge.

Tailored Tools

The cybersecurity landscape is evolving at a frightening pace, and with an ever-widening array of threats, the ideal solution should combine the benefits of the two approaches above, without being bogged down by the setbacks.

The preeminent solution is a "tailored tools" approach – it supports a highly customizable suite of tools, while remaining centralized and comprehensive enough to cover any gaps. These cybersecurity solutions are designed for flexibility – security teams can pick and choose exactly what they need to address the unique challenges and vulnerabilities of their organization. This way, companies only pay for the solutions they need, resulting in a more affordable and organizationally relevant security posture. A small business, for example, could adopt a tailored package that doesn't include unnecessary or complex features that are only relevant for large enterprises.

Like cure-all tools, tailored solutions also provide integrated dashboards, allowing organizations to manage their entire security posture from a single platform. Yet, unlike an all-in-one solution, these platforms aren't cluttered with irrelevant functionalities or alerts. Rather, tailored solutions are configured specifically to focus on the most relevant threats, resulting in faster response times and fewer gaps. This approach also allows for data consolidation from each solution to provide more holistic visibility for streamlined communication and data-informed decision-making – both of which are difficult to achieve in the current cybersecurity landscape.

New solutions for a changing world

In a world where hackers run rampant, empowered by new technology and increasingly complex digital networks to exploit, spending on comprehensive cybersecurity could be the most important investment an organization makes. But traditional approaches to cybersecurity continue to prove inadequate, and the cybersecurity industry is reaching the point of desperation to evolve beyond its reliance on rigid or siloed solutions.

A tailored solution approach not only addresses the limitations of existing models, but will pave the way for a more effective, efficient, and agile method of defense against the widening threat landscape. By optimizing cybersecurity spend, companies can invest more time and money into growing their business without compromising on security. It's a win-win proposition for organizations of any kind and size.

About the Author

Guy Flechter is the CEO and Founder of Sola Security. His passion for innovation and disruption of the Security industry led him to co-found Cider Security, which was acquired by Palo Alto Networks in 2022. His career in the industry spans over 20 years, with key roles at AppsFlyer, LivePerson, and Palo Alto Networks.

Integrating AI into Network Security for Improved Threat Detection

By Kelsey Livesey, Zero to Mastery

Have you ever wondered how your digital security can keep up with the lightning-fast evolution of cyber threats? The world of cybersecurity is changing faster than ever, driven by relentless cybercriminals and increasingly complex digital environments. From sneaky polymorphic malware to clever zero-day exploits and sophisticated AI-generated phishing schemes, the threats are not just multiplying—they're evolving to sidestep traditional defenses. That's where AI comes in, offering you a secret weapon that far surpasses old-school methods. Imagine having a guard that never sleeps, one that learns and adapts, constantly on the lookout for danger, and preemptively counteracting potential threats before they can do harm.

That's where artificial intelligence (AI) steps in, offering you a secret weapon that far surpasses old-school methods. Imagine having a guard that never sleeps, one that learns and adapts, constantly on the lookout for danger, and preemptively counteracting potential threats before they can do harm. This isn't just any guard—it's an AI-driven system that transforms your network security from reactive to proactive.

In this guide, we'll dive deep into how integrating AI into your network security isn't just a nice-to-have, it's a must-have to stay ahead. I'll walk you through each step, explaining why AI could be your best ally in this ongoing battle and how you can leverage it to fortify your defenses.

Ready to make your network security smarter, faster, and more resilient?

Let's get started!

Navigating the Shifting Sands of Cybersecurity

As you sit back and manage your daily tasks, behind the scenes, the cybersecurity landscape is shifting dramatically. Think about it: cybercriminals never rest. They're innovating and scheming around the clock, and as our digital spaces grow more complex, the methods they use grow more cunning.

Have you heard of polymorphic malware or zero-day exploits? These aren't just buzzwords—they are real threats that adapt and evolve to bypass what used to be robust defenses. With the rise of such sophisticated attacks, the global cost of cybercrime is predicted to reach $10.5 trillion annually by 2025, up from $3 trillion in 2015 .

Why does this matter to you?

Because every evolution in attack strategies directly challenges your current security measures. AI steps onto this ever-changing battlefield as a pivotal ally. Unlike traditional security systems that wait to be hit, AI-driven security is like having a sharp-eyed sentinel that's always on guard. It sifts through oceans of data in real time, spotting threats that humans or conventional systems might miss. Whether it's a bizarre pattern in network traffic or a subtle anomaly in user behavior, AI is on it, learning and adapting as it goes. This proactive approach in network security ensures that you are always one step ahead of potential threats.

By 2025, it's expected that there will be about 30.9 billion IoT devices worldwide, making them an essential part of both business operations and our daily lives. With this rapid growth, it's crucial to implement strong security measures to prevent potential breaches and disruptions. Keeping these devices secure will be more important than ever. Properly managing and securing these devices is essential to prevent security breaches, operational disruptions, and financial losses. With the rise of Internet of Things (IoT) devices, cloud computing, and mobile technologies, your network's boundaries have blurred. More endpoints mean more vulnerabilities.

Here's where AI isn't just useful; it's indispensable. By processing and analyzing data from diverse sources, AI offers you a panoramic view of potential threats, allowing you to secure these new fronts with confidence.

As we explore the critical role of AI in network security, it's clear that AI's capabilities extend far beyond traditional methods. Let's dive deeper and uncover how AI not only keeps pace with cybercriminals but

actually stays one step ahead, preparing your defenses against attacks you didn't even know were possible.

Why AI is Essential in Network Security

In today's world, where cyber threats are evolving at an unprecedented pace, traditional security systems, which operate on predefined rules and signatures, often fall short. These systems react to known threats but struggle against new, sophisticated attacks that emerge daily. This is where AI steps in, revolutionizing network security with its proactive and predictive capabilities.

Proactive and Predictive Approach

AI functions as a tireless security analyst, constantly scanning data to detect patterns and anomalies indicative of potential threats. Unlike traditional systems, AI anticipates problems by leveraging machine learning to analyze vast datasets, learning from each interaction to get smarter over time. This proactive stance means potential threats are addressed before they escalate into crises.

Enhanced Detection Capabilities

With AI, your network enjoys round-the-clock monitoring. AI learns normal behaviors within the network and swiftly identifies deviations, catching both known and emerging threats. This advanced threat detection is akin to spotting a needle in a haystack, enabling rapid responses to potential issues.

Automation of Routine Tasks

AI also excels at automating mundane tasks such as monitoring network traffic, applying security updates, and scanning for vulnerabilities. By handling these routine processes, AI frees up your security team to focus on more complex challenges, which often require human intervention. This automation not only enhances operational efficiency but also ensures consistency in task execution.

Adaptability and Continuous Learning

As cyber threats evolve, so does AI. It continuously refines its algorithms with each new piece of data, ensuring your defenses remain up-to-date. This adaptability means AI can scale with your organization, expanding its capabilities as your needs grow.

Transforming Network Security Operations

AI's integration into network security operations brings numerous benefits. Firstly, it accelerates detection and response times, cutting through data noise to quickly pinpoint anomalies. This swift action drastically reduces the window for potential attacks.

Secondly, AI's superior analytical abilities enable it to sift through massive amounts of data, providing deep insights that are hard to achieve manually. It examines network logs, user behaviors, and external threat intelligence to offer a comprehensive security overview.

Proactive Security Posture

AI's predictive analytics help shift your security posture from reactive to proactive. By analyzing patterns over time, AI anticipates potential breaches, allowing you to fortify defenses preemptively. This proactive approach not only blocks attacks but also prepares for them in advance.

Continuous Improvement and Scalability

The best part about AI is its continuous improvement. Each new data point refines its understanding, making your security measures smarter day by day. Furthermore, AI's scalability ensures that as your organization grows, your security capabilities grow with it, tailored to your evolving needs.

Navigating the Challenges of AI in Network Security

As transformative as AI is for network security, its implementation comes with its own set of challenges. Understanding these hurdles is essential for leveraging AI effectively and responsibly in your security strategies.

Privacy Concerns

First up, privacy. AI requires access to vast amounts of data to function, which often includes sensitive information. It's crucial to ensure that this data is handled securely and in compliance with regulations like GDPR or CCPA. Employing techniques like data anonymization can help protect individual privacy while still allowing AI to perform its analyses.

Transparency and Complexity

Then there's the issue of transparency—or the "black box" problem. AI systems can be complex, and it can be tough to understand how they arrive at certain decisions. This lack of clarity can be a real

headache when you need to troubleshoot or adjust these systems. Using explainable AI (XAI) techniques can help demystify the processes, making it easier for your team to trust and manage the AI tools.

The Skills Gap

Another challenge is the skills gap. AI in network security requires a blend of expertise in both cybersecurity and machine learning—skills that aren't always available in-house. Bridging this gap might mean investing in training for your current team or bringing in new talent that can navigate the complexities of AI-driven security.

IBM's Cost of a Data Breach Report 2023 highlights that human error remains a primary factor in 95% of all breaches. AI can mitigate this by automating routine security tasks and providing real-time threat intelligence.

Ethical Considerations

Ethics also play a significant role. There's a risk that AI systems might develop biases, which can lead to unfair or ineffective security practices. Regular audits, using diverse training datasets, and implementing bias detection mechanisms are essential steps in ensuring your AI systems act fairly and effectively.

Integration Efforts

Integrating AI with your existing security infrastructure also presents significant challenges. This process requires careful planning and phased implementation. Initiating with pilot projects can offer valuable insights into AI's impact and help refine your approach before rolling it out on a larger scale. It's crucial to ensure that AI systems work harmoniously with your existing tools, maintaining smooth operations and optimal security.

Looking Ahead…

Navigating these challenges requires a thoughtful approach, but the benefits of AI in enhancing your network security are undeniable. As you consider integrating AI, these considerations will help you maximize its advantages while minimizing potential downsides.

Secure Your Future with AI-Driven Network Security

So, integrating AI into network security isn't just a fancy idea—it's a game-changer in today's crazy fast-paced cyber world. AI takes threat detection to the next level, giving you a proactive and predictive edge that old-school methods just can't match. It's like having a tireless watchdog that keeps learning and adapting, keeping your network safe 24/7.

Sure, there are some bumps on the road to AI integration, like privacy concerns, transparency issues, and the skills gap. But the payoff is huge. With AI, you're not just keeping up with cyber threats; you're staying ahead and protecting your organization's future. Don't wait for the next cyber attack to show you the weak spots. Dive into AI now and turn your network security into a smart, adaptive shield.

What do you think about bringing AI into your network security?

About the Author

Kelsey Livesey is a creator at Zero to Mastery, a company passionate about empowering individuals through high-quality tech education. Kelsey is dedicated to creating engaging content that informs and inspires learners on their journey to mastering new skills.

X: @zerotomasteryio

Website: https://zerotomastery.io/

LinkedIn: www.linkedin.com/in/kelsey-livesey

Binary Cryptology with the Internet of Things Communication

By Milica D. Djekic

The home and office-based internet is a quite cheap resource that is everything, but not reliable and trusted as it is possible conducting a cyber-attack from anywhere and anytime, so far. Also, the other sorts of the wireless web information transfer such as mobile and satellite girds are with suitable pricing, but yet without any kind of the stable security. The greatest vulnerability of the web communication is it uses the IP addresses to establish some way of the packets exchange and that sort of the parameters are very easily trackable and matter of being exposed by a third party. In other words, in order to make a communication between two or more devices it is needed to go deep into data science which might explain how digital contents are manageable on rest, in motion or within storage.

On the other hand, the Internet of Things (IoT) is a web-driven asset that literally overwhelmed the marketplace with some advantages, but also with a plenty of the defense challenges seeking the next generation information exchange solutions or better protection of the ongoing technological and technical systems, so far. The current IoT ecosystem has a couple of billions of consumers over the globe and the tendency is that number will go up as time goes on. In addition, the online world is still convenient for the asymmetric warfare high-tech operations, so the IoT systems also being the web-based ones will definitely need to look for a stronger security at least or at most that concept will as many others before be sent to the history. The idea to invoke a binary encryption into the entire story could sound as applying a heavy arterially gun on a little bird which equally well can be killed using a stone gun, so far. In a case

of the IoT, even if the next step in its development and deployment could be making a shift from the web to GSM technologies, which are also a part of the cyber family, it is clear that nothing revolutionary new will be created and the technology will make only a new transformation causing everyone remaining in the magic cycle without any chance to get a road out.

The main advantage of the binary cryptosystems is they might be pretty inexpensive, but yet very functional which gives a space to the possible investors to provide some funds, grants and finances to those engineering projects as they could be resolved smoothly in the both – hardware and software fashion, so far. As a paradigm of the novel time, the IoT could be assured using such an approach which means the good security performances, as well as the good cost-effectiveness to those being the users of such products and services as the major remark with such projects could be their operability and optimization in a sense of the safety, security and potentially privacy that are the leading imperatives in the case of the IoT technology and its still quite well accessibility on the marketplace, as well as the entire communities, societies and international scales.

About The Author

Milica D. Djekic is an Independent Researcher from Subotica, the Republic of Serbia. She received her engineering background from the Faculty of Mechanical Engineering, University of Belgrade. She writes for some domestic and overseas presses and she is also the author of the books *"The Internet of Things: Concept, Applications and Security"* and *"The Insider's Threats: Operational, Tactical and Strategic Perspective"* being published in 2017 and 2021 respectively with the Lambert Academic Publishing. Milica is also a speaker with the BrightTALK expert's channel. She is the member of an ASIS International since 2017 and contributor to the Australian Cyber Security Magazine since 2018. Milica's research efforts are recognized with Computer Emergency Response Team for the European Union (CERT-EU), Censys Press, BU-CERT UK and EASA European Centre for Cybersecurity in Aviation (ECCSA). Her fields of interests are cyber defense, technology and business. Milica is a person with disability.

Can Your Security Measures Be Turned Against You?

The Intriguing Case of Windows SmartScreen Vulnerabilities

By Yonatan Keller, Analyst Team Lead, Zafran

Throughout history, the concept of defeating an opponent's defenses has been central to warfare strategies. From ancient sieges using tunnels and siege engines to modern tactics aimed at neutralizing air defenses before launching a major offensive, the principle remains the same: breach the defenses to open a path for attack. This strategy is just as relevant in the realm of cybersecurity, where attackers aim to compromise security systems themselves, turning protective mechanisms into pathways for initial access, lateral movement or defense evasion.

In cybersecurity, targeting security tools—especially those designed to protect networks and endpoints—is an increasingly used tactic. By exploiting flaws within these security controls, attackers can transform them into conduits for further attacks. Such a tactic offers significant advantages, including bypassing authentication processes, evading detection by security monitors, and escalating privileges to conduct

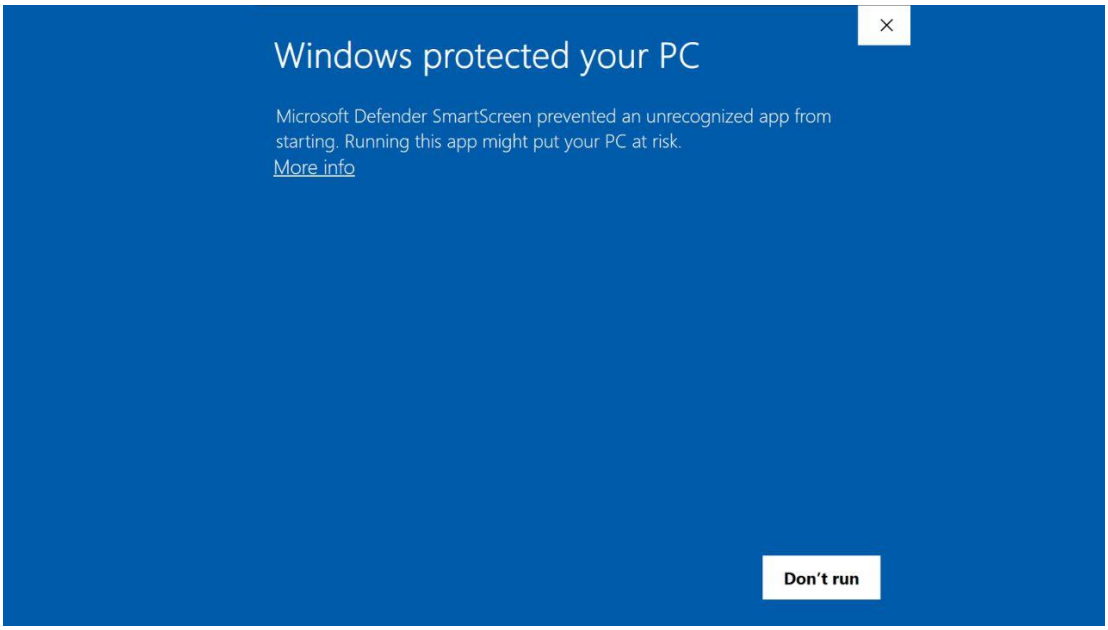
reconnaissance or move laterally within a network. Furthermore, security mechanisms often operate with elevated privileges and broad network access, making them attractive targets.

Over-reliance on certain security products might also allow attackers to extend their reach across various organizations. For example, the recent failure of CrowdStrike's endpoint detection and response (EDR) tool, which caused widespread global outages, highlights the risks associated with depending too heavily on a single security solution. Although this incident wasn't the result of a cyber attack, it clearly demonstrates the potential issues that can arise from such reliance.

For years, the cybersecurity community has been aware of the risks posed by vulnerabilities in security products. A notable example from 2015 involved a critical flaw in FireEye's email protection system, which allowed attackers to execute arbitrary commands and potentially take full control of the device. More recently, a vulnerability in Proofpoint's email security service was exploited in a phishing campaign that impersonated major corporations like IBM and Disney.

Windows SmartScreen is designed to shield users from malicious software, phishing attacks, and other online threats. Initially launched with Internet Explorer, SmartScreen has been a core part of Windows since version 8. It works by analyzing downloaded files and websites and comparing them against a constantly updated database of known threats. If a file or website appears suspicious, SmartScreen issues a warning before the user proceeds. This protection relies on URL filtering, application reputation, and cloud-based heuristics.

SmartScreen is officially a Microsoft Defender feature and configurable at scale through Microsoft Defender for Endpoint Manager. However, SmartScreen’s integration with the Microsoft Edge browser and other Windows components means it remains active even if Microsoft Defender is not the primary antivirus solution. However, since mid-2023, several vulnerabilities in SmartScreen have been exploited, undermining its ability to prevent attacks.



Since March 2023, at least seven SmartScreen vulnerabilities have been used in various attacks. These flaws have enabled attackers to bypass SmartScreen warnings, tricking users into downloading malicious files. These files have been used for a range of harmful activities, from establishing communication channels with attackers to cryptocurrency mining, information theft, and integrating systems into botnets.

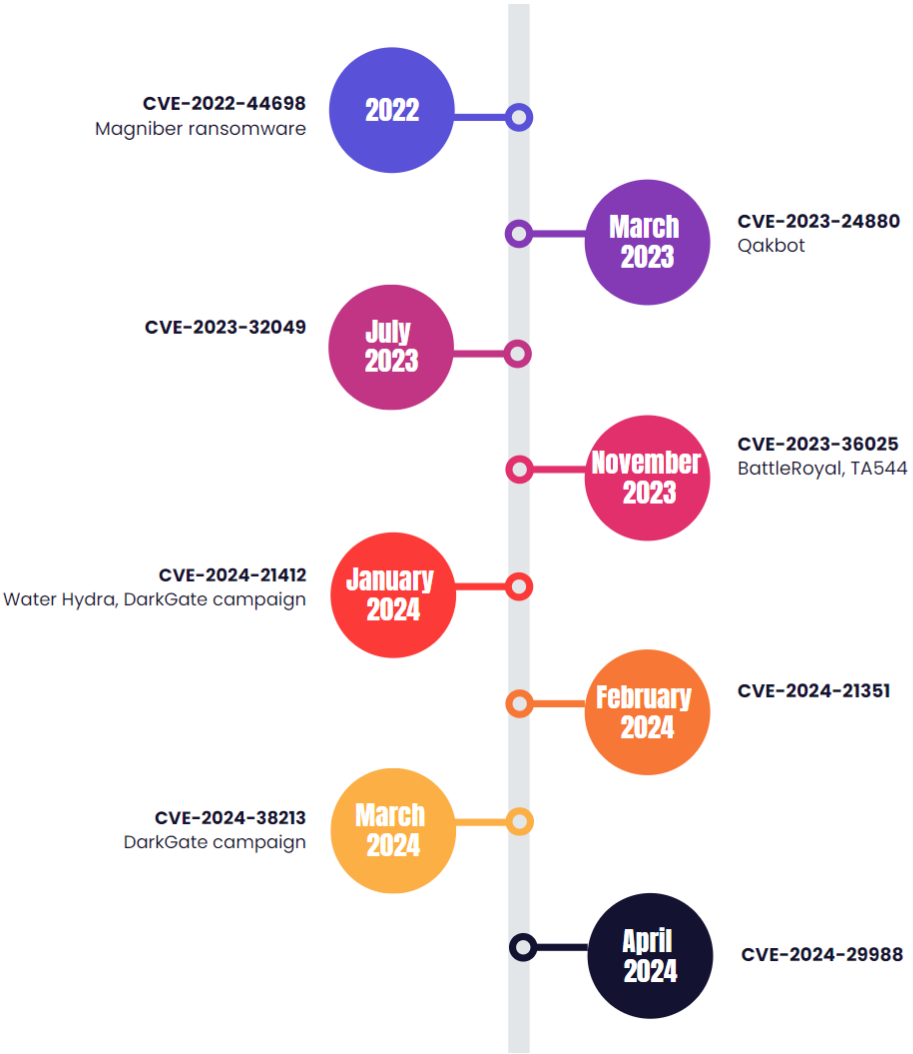


Photo Credit: Zafran

For instance, in March 2023, a vulnerability (CVE-2023-24880) was exploited by the Qakbot malware. This vulnerability, related to an earlier flaw (CVE-2022-44698), was initially used by the Magniber ransomware to target South Korea. The attack involved a specially crafted JavaScript file that bypassed SmartScreen's warning system. In July 2023, Microsoft patched another SmartScreen vulnerability (CVE-2023-32049) that was being exploited as a zero-day to bypass specific security features.

In November 2023, a critical vulnerability (CVE-2023-36025) was discovered, which had been exploited by both the emerging cybercrime group BattleRoyal and the APT group TA544, known for targeting organizations in Europe and Japan. These attackers hosted malicious URLs on legitimate cloud services, causing Windows to mistakenly identify them as safe. When users clicked on these links, SmartScreen failed to issue warnings, allowing the attackers to deliver a disguised ZIP file containing the Phemedrone malware, a sophisticated information-stealing tool.

By January 2024, another SmartScreen vulnerability (CVE-2024-21412) was exploited in a phishing campaign aimed at trading platforms, orchestrated by the Russian group Water Hydra. The situation escalated in March 2024 when the DarkGate malware, known for bypassing Kaspersky antivirus, widely exploited this vulnerability. Additional vulnerabilities, such as CVE-2024-21351 and CVE-2024-29988, have also been observed in the wild, further demonstrating the ongoing threat to Windows Defender's SmartScreen.

The ongoing exploitation of Windows SmartScreen vulnerabilities underscores a critical lesson: even the most trusted security controls can be compromised, turning protective measures into potential risks. This situation highlights the importance of continuous vigilance and prompt action to mitigate emerging threats.

To prevent such incidents, organizations should prioritize the detection and investigation of existing SmartScreen vulnerabilities to accurately assess their risk exposure. By thoroughly analyzing the tactics and techniques recently employed by threat actors, they can evaluate the effectiveness of their current security measures across all controls. Most importantly, an automated, comprehensive risk assessment that covers vulnerabilities, threat groups, and controls will empower organizations to strengthen their defenses swiftly and effectively at scale.

About the Author

Yonatan Keller leads the Analyst team for Zafran Security, an innovative threat exposure management company that integrates enterprise security tools to reveal, remediate, and mitigate the risk of exposures across entire infrastructures. Yonatan spent over two decades in the elite IDF intelligence corps and Cyber Defense Directorate, in which he managed a Cyber Threat Intelligence department.

20% of Organizations Have Experienced a Non-Human Identity Security Incident

By Alon Jackson, CEO & Co-Founder of Astrix Security

Today's business environment requires teams to do more — better than before, and at a faster rate. Thanks to third-party apps, no-code platforms, GenAI, and other forms of automation and integration, enterprises are able to achieve that, but not without a deeply-embedded reliance on the true building blocks of automation and integration — non-human identities (NHIs).

These NHIs (i.e. bots, API keys, service accounts, OAuth tokens) are critical to innovation and efficiency yet remain the biggest security blind spot, hence the recent headline-grabbing attacks like the ones on AWS, Microsoft, Cloudflare, and Okta, to name a few.

The growing frequency of attacks serves as a testament to the harsh reality that 1) hackers have taken notice of this shiny new opportunity, and 2) organizations are still ill-equipped to protect against NHI-related threats.

Knowing that the sheer volume of NHIs, which outnumber human identities by 20 to 1, already pose a significant challenge for security practitioners, we set out to explore the additional blockers and further understand where NHIs fall on the security priority list. The 800-person survey facilitated by the Cloud Security Alliance set a baseline for the current situation: 1 in 5 organizations have already experienced an NHI-related security incident.

Confidence gap in securing NHIs

Human identities are familiar territory at this point, yet only 25% of IT and security practitioners express "high confidence" in securing them, according to the report's findings. Naturally, the numbers are even more grim for securing non-human identities, with only 15% expressing "high confidence."

With 69% of organizations expressing moderate-to-high concern about NHIs as an attack vector, it emphasizes an awareness of the risks, but a challenge in addressing the risks head-on, due to a broad range of reasons.

Service accounts, permissions, offboarding – and more

The findings made the point evidently clear: the most challenging aspect of NHI security is managing service accounts, with 32% citing this as their top challenge. Additional pain points include auditing and monitoring (25%), access and privileges (25%), discovering NHIs (24%) and policy enforcement (21%).

The lack of visibility into third-party vendors and OAuth apps also presented a significant concern, with 38% of organizations reporting little-to-no visibility.

The findings show that the management of API keys is another critical area where organizations struggle. Only 20% have a formal process for offboarding and revoking API keys, and only 16% have a process for rotating or rolling back API keys. This lack of a formal process leaves API keys active and potentially exploitable.

Fragmented security approaches

NHIs present a unique challenge, requiring tools that address this specific subset of security. Currently, organizations are relying on a broad range of tools and solutions to secure NHIs — most often IAM (58%), PAM (54%) and API security (40%). These tools are either indirectly or non-comprehensively addressing the problem, leading to a fragmented approach that actually leads to more security incidents.

Future of NHI security

The report reveals that there's a growing recognition of the importance of investing in NHI security with 25% of organizations already investing and an additional 60% planning to within the next 12 months. By

giving non-human identities the same attention that we currently give to human identities, we as an industry can lay the foundation for a protected business environment that's future-proofed.

It's time to automate critical processes such as permission management and API key handling, as well as adopt a more targeted and unified approach to protecting NHIs.

About the Author

Alon Jackson is the CEO and Co-Founder of Astrix Security, a leading Non-Human Identity Security provider. Prior to founding Astrix, Jackson served in various strategic roles in the Cyber Security Division of the Israeli Military Intelligence Unit 8200, including leading the Cloud Security Division and serving as the Head of the Cyber Security R&D Department. His experience also spans the private sector, where he served as Head of the R&D Group at automotive cyber security company Argus (acquired by Continental AG). Jackson received an MSc in Computer Science with honors, specializing in cryptography. To learn more about Jackson and Astrix Security, visit https://astrix.security/.

Navigating the New Frontier: Strengthening Cybersecurity Through Next-Gen Identity & Access Governance

By Pankit Desai, Co-Founder and CEO, Sequretek

It can be difficult to fully appreciate just what has changed when it comes to cybersecurity – and by how much. Up until around two decades ago, the network was *the* definitive perimeter of cyber defense, the place where organizations set up the sentinels to protect their digital environments. A decade later, with laptops and desktops, the focus shifted to the endpoint as the security perimeter. The thinking was clear: secure the endpoint that accesses the network, and you have the digital environment secured.

In today's mobility-driven world, however, the endpoint has become quite fluid. Users, be they employees or end-users, are accessing a host of interconnected applications and services across multiple devices—from laptops and desktops to tablets, smartphones, and other IoT-driven gadgets and appliances. This holds truer in the post-pandemic era than it did before; businesses now have work-from-home access given to their employees through VPNs and cloud-based enterprise sandboxes. The device no longer matters –the user does.

The Emerging Threat Landscape: Why We Need to Rethink Security

Identity, as a result, has become the only constant in enterprise digital environments that shift, change, and evolve at an unprecedented pace. With the rise of cloud computing, remote work, and the Internet of Things (IoT), the attack surface for identity and access-based cyberattacks has also expanded dramatically.

Threat actors today are using increasingly sophisticated methods and Gen AI to exploit weaknesses in identity and access management, from phishing attacks and insider threats to social engineering. Why? Because identity *is* everything. If they gain access to even one set of user credentials, they can move laterally within the network to access sensitive data, compromise even more users, and cause significant damage. This is why next-generation identity & access governance (IAG) is a nice-to-have feature and an absolute cornerstone of modern cybersecurity strategies.

Next-Gen IAG Solutions: Where Innovation Meets Security

What makes next-gen IAG different? In a word: intelligence. New-age IAG solutions are smarter, more adaptable, and far more effective at helping organizations, especially those in critical sectors such as BFSI, to protect themselves against identity-based threats and vulnerabilities.

One of the most significant advancements in this space is the integration of artificial intelligence (AI) and machine learning (ML). These technologies allow IAG systems to continuously monitor and capture user behavior in an access data lake, which learns what normal activity looks like, analyzes it, and flags anything that deviates from the pattern. For instance, if an employee who typically logs in from one location suddenly tries to access the enterprise network from another, using identity binding, the system can automatically trigger the most relevant security protocols such as requiring additional verification or locking the account. Next-gen IAG also allows for more stringent and effective zero-trust protocols and frameworks to be implemented across the enterprise digital ecosystem (customers and partners included).

IAG complements enterprises by assessing and providing the entitled requirements for each user within the network. This ensures that each time a new user is created, all required details are passed onto the host application for ID creation. All new non-entitled requests must go through workflow-based approvals before access is granted. It also manages access across the user life cycle of Joiners, Movers, and Leavers (JML) through automated user access review and recertification (UAR). Presenting information on access provisioning, deprovisioning, and other identity administration on a centralized dashboard is required. This addresses major security issues such as stale and dormant access and allows the relevant stakeholders to view and manage their users and access levels in real-time from day 1 via a single dashboard.

Next-gen IAG also balances the need for security with usability and agility. The focus is on strengthening the governance of access and identity through additional layers to balance security with usability. For example, multifactor authentication (MFA) and single sign-on (SSO) provide a robust layer of additional security to complement typical measures such as only OTPs and ID/password-based logins, while being

easy to use. This ensures that the functionality, usability, and security remain unimpacted even if user login credentials are compromised, especially when accessing the network through a mobile device.

Integration Benefits: Why It's Worth the Investment

Implementing next-gen IAG solutions can require some upfront investment, but its benefits far outweigh its costs. When you consider the potential cost of a data breach—not just in terms of money, but in lost trust, damaged reputation, and legal consequences—investing in an IAG solution starts to look like a bargain. IBM Security's *Cost of a Data Breach Report (2024)* revealed that a single data breach within the financial sector could end up costing enterprises around $6.08 million on average. That a significant number of these breaches were identity-based—about 19% of all breaches committed by compromised or stolen credentials—only adds to the importance and criticality of investing in state-of-the-art IAG solutions.

But beyond just preventing breaches, next-gen IAG offers several operational benefits. For one, it significantly reduces the burden on IT teams. With automation handling many of the routine tasks associated with identity and access management, IT professionals can focus on more strategic work such as improving overall security posture or developing new initiatives. Automated systems also help reduce human error, which is one of the leading causes of security breaches.

Another benefit is scalability. As an organization grows, managing identities and access becomes more complex. New-age IAG solutions are designed to scale with business needs, ensuring security remains robust no matter how large the digital environment becomes. This comes with the additional benefit of improved performance on several key parameters such as productivity and operational costs. For instance, IAG can help enterprises identify cost optimization opportunities such as license harvesting. This ensures they don't pay for dormant and stale licenses once the user moves to a different role or leaves the organization.

Organizations, particularly the larger ones, conduct bi-yearly reviews and audits of their processes. In most cases, these reports can take anywhere between a week to a month to generate–time that can prove extremely costly for enterprise security in the event of compromised access. Through single-point dashboards with real-time visibility into user identities and access, organizations can generate detailed reports about the overall security posture of their digital environments at the touch of a button. This helps meet governance and compliance stipulations as well as mitigate risks with the required urgency.

Real-World Success Stories: Learning from the Best

When it comes to the impact that next-gen IAG solutions can have on businesses, let's take a recent real-world example from the financial sector. A prominent bank in India, founded in 1943, wanted to address security issues caused by manual provisioning and deprovisioning of user access. It also faced several challenges with UAR as well as audit and compliance, as it lacked controlled processes for user identity and access life cycle management. The fact that this needed to be done for over 15,000 users and 200 applications only added to the task's complexity.

The cutting-edge IAG solution brought on board helped address this issue with end-to-end automation of access provisioning and deprovisioning and enterprise-wide user life cycle management. Through a centralized dashboard, it also ensured better access governance and compliance through audit reports generated in real-time, with to-the-minute details about the health of identity and access security. The single pane of glass that this solution provided also enhanced user access visibility, enabling internal security teams to bolster the overall security profile of the organization.

Future Trends: What's on the Horizon?

As we look to the future, it is clear that the role of IAG in cybersecurity will only continue to grow. One trend gaining traction is the concept of decentralized identity, where individuals control their own digital identities, reducing reliance on centralized systems that are prone to attack. This could fundamentally change the way we think about identity management, making it more secure and user centric.

Blockchain, in particular, will play a major role here by decentralizing identity management. Storing identities across secure distributed networks will make it much harder for threat actors to access, tamper with, or steal information. Doing so will also address the burning 'single point of failure' issue that traditional systems often struggle with.

Another trend to watch is the increasing integration of AI and machine learning into IAG. As these technologies become more advanced, enterprises can expect to benefit from even more sophisticated vulnerability detection, threat nullification, identity governance, access provisioning/deprovisioning, 24x7 identity threat detection & response (ITDR), and UEBA capabilities with next-gen XDR and SIEM SOC operations. We are also likely to see greater adoption of cloud-native IAG solutions, which offer the flexibility and scalability needed to secure complex, multi-cloud environments.

The Path Forward

In the ever-evolving landscape of cybersecurity, staying ahead of the curve is not just a challenge – it's a necessity. By embracing these advanced solutions, businesses can implement a federated and simplified identity and access model designed for enterprise-scale needs. This approach powered by AI offers transformational insights and a comprehensive method for managing identity and access. It not only secures digital environments but also creates a safer, more seamless experience for users.

As we navigate this new frontier, one thing is clear: the future of cybersecurity lies in the intelligent, adaptive, and resilient capabilities of next-gen IAG.

About the Author

Pankit Desai, Co-Founder and CEO, Sequretek. Pankit Desai is an entrepreneur and the co-founder and CEO of Sequretek, a cybersecurity, cloud security products and services company. He Co-founded Sequretek in 2013, along with Anand Naik, and has been instrumental in growing the company into a leading provider of cybersecurity and cloud security solutions. Before starting Sequretek, Pankit held various technology leadership and management roles in the IT industry across companies such as NTT Data, Intelligroup, and Wipro Technologies. He holds a degree in computer engineering and has a strong background in technology and entrepreneurship.

At Sequretek, he is proud of the growth that this team has been able to achieve within a short duration. With product offerings that have found resonance with over 200 customers across industry segments, it has been able to grow at phenomenal growth rates and has ambitions to create India's first truly global security product and solutions company. The success of the company got a boost with multiple rounds of funding by very renowned funds including Omidyar Network India, Narotam Sekhsaria Family Office, Alteria Captial, FIS, ICBA, Pontaq Ventures, GVFL, and Unicorn Ventures. Under Pankit's leadership, Sequretek has won several awards and recognition for its innovative solutions and commitment to the cybersecurity industry.

Pankit can be reached at pankit.desai@sequretek.com and at our company website https://sequretek.com/.

Cyber Security in Customer Engagement: The Triple Defence Strategy

By Pat Carroll, Founder, Executive Chairman and CEO, ValidSoft

As digital interactions dominate modern communication, the rapid evolution of cyber threats demands robust security measures in customer engagement as a critical imperative. Traditional security methods are no longer sufficient, as cybercrime costs rise into the trillions annually. Addressing these challenges requires a comprehensive, triple-layered security approach in the Contact Center and Help Desk: ensuring the authenticity of the human, verifying the genuine user, and confirming the authorized agent.

Check #1: Is it Human? The Deepfake Check

One of the most insidious threats in today's cyber landscape is deepfake audio. Deepfake technology uses AI to create highly realistic synthetic audio that mimics the voice of a real person, posing significant risks for identity theft and financial fraud. The sophistication of deepfake technology means that these

synthetic voices can bypass traditional voice recognition systems, making it imperative for organizations to adopt advanced detection solutions.

Advanced solutions employ sophisticated algorithms to monitor and detect generative AI deepfake audio, computer-generated speech, and robocalls in real time. These technologies leverage machine learning models trained on vast datasets of genuine and synthetic audio to identify subtle anomalies and patterns that are imperceptible to human ears. Serving as the first line of defense, these technologies ensure that every call to Contact Centers and Help Desks, Agents, IVRs, or IVAs is genuinely human. This high-accuracy deepfake protection operates seamlessly and invisibly, providing an enhanced risk-based approach to every interaction while maintaining strict privacy standards without storing any Personally Identifiable Information (PII). Furthermore, no enrollment is required, operates in real-time and is totally language, dialect and idiolect agnostic.

Check #2: Is it the Genuine User? Voice Biometrics Verification

The second critical layer in this security architecture is the Voice Biometrics (VB) Check, ensuring that the individual interacting with the system is indeed the genuine user. This technology, known for its reliability, is available in multiple deployment formats including On-Premise, Private Cloud, Public Cloud, SaaS, Hosted, SDK, MicroSDK, and On-Chip. Voice biometrics verification works by analyzing the unique vocal characteristics of an individual, such as pitch, tone, and cadence, to create a distinctive voiceprint.

It uses advanced machine learning and large-scale Deep Neural Network (DNN) techniques to create and validate unique voiceprints for each user in real time. These voiceprints are language, dialect, and idiolect agnostic, ensuring inclusivity and broad applicability. Offering both active/dynamic and passive biometric verification, this approach enhances security and improves user experience by eliminating cumbersome traditional authentication methods such as passwords, PINs, or knowledge-based questions.

Furthermore, voice biometrics are continually evolving, incorporating advancements in AI to improve accuracy and resilience against spoofing attacks. These systems can also adapt to changes in a user's voice due to aging, illness, or emotional state, ensuring ongoing reliability and user satisfaction.

Check #3: Is it the Authorized Agent? Agent Voice Verification

Ensuring that the agent handling the interaction is authorized and genuine is the third pillar of this security strategy. This is crucial as a significant proportion of fraud originates from contact centers and over-voice channels. Furthermore, many Contact Centers are run through remote/off-site operations and are a prime target for malicious actors who often exploit weak points in customer service operations to try to gain unauthorized access to sensitive information.

Voice biometrics technology extends to agent verification, ensuring that only authorized personnel can access and manage customer interactions, and maintaining compliance in contact center operations. This layer of security protects against internal threats and mitigates the risk of unauthorized access,

preventing significant breaches and fraud. By verifying the identity of agents through real-time, continuous voice biometrics, organizations can ensure that every interaction is secure, trusted, and compliant with regulatory standards.

Agent verification not only enhances security but also boosts customer trust and confidence. Knowing that their interactions are handled by verified and authorized personnel, customers are more likely to engage openly and trust the service provided.

The Importance of Comprehensive Security Solutions

The sophistication of fraud tactics necessitates a robust, multi-faceted defense strategy. Integrating deepfake detection and voice biometrics, as offered by **ValidSoft,** not only fortifies security but also ensures compliance with stringent privacy laws such as GDPR, CCPA, BIPA, and all major jurisdictions worldwide. This compliance is crucial for organizations seeking to maintain ethical and regulatory standards while implementing advanced security measures.

ValidSoft's advanced security technologies are already deployed in real-world environments, protecting some of the world's largest financial institutions, enterprises, and government organizations. They offer high accuracy, rapid deployment, and significant return on investment, making them essential components of any organization's cybersecurity framework.

In addition to their security benefits, these technologies also provide valuable data analytics capabilities. By analyzing interaction patterns and voiceprints, organizations can gain insights into user behavior, identify potential security risks early, and enhance their overall customer engagement strategies.

In a world where cybercrime is the fastest-growing crime, affecting millions globally, the need for advanced and reliable security solutions has never been greater. By implementing a triple-layered security approach, organizations can protect their customers and users, safeguard their reputations, and lead the field in cybersecurity defense. Ensuring that every digital interaction is secure, trusted, and genuine is not just a necessity but a strategic imperative in the fight against evolving cyber threats.

Triple Defence Strategy

The Triple Defence Strategy is more than a theoretical approach; it is a practical, necessary response to the escalating sophistication of cyber threats. As cybercriminals continue to develop more advanced tactics, businesses must stay one step ahead by integrating deepfake detection, voice biometrics verification for users, and agent voice verification. This multi-layered defense not only enhances security but also streamlines user experiences and ensures regulatory compliance.

Organizations that adopt this strategy will be well-positioned to defend against the growing tide of cybercrime. By doing so, they not only protect their assets and reputations but also contribute to a safer, more secure digital world. The time to act is now, and the Triple Defence Strategy offers a clear, effective path forward in the ongoing battle against cyber threats.

About the Author

Pat Carroll is the Founder, Executive Chairman and CEO of ValidSoft. With over 25 years of experience in Information Technology and Financial Markets, Pat is a recognized industry thought leader and domain expert in security, strong authentication, and voice biometrics. At ValidSoft, he spearheads the commercialization of the company's extensive research and development efforts. Before founding ValidSoft, Pat held significant roles at Goldman Sachs as the European Head of Electronic Trading Technology, co-head of the European Equities Technology, and a technical advisor to the Investment Banking Division. He also has a robust background in Financial Services and technical roles from his tenure at J.P Morgan, Credit Suisse Financial Products, and Bankers Trust Company.

Pat Carroll can be reached online at pat.carroll@validsoft.com and at ValidSoft's website https://www.validsoft.com.

How to Root Out Malicious Employees

Understanding and mitigating the risk of insider threats

By Louis Blackburn, Operations Director, and Martin Ellis, Swarm Member at CovertSwarm

Malicious employees and insider threats pose one of the biggest security risks to organizations, as these users have more access and permissions than cyber criminals attacking the organisation externally.

It often seems that most organizations are not aware of the scale of these threats and do not prepare employees or distinguish guidelines for rooting out malicious and negligent employees in the way that employees usually receive training around spotting the signs of external hackers through phishing and vishing messages.

A recent report from DTEX highlighted that IP theft is at an all-time high because insiders are colluding with foreign governments. Uber's breach just a few years ago, which involved an adversary purchasing access to an internal user account, demonstrates the detrimental impact that can arise from a lack of awareness and policy in place around internal threats.

Understanding the type of threats to look out for and putting the correct frameworks in place will help to mitigate against the likelihood of insider threats taking place.

The main insider threats to businesses

There are several critical insider threats that organizations need to remain vigilant against. Denial-of-Service (DoS) attacks are a common concern; these attacks are often carried out by malicious employees

who possess extensive knowledge of the company's systems and networks, flooding it with illegitimate requests or attacking vulnerabilities that can cause it to crash or become unavailable to its users.

The risks associated with employees leaving the company with sensitive information or access credentials needs to be considered as well. A standard protocol should be in place to ensure access for former employees and their ability to compromise security after their departure is removed.

Malicious deletion of crucial systems or data by an insider can have a catastrophic immediate impact on a company. A loss of data or period of inactivity can lead to significant complications, including financial losses, damage to reputation, and a loss of trust from clients and partners. Legal recourse may be available to address the employee's actions but the damage will have already been done.

Negligent employees pose a similar threat

Not all insider attacks are caused by malicious employees; some may be due to negligence instead, but pose just as many dangers. The rise in AI usage and LLM tools has increased the chances of negligent employees leaking information to cyber criminals through accidental disclosure.

Employees may post data into AI or LLM tools to carry out activities such as data sorting or code checking, which is likely to be 'ingested' by the AI learning model (often allowed and outlined in the T&Cs) and then used to provide answers to other users, leaking that sensitive information. For example, if a user uploads details of a confidential project to an LLM, the data in the system might be used to provide answers to other individuals who ask questions like "Tell me about Project X." Companies need to make sure clear policies are in place when it comes to the use of AI and LLM tools for professional use.

Additionally, some LLMs are utilising 'add-ons' that can be leveraged to exfiltrate data input into an AI or LLM tool, leading to similar data leakage issues, making it all the more critical that organizations have systems in place to limit unauthorised exposure of data.

Organisations need to put the right tools in place to prevent insider threats

Despite the rising sophistication of insider threats, many organizations still lack the necessary tools to detect or prevent employees from copying sensitive information to portable devices and leaving the premises. This fundamental vulnerability highlights a critical area where many organizations need to improve their security measures and monitoring capabilities to effectively combat insider threats.

To effectively root out malicious insiders, organizations must invest in comprehensive security tools and practices, such as robust monitoring systems, strict access controls, and regular audits.

Additionally, fostering a culture of security awareness and implementing clear guidelines for reporting suspicious activities are essential steps in mitigating the risk posed by insider threats.

The first step to mitigating insider threat

Implementing ISO 27001 and ISO 42001 into business operations are great ways to begin reducing the risk of insider threats. Both are valuable frameworks and help to establish rigorous procedures and controls.

It's important to make sure these frameworks aren't merely reduced to tick-box exercises and are fostered into daily operations.

ISO 27001 focuses on a systematic approach to information security management, emphasizing regular audits, access controls, and comprehensive employee training.

Similarly, ISO 42001 provides a structured approach to occupational health and safety management, which can indirectly support security efforts by promoting a safer work environment.

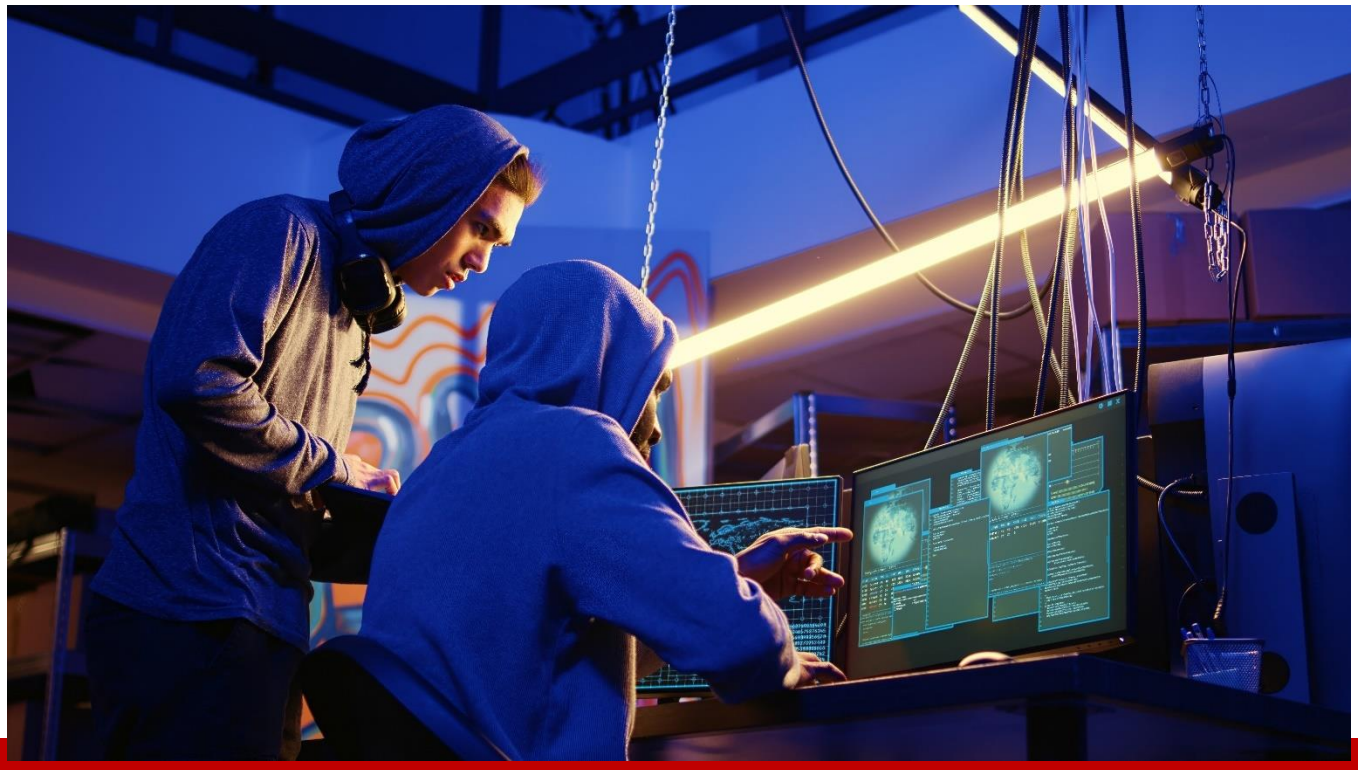
The challenge is integrating these standards into everyday business practice, and ensuring they are enforced and updated. Organizations need to embed them into their operational practices, taking a proactive stance against insider threats and increasing security awareness among employees.

About the Author

Louis Blackburn is Operations Director at CovertSwarm. As Operations Director, Louis brings robust commercial cybersecurity and red-teaming experience to his role overseeing the company's day-to-day operations. His focus is on optimizing the functionality of the company's growing team of ethical hackers - known internally as the Swarm. He is also responsible for identifying evolving attack vectors crucial to advancing CovertSwarm's groundbreaking Attack Surface Management Platform – the CovertSwarm Portal.

Previously, Louis led the internal Red Team at Lloyds Banking Group and served as a Computer Forensic Analyst at the Eastern Region Special Operations Unit.

Martin Ellis, is a Swarm Member at CovertSwarm. Part of the founding team at CovertSwarm, Martin is responsible for helping clients improve their security posture through offense review of application, guidance in best practices and training on security principles. Martin possesses a demonstrated background of working in the cyber security industry, with a focus on application testing.



Why the Growing Risk of Cyber Inequity Threatens Critical Infrastructure

By Fran Rosch, CEO, Imprivata

Cyber inequity is a growing chasm that continues to separate organizations with robust cybersecurity and technology capabilities from those without. This digital divide is a global cybersecurity crisis in the making.

The World Economic Forum identifies cyber inequity as a high-impact issue, defining it as the widening divide between organizations equipped to defend against cyber threats and those that lack the basic means to do so. This gap is especially evident in smaller, under-resourced organizations, which are highly prone to cyberattacks.

The Widespread Impacts of Cyber Inequity

Ransomware attacks or IT outages can have a significant effect on the public, impacting the accessibility of critical needs like healthcare, transportation, and other goods and services. For example, patients may be diverted to other medical facilities if one hospital system goes down, potentially creating a 'medical desert' in rural areas and putting public health at risk. Or manufacturing plants may pause production, impacting their bottom line and causing supply chain shortages. Organizations without adequate

cybersecurity resources are at an increased risk of being attacked, impacting the communities and businesses that rely on them.

Even if a business isn't directly targeted by a cyberattack, it can still be impacted by one. Supply chain attacks, for example, exploit vulnerabilities in the supply chain network, targeting less secure elements, such as third-party vendors or software providers with access to sensitive information. The fallout from these attacks reveals the cyber inequity gap in the context of cybersecurity preparedness. Those with stronger cybersecurity programs who are better prepared to deal with the fallout will likely recover faster than those without the resources to do so, further expanding the cyber inequity divide.

Cybersecurity Challenges for Critical Industries

While there's no shortage of regulatory guidelines for critical industries like those from NIST and CISA, under-resourced organizations face an uphill battle with cybersecurity investment, largely exacerbated by budget constraints.

Notorious attacks like SolarWinds, Colonial Pipeline and recently ChangeHealthcare reveal the concerning reality that many organizations do not have the resources to invest in cybersecurity at a rate necessary to outpace attacks - or to deal with the fallout. Already forced to use limited budgets for cyber insurance, many organizations do not have enough resources or the necessary IT talent to implement robust cybersecurity programs. In fact, only 22% of global organizations say that they have the resources to meet their cyber objectives, in what is sometimes referred to as the "cyber poverty line," according to the World Economic Forum.

Those who are less equipped to thwart threats or recover from them will remain at the greatest risk, as will the communities and individuals who rely on them. Unfortunately, those in rural or under-resourced areas tend to be at the greatest risk. Understanding and recognizing the collective risks posed to the public underscores the responsibility and important role that legislative bodies have in addressing this challenge.

Taking Action & Closing the Cyber Inequity Gap

Without legislation, defined standards, and/or incentives, critical industries face significant challenges in adopting comprehensive cybersecurity strategies. However, these mandates and incentive programs must be aggressive enough to truly address the problem.

For instance, critical industries like healthcare and manufacturing are dependent on numerous technical partnerships and work with countless vendors who access their systems, resulting in a substantial volume of third-party attacks and placing them at increased risk. Although there are pledges from organizations like CISA asking vendors to meet certain standards by 2025, these do not impose any penalties for non-compliance. In the absence of more motivating mandates or incentives, organizations without adequate cybersecurity budget or resources are often unable to address supply chain risk and they remain vulnerable.

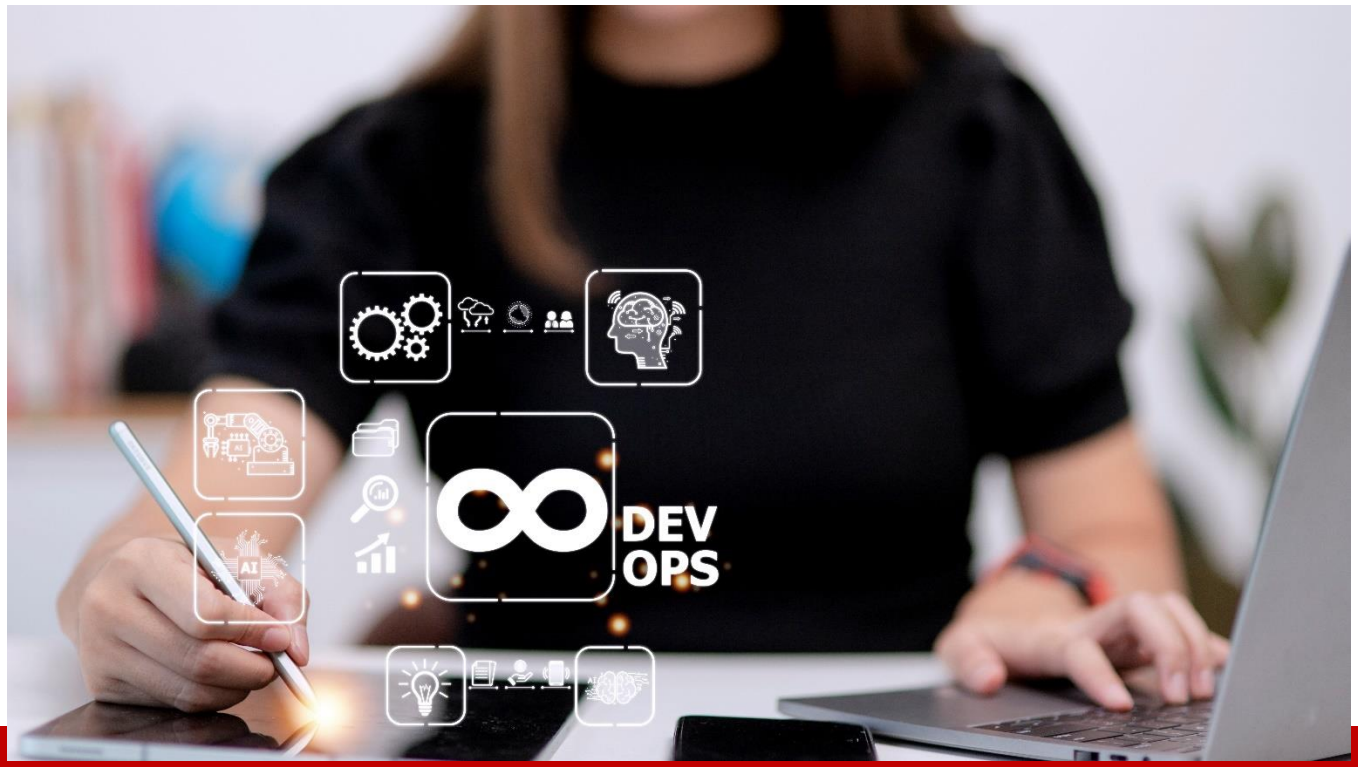
Another example is mitigating the risk of credential theft caused by human errors, which account for more than 60% of compromise factors, according to Google Cloud's 2023 Threat Horizons report. Employing access management solutions can address this threat and improve security by reducing phishing risks and other attacks associated with credential theft. However, implementing an enterprise-wide access management strategy takes investment and resources. For those organizations facing cyber inequity, this often leads to choosing inferior solutions or continuing to rely solely on passwords to protect critical resources.

Security remains a top priority across these critical industries, even for the cyber "have nots." Therefore, it is incumbent on IT leaders, cybersecurity vendors, lawmakers, and other regulatory bodies to work together to create meaningful policies, guidelines, and incentives to close the cyber equity gap. This collaboration must move forward with urgency, showing substantive progress in short order. Otherwise, the cyber equity gap will continue to widen, leaving critical industries – and the public they serve – at risk.

About the Author

Fran Rosch, President and CEO of Imprivata, is a seasoned leader with over 25 years of experience in the field of enterprise security and identity management. Rooted in security, privacy, and trust, Fran has built a distinguished career marked by significant achievements, previously serving as the CEO of ForgeRock. During the five years of Fran's leadership, ForgeRock grew over 400%, executed on a SaaS transition and cemented itself as a leader in both the Consumer Identity and Access (CIAM) and Workforce Identity markets, completing a successful IPO in 2021 and a sale to Thoma Bravo in August of this year.

Fran can be reached online via LinkedIn, X, and at our company website https://www.imprivata.com/.



Is Platform Engineering a Step Towards Better Governed DevOps?

By Kapil Tandon, VP of Product Management for Perforce

Since 2010, Puppet's annual State of DevOps Report has tracked trends in IT, including security and, more recently, the growth of platform engineering. 2024's edition, which includes the results of a survey of over 600 IT professionals worldwide, shows that security and platform engineering are now closely intertwined, with platform engineering teams now taking on more responsibility for security. Plus, the results show that these teams are making a tangible difference.

Before diving into more details, it is crucial to understand what platform engineering provides. Platforms aim to give end users — especially software developers within organizations — fast and simplified self-service access to the technologies they need to do their jobs. These platforms are managed by platform engineering teams, who provision and manage all workflows, tools, and platforms involved. Platform engineers typically come under operations or engineering as part of teams or separate ones. They could even be part of product teams. Their area of focus is ensuring that their primary customer, the developers, get what they need to deliver at speed on the organizational needs.

Platform engineering is not just some fad. Gartner has predicted that 80% of global organizations plan to have a team dedicated to platform engineering by 2026. The State of DevOps Report found that 43% of

respondents have had a platform team for at least three years and a quarter for six to nine years. 65% said that platform engineering teams will receive continued investment.

Platform engineering offers multiple benefits to businesses and their employees. First, it reduces the volume of support requests to IT operations teams, allowing them to focus on tasks other than firefighting. Second, developers can concentrate on their core work, knowing that what they need is being provided without the need to search for it or verify its accuracy.

The value of all this cannot be underestimated, given the growing complexity and scale of many software development environments today. Software development is the point at which vulnerabilities can occur, leaving the door open for future exploitation. Think of platform engineering teams as the protective barrier between developers and potential chaos.

And it is working. When asked about the benefits of platform engineering, 31% of respondents in the State of DevOps survey reported a reduced risk of security breaches. Improved compliance and security was also the third-highest use case (49%), surpassed only by improved productivity and automated, standardized processes.

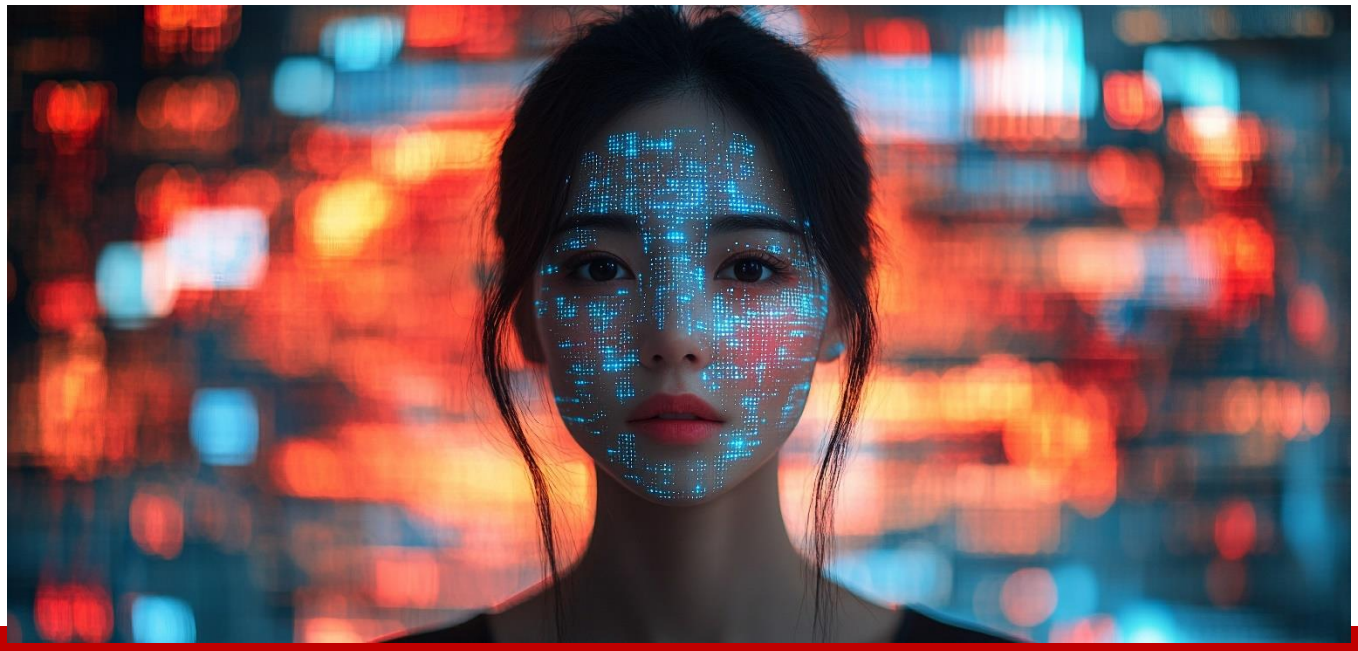
This demonstrates a significant shift in DevOps: security is being integrated up-front and considered right at the start of platform strategies. 70% claim that security was built into their platforms from the beginning. A further 60% cite security and compliance as the leading benefit of platform engineers. This is a sea change. Previously, while security may have been acknowledged as necessary, implementation was typically left to individual teams to implement.

With platform engineering, security management can become controlled and consistent across organizations. In addition, they are increasingly likely to have a platform dedicated to security (and other platforms for other functions). Having specialized platforms allows teams to focus on the excellence of what they do rather than over-centralizing and forcing people to potentially use tools and take on responsibilities they don't want or need. The survey found that 56% have five or more platforms, with almost 10% reporting they have at least 10.

Platform engineering has evolved significantly in just a few years, and its value is now well understood by many organizations. We see it as a crucial stepping stone in creating more governed DevOps. Embracing platform engineering's contributions to better security and compliance is important, as is managing an estate that is continuously patched to ensure uptime. The trend of delivering patches to the estate automatically, rather than through manual patch management, is growing and is expected to continue throughout 2024 and beyond.

About the Author

Kapil Tandon is the VP of Product Management for Perforce Software. He has more than 25 years of experience in product roles within tech, and has previously served as the VP of product growth for Tricentis and as a principal PM lead for Microsoft. Tandon holds a master's in marketing from Pace University. Kapil Tandon can be reached online at kapil.tandon@perforce.com, https://x.com/kapilt, https://www.linkedin.com/in/kapilt/ and at our company website https://www.perforce.com/.



Deepfakes: How Deep Can They Go?

By Arik Atar, senior threat intelligence researcher for Radware

With the help of today's technology, virtually anyone can create a passable deepfake—a manipulated image, video, or audio recording that seems real. All that is required is a consumer-grade computer or smartphone and an internet connection. Without question, we are fast approaching an era where audiovisual content is no longer inherently trustworthy.

In fact, a recent Dimension Market Research report reveals that the global deepfake AI market is expected to reach a value of $79 million by the end of this year, and a market value of nearly $1.4 million by 2033.

Damages Posed by Deepfakes

Undetected deepfakes can be used in multiple ways to target and compromise businesses, spread misinformation, disrupt markets, business operations, and supply chains. For example, they can be used to impersonate executives in fake video calls, or audio recordings, tricking employees into taking action, like revealing sensitive information or transferring funds. Deepfakes can also be used to generate phony social media content intended to damage a company, its reputation, or stock price, or to doctor product images and videos as part of counterfeiting operations. In addition, they can be used to make fraudulent transactions by spoofing biometric security systems with fake facial impressions and voice prints as well as synthetic identities. These events threaten privacy and security by enabling fraudulent accounts and transactions.

The potential financial and reputational damage posed by deepfakes is significant. Fraudulent wire transfers from a single deep-faked executive video could cost a business millions of dollars. And viral, deep-faked social media posts could undermine consumer trust and market value.

One particularly alarming example of a successful deepfake attack occurred at an international company based in Hong Kong. According to an article in the South China Morning Post, attackers successfully stole $25 million from the company by organizing a video meeting that was faked using deepfake technology. A company employee received a phishing email from the CFO (so he thought), requesting a funds transfer. Thinking it was legitimate, the employee was tricked into joining a video call, which included the employee and deepfaked versions of the other participants, including the fake CFO, who instructed the employee on how to make 15 different transfers totaling $25 million. Unfortunately, it took several days for the employee to realize the entire event was a scam.

Keys to Defense: Swift Decisive Actions

While deepfakes might seem impossible to identify on the surface, there are several ways to spot them.

AI-based detection systems can identify fakes across large datasets by analyzing unusual movements, visual artifacts, audio distortions, contextual inaccuracies, and other signatures. However, it remains an arms race as deepfake creators learn to overcome imperfections. Some experts estimate detectors will be unreliable within 12-18 months.

Metaphorically, spotting deepfakes is like playing the world's most challenging game of "spot the difference." The fakes have become so sophisticated that the inconsistencies are often nearly invisible, especially to the untrained eye. It requires constant vigilance and the ability to question the authenticity of audiovisual content, even when it looks or sounds completely convincing.

Recognizing threats and taking decisive actions are crucial for mitigating the effects of an attack. Establishing well-defined policies, reporting channels, and response workflows in advance is imperative. Think of it like a citywide defense system responding to incoming missiles. Early warning radars (monitoring) are necessary to detect the threat; anti-missile batteries (AI scanning) are needed to neutralize it; and emergency services (incident response) are essential to quickly handle any impacts. Each layer works in concert to mitigate harm.

It's important to take a multi-pronged approach when dealing with deepfakes. An effective strategy should include employee training in awareness and identification and strict authentication measures for sensitive requests. It should also include designated secure channels for executive communications, monitoring for suspicious assets, AI-based scanning of incoming media content, and a healthy incident response plan. The key is to act swiftly and decisively.

Reversing Deepfake Damage

If a deepfake attack succeeds, organizations should immediately notify stakeholders of the fake content, issue corrective statements, and coordinate efforts to remove the offending content. They should also

investigate the source, implement additional verification measures, and provide updates to rebuild trust and consider legal action. It's crucial for leadership to get ahead of the narrative. They must be transparent and accountable and take concrete corrective actions to mitigate long-term financial loss and reputational harm.

The more that false information goes unchecked, the more damage it can do. Having a rapid response playbook ready is essential to a good defense.

The Future of Audio and Visual Communications

In addition to direct attacks, enterprises must also prepare for deepfakes to be weaponized across other domains, such as politics, regulations, and social unrest. Deepfakes not only raise security concerns but also pose harmful enterprise risks.

As synthetic media becomes more widespread, video and audio may lose their inherent credibility. Consequently, enterprises need to shift communication and authentication approaches, relying less on audiovisual content and more on cryptographically secure channels.

It's important to note, however, that not all synthetic media is malicious. For instance, "Shallowfakes" and virtual avatars are being adopted more often for legitimate uses in industries like entertainment and education. Regardless, as generative AI technologies become more and more sophisticated, companies should act now to establish explicit policies that distinguish between permissible and prohibited uses.

About the Author

Arik Atar is a senior threat intelligence researcher at Radware, where he helps identify security vulnerabilities, thwart attacks in real time, and proactively mitigate potential attacks for clients. He brings a wealth of experience in cyber threat hunting, combining strategic cyber threat analysis with social psychology. Before Radware, Arik worked at PerimeterX, where he focused on researching underground bot-for-hire marketplaces, leveraging his expertise in threat hunting to mitigate Denial-Of-Inventory and Account-Take-Over attacks. Before that, he joined Bright Data where he led investigations against high-profile proxy users, uncovering and addressing cyber adversaries' tactics, particularly in DDoS and bot attacks. Arik has delivered keynote speeches at conferences such as Defcon, APIParis, and "The-Fraud -Fighters' Cyber Defenders" meetups. Arik studied counterterrorism and international relations at IDC University, which assisted in shaping the strategic macro perspective he uses in threat actor research.

LinkedIn: https://www.linkedin.com/company/radware/

Company website: http://www.radware.com

Incident Response Planning: A Portion of Planning is Worth a Pound of Gold

By Chris Snyder, Principal Sales Engineer, Quadrant Security

When you are hacked, you want to recapture control quickly as hackers move through systems, locking sensitive information and holding it for ransom. You need to determine the extent of the breach immediately, the exact attack vector, and how to insulate the rest of the network. Organizations need an effective incident response (IR) plan to accomplish these actions.

However, not all IR plans are effective or contain the necessary elements to help restore calm in the employee maelstrom unleashed after a breach. We all know the idiom, “An ounce of prevention is worth a pound of cure.” In case of a pending breach, this idiom can be rephrased to “a portion of planning is worth a pound of gold;” planning refers to incident response and gold being extortion funds saved. This article outlines six best practices for effective IR planning.

Best Practices for IR Planning

1. Have an IR plan ready before the incident happens.

You already have a plan for natural disasters, civil unrest, or other disruptions. The same goes for your incident response—have a plan and ensure it's part of your continuity of operations (ConOps) planning. The IR plan should be a part of your knowledge base and disaster recovery planning process. Outline clear and deliberate steps that are well-informed, specific, and actionable. The goal is to identify, validate, and remediate an incident quickly and safely. A big part of the plan's success is ensuring that your staff understands and knows how to execute it in challenging circumstances; this requires covering scenarios like compromised cloud-based or on-prem IT services.

2. Obtain visibility; understand the circumstances.

Visibility is paramount; you cannot mount an effective response if you don't know where the malware lurks and how it got into your network. Adequate visibility comes from advanced detection tools, plus expert guidance from service desk professionals. Together, they validate the attack, determine its severity, and how the malware gained access. Without the aid of IT cybersecurity professionals, you may be overmatched by the sophistication of today's hackers.

3. Prepare for out-of-band communications.

Malware attacks often affect email servers, messaging systems, and VoIP phone systems. A dimension of the attack almost always involves taking over all communications. Hackers monitor and control these channels to interrupt your ability to manage the attack. Your plan needs a physical communication protocol with a hierarchical order of up-to-date contact information. This information includes mobile phone numbers and alternate, off-network email addresses. It's imperative to communicate about the breach over out-of-band channels immediately. The idea is to stay in control and ahead.

4. Don't panic or overreact.

Being hacked is stressful. You want to avoid making rash, heat-of-the-moment decisions. The IR plan defines protocols your incident response team, a group of individuals within your organization trained to respond to and mitigate the effects of a cyber attack, can follow instead of wasting time seeking decision-makers and executing unnecessary actions. If you are hacked, the malware is already in your systems, seeking to do some damage. The incident response team needs a playbook to detect where they'll be pivoting and how they're moving around. Responding and mitigating usually take several days, so staying calm and patient is required. The best remediation techniques involve watching the activities related to the breach—when and where they're logging in, hiding the malware, and what data they're accessing.

5. Create and implement an incident-specific remediation plan.

Once you have identified the proper channels of out-of-band communications, coordinate efforts in a well-defined chain of command to identify the attack extent while remaining vigilant of all downstream networks, including channel and partner networks. Hackers often return looking for new or previously exploited weaknesses. Your cybersecurity team needs to perform 7/24 monitoring, which refers to

continuous, round-the-clock network monitoring for any signs of a cyber attack. This level of vigilance is necessary to ensure that any subsequent attacks are detected and mitigated as soon as possible.

6. Seek help when necessary.

Creating an effective IR plan is time-consuming. Most organizations need in-house service management resources to deal with an attack while running daily operations. Many cybersecurity companies notify you about the data breach but must help you understand the procedural steps to navigate the incident. When a bad actor has infiltrated the network, a third-party cybersecurity company will provide the calm, skilled, around-the-clock support needed to manage the situation effectively. Remember, your single breach situation is only one of the critical circumstances these cybersecurity companies can handle. Dealing with attacks in a timely and quality-assured manner is their job.

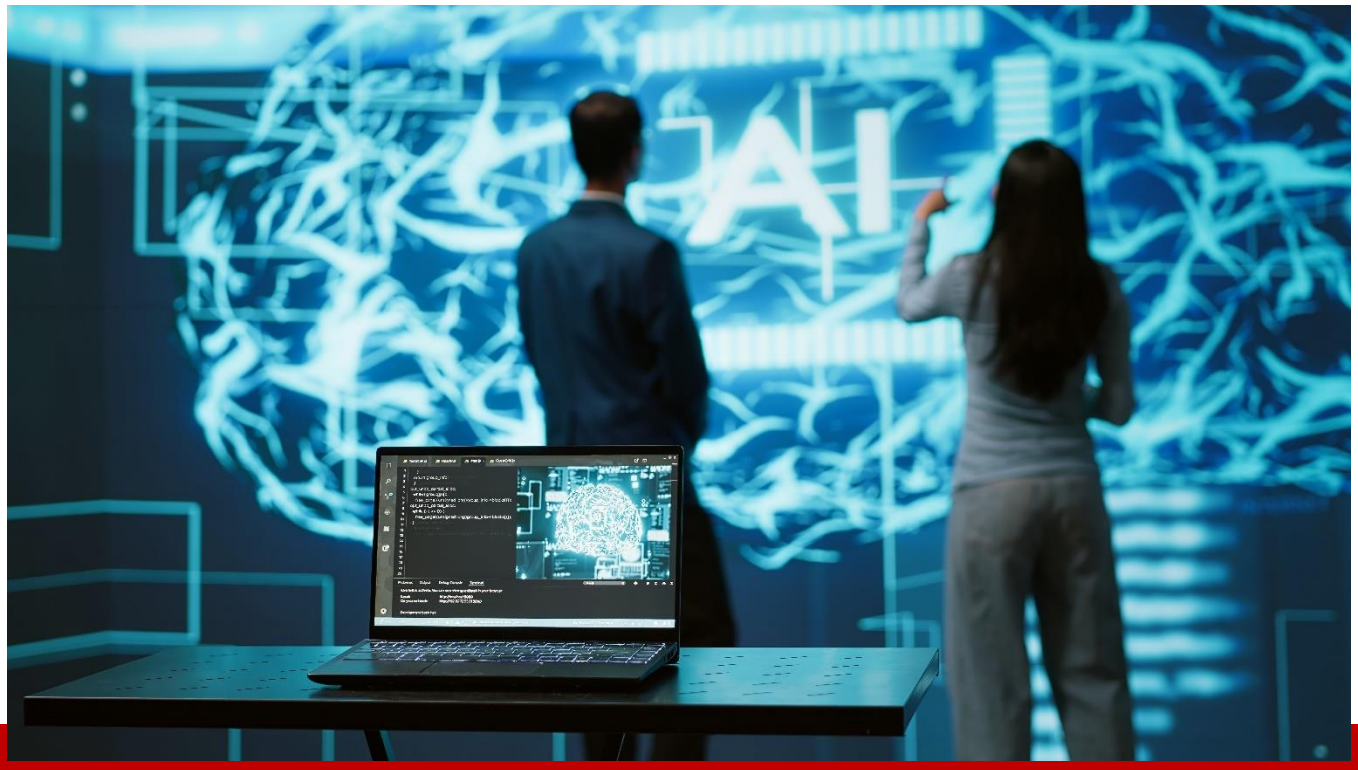
Conclusion

One of the most effective tools at a bad actor's disposal is chaos. The more an organization exhibits a dysfunctional and emotional response, the more time the hacker has to lock your IP and the less time you have to halt the advancement. Most people are familiar with life circumstances that require advanced planning, such as 529 college funding, IRA retirement, and life insurance. For almost every organization, SMB to Fortune 50, a hack is as inevitable as the aforementioned financial planning milestones. The difference between them is that in our personal lives, we have succumbed to the notion that these are inevitable; in our corporate lives, we hedge our bets that a hack will happen to the "other guy."

If a corporate hack is inevitable, you will need assistance navigating the turbulence, and IR planning should be placed with a higher degree of urgency; in the same manner, we turn to professional money managers to help us prepare for personal events. Corporations need to align with cybersecurity professionals who have navigated many breaches and can incorporate best practices into action items proven to regain control. Just a portion of good IR planning can save a pound of corporate gold.

About the Author

Chris Snyder is a Cybersecurity Expert and Principal Sales Engineer at Quadrant Security, having honed his skills as a Systems Administrator, Threat Analyst, and Paratrooper Infantryman in the US Army. He leverages his diverse background and cybersecurity knowledge to help clients find the best security solutions for their unique needs. Chris can be reached online at csnyder@quadrantsec.com, https://www.linkedin.com/in/christopher-snyder-17336b135/, and at https://www.quadrantsec.com/.



Building Contextual Data Models for Identity Related Threat Detection & Response (ITDR)

By Anil Bhandari, Chief Mentor, ARCON

Amid the rising pace of digitization, a growing number of organizations are managing their workloads based on a hybrid model. A hybrid model by design leads to dispersion of corporate data across different environments. Against this backdrop, it has become more difficult than ever to secure and protect the data from many digital identities that are used to access various systems.

While security components like multifactor authentication (MFA), Single Sign-On (SSO), and Password Vaulting, among others, provide strong layers of security around data, having a corporate identity-related threat detection and response mechanism based on a data contextual model enables the organization to build a proactive information security posture.

Let us consider this: every day, a modern-day enterprise generates data in sizes of gigabytes, terabytes, petabytes, or even more. However, most enterprises are not equipped enough to manage or understand the data patterns, leading to security gaps.

Data-Contextual Models: Deep Insights

Maintaining a firm grip on sensitive enterprise data is never easy. As organizations typically operate in several functional departments, the data invariably ends up sitting in various data repositories. This is the normal scenario seen in today's highly heterogeneous IT environments with an ever-increasing number of endpoints. And with every passing day, the volume of unstructured, siloed data keeps growing. As a result, the complexities of managing this data become increasingly cumbersome, and the data risk vector expands. There is absolutely no clarity about "who" is accessing "which" data and for "what" purpose "where" and "when."

Some of the typical challenges organization face are as follows:

- Lack of awareness of what sort of data is being generated
- Absence of visibility on the volume of data exposed to end users
- Lack of categorization of data based on its sensitivity
- No mechanisms in place to restrict or grant controlled access to sensitive data
- Cumulation of stale/redundant data leading to increased attack surface, IT inefficiencies and compliance issues

ARCON, a pioneer of risk-control solutions in IAM (Identity Access Management) space, offers the "Data Intellect" model that is built on AI/ML driven context-aware models and enables the discovery, classification, and categorization of large volumes of unstructured enterprise data and helps orchestrate remedial steps to control access to data while improving compliance posture simultaneously. It offers a "Single Pane of Glass" for "comprehensive observability" and leverages machine learning algorithms, and designed in such a way that enables IT security pros to:

- Make meaningful sense out of the unstructured exposed data- "who," "which," "where," "when, and "what" of data
- Understand the data patterns from data repositories, file formats and gain actionable insights necessary for data-centric security decisions
- Build contextual security models by integrating data-context with user-context

By developing contextual data models, security and risk management teams can make more sense of the static and dynamic data that is stored in silos. This model helps in describing data and events and leverages AI and ML technology capabilities to understand the anomalies as it enables them to classify the data, itemize the exposed data, categorize the critical data, and help the team to comprehend the "where" and "what" of data.

In addition, a data contextual model provides actionable insights on data that are useful for forensic analysis and overall information security posture. There are three components that build contextual security around data.

Categorization of Data: Data Intellect allows IT security teams to get a complete visibility on the "type" and "purpose" of data generated in an organization. This functionality captures what form of data (data classification) is accumulated in the data repository; for example: excel file, word docs, JPG, among others.

Furthermore, it captures what sort of data (document classification) is being generated. For instance, what percentage of data is related to legal, commercial, IT, PII (Personally Identifiable Information) among other forms of data. This functionality offers a “single pane of glass” to comprehend the data patterns, important to classify data from security perspectives.

Classification of Data: This functionality provides deeper analysis of the enterprise data. Classification of data enables IT security and compliance teams to discover what percentage of data is “top secret,” “confidential,” “restricted,” “sensitive,” “Internal,” and “public” in nature, what percentage of data is exposed to vulnerabilities and what percentage of data is no longer required or redundant data. This functionality offers descriptive classification ensuring that there is no human error and data misclassification. It enhances the enterprise governance framework as well as data categorization, making sure that employees know what “sensitive data” and what “Vulnerable data” is lying in data repositories.

(Please note that at times the words classification and categorization may be used interchangeably by organizations as per their definition.)

Orchestration Measures to Restrict Access to Data: Another standout capability of ARCON’s Data Intellect solution is its seamless integration with another robust module- ARCON | Endpoint Privilege Management (EPM). While Data Intellect module enables IT security pros to discover, classify and categorize data, the EPM module enforces robust access control around data that is deemed “sensitive” or “exposed.” It not only helps to enhance the data-security posture but also enables data controllers and data processors to comply with regulatory mandates that require restricted access to data for maintaining confidentiality and integrity of data. In addition, Data Intellect’s timeline monitoring capability for documents enables IT security pros to track the entire history and the flow of the individual document including alerts to administrators, if any suspicious activity takes place.

To conclude...

Building contextual data models also helps in making wiser decisions about the identity and access management of Life Cycle. Deep-dive insights using such models also enable IT security and risk management teams to decide to whom they should or should not grant access and revoke rights to access systems for better identity threat detection and response, and this goes a long way toward a Zero Trust model.

About the Author

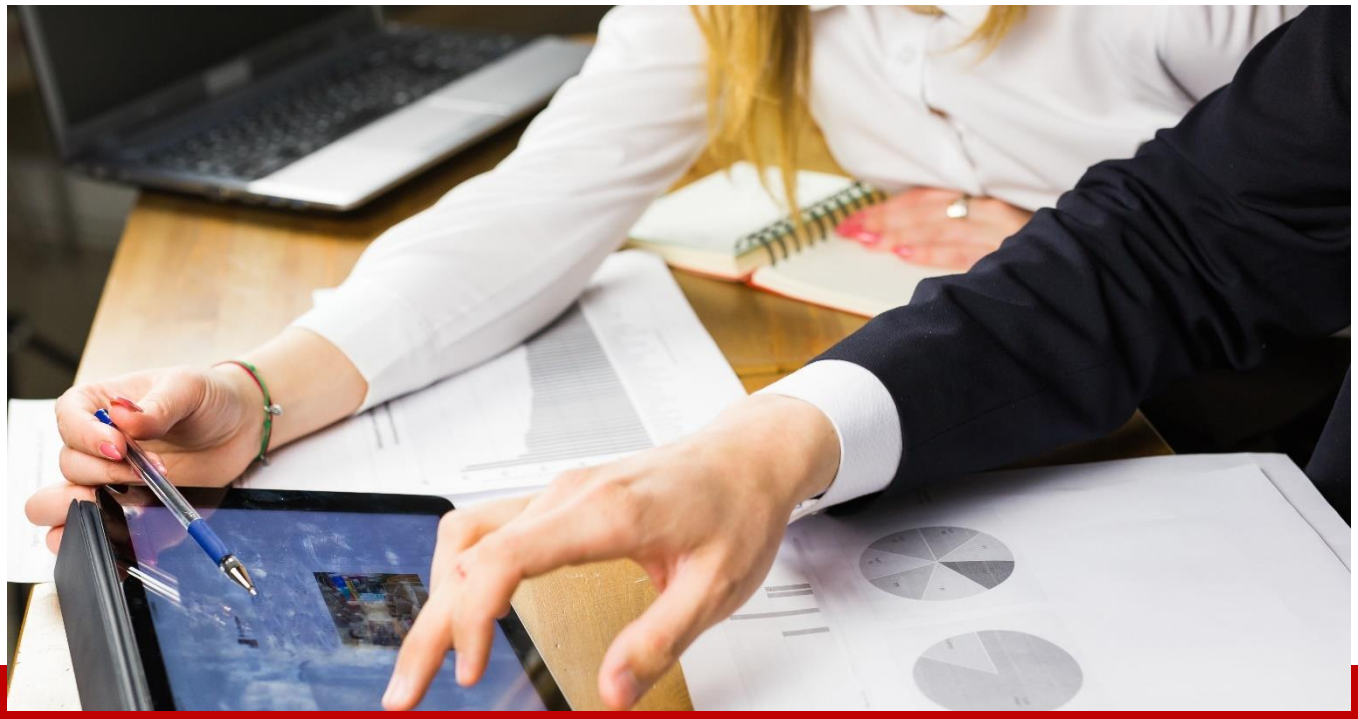
Anil Bhandari, Chief Mentor, ARCON, is an inspired innovator, technologist and thought leader in Information Risk Management. A Chartered Accountant by profession, Anil's area of interest has always been Enterprise-wide Risk Management.

Anil started his career as a management consultant, serving in many sectors which ranged from engineering to commodities and from healthcare to IT/ITES. Besides, he also led several M&A and Due Diligence teams on behalf of clients spanning several industry verticals, especially in the EU (European Union) region.

Thanks to his in-depth experience of assessing risks for data centers, networks, varied technology platforms and core IT processes, Anil possesses intensive knowledge in the Information Security and GRC domains. The knowledge acquired over the years has helped him to consult large enterprises looking to implement innovative solutions in Cyber Security and the best practices for critical functions such as BCP/DR.

Anil has been serving as a Chief Mentor since the Company was founded in 2006. In ARCON, he mentors a large team of software engineers and product managers for product innovation and technology roadmaps. Discussions and strategizing with the product development team to build robust risk control solutions that mitigate Information Security related challenges emerging in the digital sphere dominates his packed work schedule.

Anil Bhandari can be reached online through their company website https://arconnet.com/.



Experience from GAP Assessment Audits for NIS2 Compliance

New compliance requirements are in place

By Zsolt Baranya, Senior Information Security Officer of Black Cell Ltd.

The NIS2 (Directive (EU) 2022/2555 of the European Parliament and of the Council) imposes cybersecurity and information security compliance obligations on many organizations that previously had no such requirements. Most of these organizations, wishing to avoid financial penalties, aim to comply with the directive and the national implementing laws. To achieve compliance, they engage expert firms to ensure adherence. The first step towards compliance is to conduct an audit to identify any non-compliances. This article aims to highlight the experiences from the GAP assessment audits for organizations that have recently become subject to NIS2 compliance.

In most cases, the primary goal of an organization's leadership is to avoid financial penalties. This approach reflects a clear lack of full information security awareness. Organizational leaders often initially believe that hiring an expert organization to ensure compliance is a one-time task that will prevent any negative consequences. Both before and after audits, it is important to communicate that audits and addressing identified deficiencies are not one-off activities, but that the information security management system (ISMS) established must be operated continuously. A change in mindset is needed so that the goal is not merely avoiding fines or personal liability for leaders but creating value and reducing the likelihood of ever-evolving threats. Offering training opportunities is recommended to increase the awareness of both leaders and employees in different roles, laying the foundation for this change in mindset.

During the execution of audits, it is often found that the audited personnel of organizations do not fully understand the requirements of the control measures. This frequently leads to misunderstandings. It is necessary to clarify the concepts for all audited parties and highlight the connections—why certain requirements exist, how they are interconnected, what the goal of their implementation is, and whether the control in question is applicable to the organization. As a result, audits tend to take longer, and the process of educating and ensuring understanding consumes significant resources. We recommend educating the audited party prior to any NIS2 audit, especially for organizations that were previously not subject to such requirements, to explain expectations and ensure a smoother audit process. It is crucial that everyone understands how to properly provide evidence-based answers to audit questions.

As mentioned in the introduction, organizations that have recently become subject to NIS2 compliance have not previously dealt with information security compliance, do not hold an ISO 27001 ISMS certification, and were not previously subject to legal regulations. As a result, many of these organizations outsource their IT operations, which are focused solely on ensuring the functionality defined in contracts. Often, these IT service providers were selected long ago based on trust and business considerations, and there was no requirement from leadership to ensure information security on the part of the provider. Consequently, these service providers often have limited information security skill sets, which may pose challenges when addressing identified deficiencies. As part of the audit, it is important to not only ensure control compliance but also emphasize what conditions are necessary to maintain compliance, both from an IT operations and information system application perspective.

In organizations where IT operations are not outsourced but managed by in-house IT staff, the situation is slightly different. These organizations often face a shortage of skilled personnel, meaning that the system's functionality often relies on system administrators and IT staff. Typically, the knowledge resides in the heads of these IT professionals, with a lack of documentation, making the absence of these individuals potentially devastating. This means that the IT staff managing the system can be identified as Single Points of Failure. NIS2 compliance is not possible without documentation, making it crucial to have support staff who can document the controls required by information systems and create the conditions for an auditable and transparent Information Security Management System (ISMS) within the organization. It is worth noting that not only is the operation's documentation often lacking, but policies, procedures, and process descriptions are also frequently missing in audited organizations. In many cases, practices are established but not documented. It is recommended to provide suggestions for establishing an appropriate regulatory framework in audit reports, thereby assisting the audited organizations.

Even when IT knowledge is available (which is often not fully the case), IT security and information security knowledge is generally lacking, and understanding the interconnections can be challenging. As control compliance is examined, audited parties often do not understand why they need to know certain things. This brings us back to the importance of pre-audit training, where it can be explained that this is a general set of controls and not a 'one size fits all' solution. Some controls may not need to be complied with, for example, the organization does not have the relevant activities. For instance, if there is no development activity, it is impossible to identify non-compliance related to a lack of code reviews since no development is taking place. The presence of an information security specialist can address this kind of 'misunderstanding,' but such expertise is not always available in every organization.

For many organizations, the primary goal is to establish the minimum necessary conditions for operation, and beyond that, they often pay little attention to either IT security or information security. In many cases, there are deficiencies that could cause the system to collapse at any moment, or the lack of regulatory and logical protection measures leads to a high likelihood of data protection incidents, some of which may have already occurred without the organization's knowledge due to the absence of controls (such as monitoring). Given the potential for large fines, it is advisable to address these areas, especially since many organizations are pursuing NIS2 compliance primarily to avoid penalties.

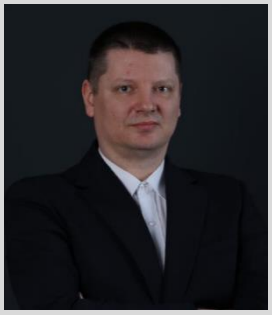
In many cases organizations do not know their processes or the supporting information systems (neither the internal nor external ones they use), nor the number of these systems or their interconnections. Organizations are simply satisfied if the IT functions and supports business operations. How it operates often does not concern upper management. However, in today's threat environment, this attitude leads to inevitable failure. Moreover, due to the lack of information on processes and information systems, the audit itself faces difficulties, the list of identified deficiencies will be incomplete, and consequently, the action plan for addressing those deficiencies will be inadequate.

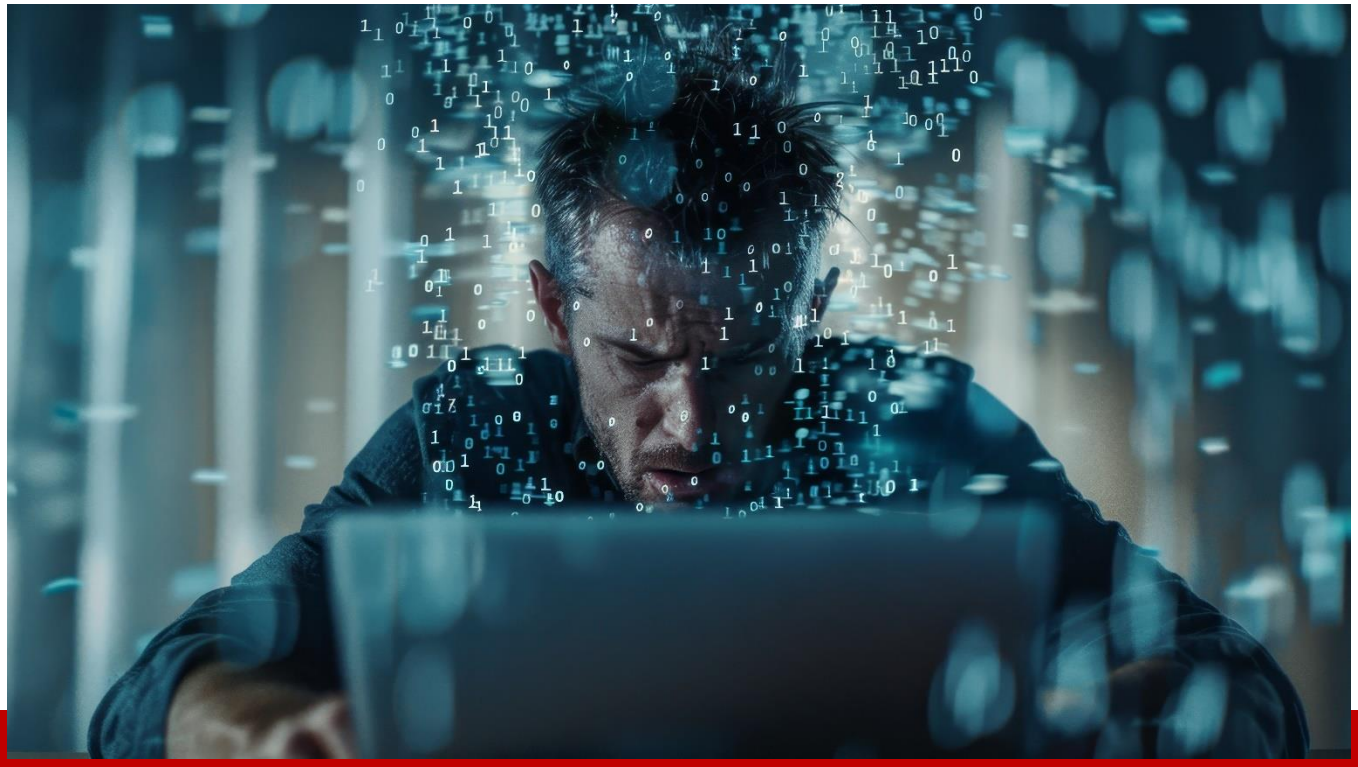
Decision-makers in organizations often believe that conducting an audit will automatically resolve identified deficiencies and that it only needs to be done once to ensure compliance with authorities. After receiving the audit reports, they are surprised to learn that further investments may be necessary (such as vulnerability assessments, penetration test or the implementation of security systems) and that after addressing the deficiencies outlined in the post-audit action plan, they will need to operate the established ISMS. It is recommended to share this information with the audited party and decision-makers even before the audit is conducted, so they are aware of what to expect in the future.

Audit experiences often reveal that organizations are not well-prepared. Ensuring mandatory compliance will pose significant challenges for certain organizations. However, conducting an audit is unavoidable if the organization wants to understand its current standing, its maturity level, and what future resource allocation will be necessary to not only achieve NIS2 compliance but also to develop adequate responses to the growing cyber threats.

About the Author

Zsolt Baranya is a Senior Information Security Auditor of Black Cell Ltd. in Hungary and Germany. Formerly, he has been in information security officer and data protection officer roles at a local governmental organization. He also worked as a senior desk officer at National Directorate General for Disaster Management, Department for Critical Infrastructure Coordination, where he was responsible for the Hungarian critical infrastructures' information security compliance. Zsolt can be reached at zsolt.baranya@blackcell.io and at his company's website https://blackcell.io/.





Deciphering End User Data Access Patterns is Key to a Strong SaaS Security Posture

Decoding User Behavior for Stronger SaaS Security

By Adam Gavish, Co-Founder & CEO, DoControl

It's all about patterns.

Long before cybersecurity was on anyone's radar, defensive intelligence - like catching an enemy spy in your ranks - was about being able to recognize patterns and interpret their meaning correctly.

Security's reliance on pattern recognition and interpretation is no less true in the age of cyber.

And nowhere is it more true than in the world of SaaS.

In SaaS, you are what you do.

In the SaaS environment, identity is a matter of access credentials.

Anyone who enters your organization's Vice President of Sales' access credentials IS the VP Sales. They will be treated as the VP Sales, given the privileges of the VP Sales, and all their actions will be attributed to the VP Sales.

When this VP Sales uses a corporate SaaS app to send you a message with a request or instructions, you can't really know whether the flesh-and-blood entity sending the message is actually the VP Sales. It could just as easily be the VP Sales' teenage daughter, a disgruntled employee who's planning to leave the company and take your best prospects with them, or worst case, a threat actor who's managed to get their hands on your VP Sales' access credentials.

Fortunately, you should have all the information you need to reveal the truth about identities and their intentions right there in your SaaS systems, as long as you know how to interpret them.

So where do you find this critical information?

In SaaS data access patterns.

SaaS application audit logs should collect information about all SaaS identities' interactions with the application and assets therein. After normalization and enrichment, they can be imported into a security tool for cross-application comparisons and analysis. The goal is to find patterns and anomalies that may indicate threats, then confirm, dismiss or address any risk.

The following represent several problematic patterns that might be brought to light by a given user's data access information. We'll identify elements of the data access pattern, note the possible conclusions and touch on potential remediations.

Profile 1: The "That's a problem?" user

One of your biggest SaaS security risks is end users who don't know enough about SaaS security risks. They're not trying to cause a data security problem; they just ARE.

What is the data access pattern you're likely to see among this end user group?

- Excessive sharing (e.g. sharing organization-wide and/or sharing publicly when there is no apparent need for it)
- Logins and logouts from locations that fit other internal users (i.e. indicating sharing of access credentials)
- Updating shared assets with sensitive information (e.g. credit card numbers, AWS keys, other secrets)
- Sharing sensitive assets externally

While many organizations have security education programs, these passive, one-time events often aren't enough to change participants' awareness and actions.

In addition to removing shares or data, the long-term mitigation for this problematic user pattern is education in real time, as a risky action is performed. Using this approach, a user attempting to share a sensitive SaaS asset with a personal email address, or to post an encryption key to a Slack channel, would receive a message informing them of and explaining the issue, and requesting them to remediate.

Profile 2: The "Oh, come on - nothing's going to happen" user

In contrast to the first problematic user described above, there are users who are very well aware of what is considered risky from a SaaS security perspective - and yet they choose to ignore that knowledge and take the risky action anyway. This user's actions are often driven by convenience, perceived invulnerability or a calculated risk assessment that undervalues the importance of security measures.

Just looking at data access patterns, it's hard to tell the difference between the user who isn't aware of SaaS security practices and the one who is aware but careless. Fortunately, mitigation is basically the same - undoing their problematic action and sending a real-time security education message - although the purpose of the message is different:

- In the case of the ignorant user, the message makes the user aware of the security principle.
- In the case of the negligent user, the message makes the user aware that their actions are being monitored for compliance with the safety principle.

Profile 3: The "Let's take advantage" user

So far, we've dealt with users who may be causing you risk, but they don't actually intend to harm your organization. Now we're going to move on to your classic malicious threat actor: the one who is out to leverage their data access for personal gain.

Data access patterns you are likely to see among this end user group include copying and/or exporting unusually large numbers of data assets, especially sensitive data assets. Searches for sensitive data types and sharing sensitive assets with private email accounts are also common indicators.

It's important to combine these data access patterns with business contextual information, such as the user's HR status or approved involvement with external parties (e.g. M&A teams). This business context reduces the risk of false positives or negatives.

In any of these "let's take advantage" user cases, the actual actor may be the real owner of the user identity in question, or they may be an external threat actor who has gotten the identity's access credentials, for example, through social engineering tactics. Business contextual information (as in the case of the departing executive) or SaaS app access information (e.g. password changes or resets) can sometimes give hints as to which one it is. In order to be sure, however, you'll probably have to take the investigation outside of your SaaS ecosystem.

Profile 4: The "They'll be sorry" user

Revenge. Retaliation. 'Righting' a 'wrong.'

Users acting out grievances are less common than the other user risk threat types. Which is a good thing, because harm to your organization is not just a byproduct of their risky actions - it's their goal.

Data access patterns you are likely to see among this end user group include deleting data assets or modifying them in a manner unexpected for that user. They may also export unusually large numbers of data assets and share sensitive data publicly.

Like the "Let's take advantage" user, business contextual information is also helpful for determining the vengeful user. The following HR data can serve as a red flag to identify users who might be harboring a grievance:

- Low performance reviews
- Termination

When it comes to mitigation, it's critical to detect and react to this user's actions rapidly, before they can carry out their intentions. Relevant mitigation actions include holding the implementation of their attempted changes (e.g. asset deletion or modification) until further investigation, revoking their access to sensitive assets or suspending their user account. The InfoSec and HR teams should be alerted as well.

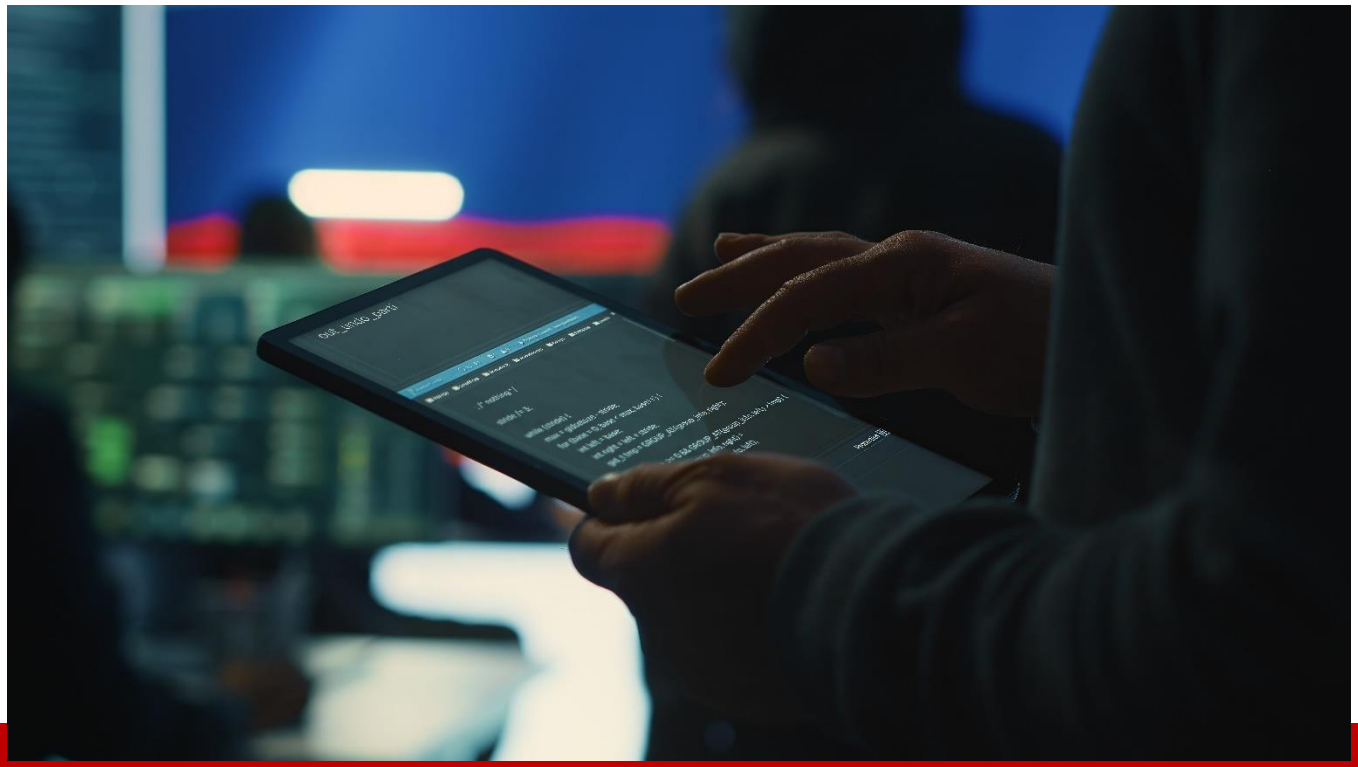
From users who are blissfully ignorant of SaaS security to users who are bent on breaking through your SaaS security - each has a distinctive footprint when it comes to their SaaS data access patterns.

The tools exist to collect data access information, analyze it and pick out those footprints. Use them wisely. Identify the patterns. Respond accordingly. You'll strengthen your SaaS security posture a hundredfold.

About the Author

Adam Gavish, Co-Founder & CEO, DoControl. Adam is a Cybersecurity Entrepreneur and Product Executive with 20 years of experience. Former member of the Google Cloud Security team. Leading a CrowdStrike portfolio company.

Adam can be reached online at https://www.linkedin.com/in/adamgavish/ and at our company website https://www.docontrol.io/.



RASP (Runtime Application Self-Protection) in Mobile Application Security: A Strategic Imperative for the Modern Threat Landscape

By Md Zaid Imam, Product Manager, Inka Networks (Appsealing)

Introduction

The mobile application landscape is more dynamic and challenging than ever, with businesses increasingly relying on mobile channels to drive customer engagement, streamline operations, and generate revenue. Yet, this rapid growth has been paralleled by a surge in sophisticated cyber threats, making traditional security measures inadequate. Enter Runtime Application Self-Protection (RASP) a disruptive technology that offers an inside-out approach to securing mobile applications.

This article examines the current standing of RASP within mobile app security, anticipates its trajectory, highlights emerging trends, and tackles the persistent challenges that hinder its broader adoption. Given the nature of the discussion, this analysis is directed at decision-makers and security strategists, including CISOs, Engineering Managers, Product Heads, and CEOs.

The Strategic Value of RASP Today

RASP has transitioned from being an experimental security layer to a critical component in the cybersecurity strategies of forward-thinking organisations. What differentiates RASP is its ability to operate within the application itself, offering real-time threat detection and mitigation based on contextual insight. This characteristic marks a departure from perimeter-based defences, which are increasingly ineffective against modern threats targeting mobile apps.

Key Capabilities Driving RASP Adoption:

1. **Contextual Defence Mechanisms**: By understanding the application's logic, RASP can differentiate between legitimate actions and malicious activities, reducing false positives that often plague other security tools.
2. **Real-time Response**: Unlike traditional security solutions that detect threats after the fact, RASP acts immediately to neutralise attacks as they happen, protecting sensitive data and maintaining application integrity.
3. **Comprehensive Protection**: RASP shields against a wide array of threats—ranging from code injection and reverse engineering to API abuse—making it a versatile tool in the mobile security arsenal.
4. **Adaptive Security**: As applications evolve through updates and new features, RASP adapts, ensuring continuous protection without requiring extensive reconfigurations.

Current and Emerging Trends

The security needs of mobile applications are shifting rapidly, influenced by technological advancements, user behavior, and regulatory pressures. Several trends are poised to reshape the application security landscape, with RASP playing a pivotal role.

1.The Rise of API-Centric Security:

- As mobile applications increasingly rely on APIs for functionality, securing these endpoints has become critical. RASP solutions are evolving to include API-specific protections, such as anomaly detection and abuse prevention, ensuring that the entire application stack is fortified.

2.Shift from Reactive to Proactive Security:

- The traditional reactive approach to security is no longer sufficient. Organizations are adopting proactive security measures, embedding RASP into the early stages of the development lifecycle (Shift Left Security). This integration ensures that vulnerabilities are identified and addressed long before they can be exploited.

3.Convergence with DevSecOps:

- The merging of development, security, and operations is driving the demand for automated, continuous protection solutions. RASP fits perfectly within this paradigm, offering real-time protection without slowing down the development pipeline.

4.Regulatory Pressures and Compliance:

- With data breaches and privacy violations becoming more frequent, regulatory bodies are imposing stricter compliance requirements. RASP solutions that offer robust audit trails, real-time monitoring, and detailed reporting will be indispensable for organizations aiming to meet these standards.

Challenges and Roadblocks

Despite the clear benefits, RASP adoption is not without challenges. These obstacles range from technical hurdles to organizational inertia and market misconceptions.

1.Performance Concerns:

- The primary criticism of RASP solutions is the potential impact on application performance. While modern RASP tools are designed to minimize overhead, performance trade-offs remain a consideration, especially for resource-constrained mobile environments.

2.Complexity of Implementation:

- Integrating RASP into mobile applications can be complex, particularly for legacy systems. Ensuring seamless integration without disrupting existing workflows or introducing new vulnerabilities requires careful planning and expertise.

3.Balancing Security with User Experience:

- As mobile applications become more central to user engagement, any security measure that negatively impacts the user experience is likely to face resistance. RASP providers must continue to refine their solutions to ensure that security enhancements do not come at the expense of usability.

4.Market Education and Awareness:

- RASP is still a relatively new concept in the broader security market. Many organisations are unaware of its capabilities or misunderstand its role within the larger security ecosystem. Addressing this knowledge gap is crucial for driving wider adoption.

Threat Landscape: A Shifting Battlefield

The threats targeting mobile applications are becoming increasingly sophisticated, driven by the convergence of multiple factors such as the proliferation of mobile devices, the rise of cloud computing, and the growing reliance on mobile applications for critical business functions.

1.Sophisticated Malware and APTs:

- Advanced Persistent Threats (APTs) targeting mobile environments are becoming more common, often leveraging zero-day vulnerabilities. RASP solutions must stay ahead by integrating advanced threat intelligence and adaptive response mechanisms.

2.Supply Chain Vulnerabilities:

- The reliance on third-party components in mobile applications introduces significant risk. Recent high-profile breaches have highlighted the vulnerabilities within the software supply chain, making it imperative for RASP solutions to extend protection to all application dependencies.

3.Insider Threats:

- Insider threats, whether through malicious intent or inadvertent actions, continue to pose a significant risk. RASP solutions need to include capabilities for monitoring and responding to insider activities that could compromise the security of mobile applications.

4.Polymorphic Attacks:

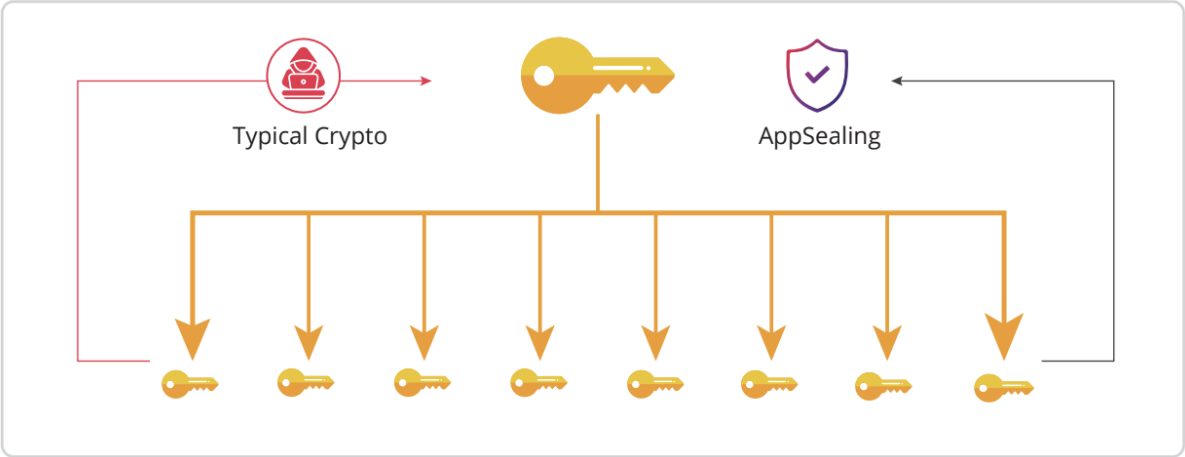
- Attackers are increasingly using polymorphic techniques to evade detection, altering the code with each iteration to avoid signature-based defenses. RASP solutions must incorporate behavioral analysis to detect these evolving threats.

How AppSealing Leads From the Front

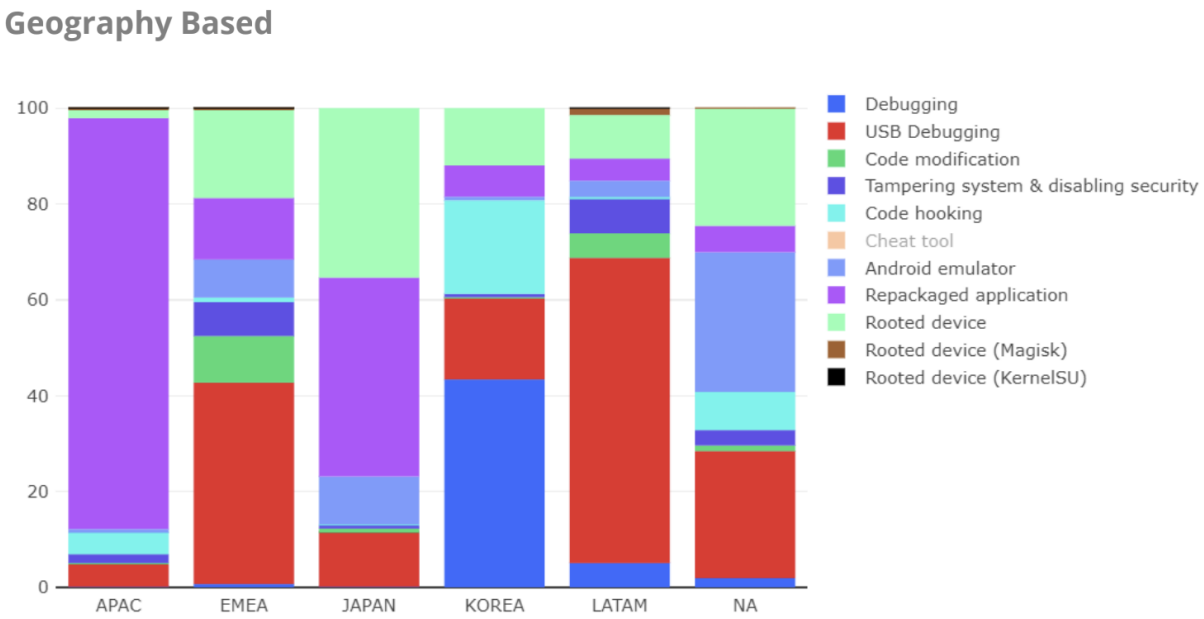
- No Coding/No SDK app security
- Efficient Memory Usage and High Encryption Speed
- Data security and app security in a single workflow
- Saas and On-prem solution
- Covers all 50+ runtime app security features
- Real-time threat analytics dashboard

AppSealing prevents abnormal execution of the app, such as running in a debugger environment. However, more fundamentally, white-box cryptography is used to prevent the exposure of keys for encrypting or decrypting crucial data even in situations where white-box attacks are possible. While various papers have proposed methods to implement the standard block cipher AES as a white-box

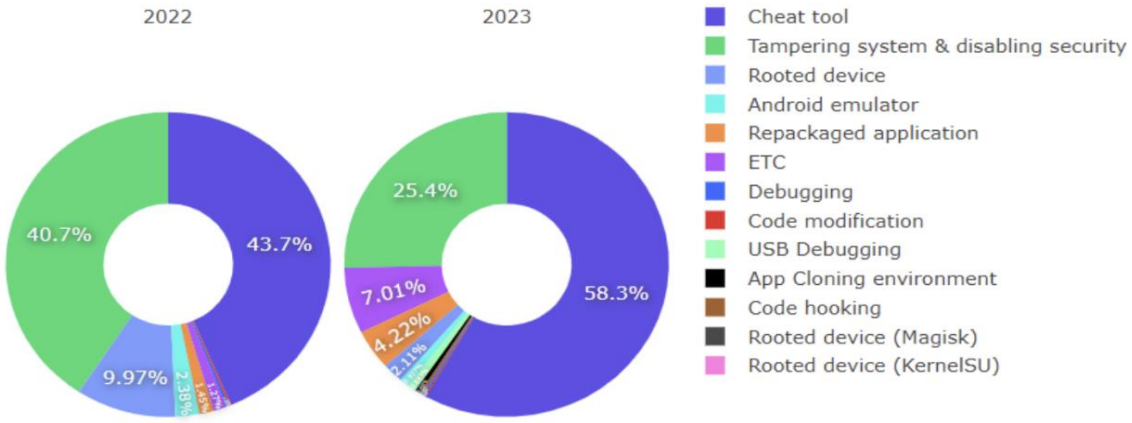
cryptography, all of them have been susceptible to attack methods. Alternatively, AppSealing has implemented the standard block cipher LEA as a white-box cryptography through modification.



Many white-box cryptography implementations adopt a key dispersion method that relies on extensive tables, resulting in substantial memory consumption. Additionally, the frequent referencing of tables in such implementations can lead to a decline in performance. For instance, the method proposed by Chow et al. (2003), a notable white-box cryptography implementation for AES, employs approximately 750 kB of tables and requires over 3,000 table lookups to encrypt a single block. The exceptional performance of AppSealing's white-box cryptography ensures quick operation of various AppSealing features, minimizing any adverse effects on the app's execution.



(All Data in millions)



Directions: The Next Frontier for RASP

As the mobile threat landscape evolves, so too must the capabilities of RASP solutions. The future of RASP will likely be defined by its ability to integrate with cutting-edge technologies, offer cross-platform consistency, and provide deeper insights through data-driven approaches.

1.AI and Machine Learning Synergies:

- **Predictive Threat Analytics**: AI-powered RASP solutions will enhance predictive capabilities, identifying attack patterns before they fully manifest. This proactive defense will be crucial as cyber threats become more adaptive and persistent.
- **Behavioral Analysis**: Machine learning models trained on vast datasets will enable RASP to recognize subtle deviations in user and application behavior, providing early warnings for potential breaches.

2.Enhanced Privacy Protections:

- As regulations around data privacy tighten globally, future RASP solutions will incorporate advanced cryptographic techniques to ensure compliance without compromising on security.

3.Seamless Multi-Platform Support:

- As development frameworks increasingly support cross-platform deployment, RASP solutions must offer uniform protection across different environments, whether native or hybrid, without adding complexity.

4. Integration with Broader Security Architectures:

- Future RASP tools will be designed to work in concert with Zero Trust frameworks, ensuring that mobile applications remain secure within the broader context of enterprise-wide security strategies.

Conclusion

As mobile applications become the linchpin of digital transformation strategies, securing them is no longer optional—it's a strategic imperative. RASP stands out as a powerful tool in the security arsenal, offering real-time, context-aware protection that adapts to evolving threats. However, its success depends on overcoming key challenges such as performance trade-offs, complexity of implementation, and market education.

Looking ahead, the future of RASP will be shaped by its ability to integrate with AI, deliver cross-platform consistency, and enhance privacy protections while remaining agile in the face of emerging threats. For CISOs, Engineering Managers, Product Heads, and CEOs, understanding and leveraging RASP is crucial to safeguarding not only their mobile applications but also the broader ecosystem in which these apps operate. As the mobile threat landscape continues to shift, the strategic deployment of RASP will be critical in staying ahead of adversaries and ensuring the resilience of digital assets.

About the Author

Md Zaid Imam is Product Manager of the INKA NETWORKS (AppSealing). With over 7+ years in product management, he has extensive expertise in cybersecurity, specifically in Bot Mitigation & Protection, API Security and Mobile Application Protection. Currently Heading Product at AppSealing that provides RASP for Mobile Application, before this he worked with ShieldSquare since inception and later joined Radware as part of acquisition. Zaid submitted a patent (pending) around the CAPTCHA solution during his Radware tenure.

Zaid can be reached online at https://www.linkedin.com/in/zaidimam101/ and at our company website https://inka.co.kr/.

Have the Last Word Against Ransomware with Immutable Backup

“It’s never going to happen to me.” famous last words

By Judy Kaldenberg, SVP Sales and Marketing at Nexsan

With incidences of ransomware on the rise, nobody should even be thinking that an attack is something that couldn’t happen to them, let alone speak those words into existence. And for organizations that believe a breach couldn’t happen to them because they store their data in the cloud are burying their heads in the sand.

All companies are vulnerable to ransomware. According to analyst estimates, cybercriminals were able to extort more than $1 billion in cryptocurrency payments from victims in 2023. What may have been a simple operational interruption 5 years ago has ballooned into millions of dollars per incident, loss of business reputation and a mystery as to how long it will take to return to viability.

Standard approaches to data security are no longer the answer

Even more disturbing is that ransomware attacks today have become more sophisticated than the “smash and grab” variety of the past. What was once regarded as a way to win a quick score has become

increasingly sophisticated, with cybercriminals content to play a waiting game to find out what data is important, which files are being accessed the most and gaining access to passwords.

Typically, organizations would utilize a system of various storage, snapshots, replication, and backup to ensure business continuity. But because this has become such a standard approach, cybercriminals have begun targeting these systems to ensure greater success at securing a payday.

Ninety-three percent of ransomware attacks today target backups. These backups are being turned off, erased and encrypted. Seventy-five percent are successful in preventing recovery and forcing payment. In addition to impacting operations, successful attacks lead to additional penalties for companies in industries that must protect personal information due to industry compliance and legal requirements.

Having your head(ache) in the cloud

In an ever-increasing automated world, the ever-increasing shift to the cloud makes sense. Public clouds offer a plethora of benefits for organizations. Costs are shifted from upfront hardware purchases that will hopefully satisfy future capacity demands to only paying what is used as it is used. Scalability is easy. IT personnel can be utilized on tasks that directly support the business with managed cloud providers doing all the heavy lifting. One thing that it is not necessarily better at – despite the proclamations – is improved security.

Data is only as secure as employees at a company or at the cloud provider make it. The challenge of the cloud for financial organizations under SEC regulations or medical providers that must contend with HIPAA requirements is that data saved to the cloud is out of their control. There are plenty of instances where cybercriminals gain access to data stores because of human error. To what degree of accountability do cloud providers truly offer their customers? What happens when a cybercriminal gains passwords to a company's Microsoft Azure store or their AWS account? And to what degree are cloud providers made accountable for breaches that result in material loss?

Backups should be protected on an immutable platform

Vulnerabilities are almost certain to occur in any software, hardware or firmware release – including cloud providers' infrastructures as well. Though not a malicious attack, the recent CrowdStrike outage shows how widespread a disastrous event can be when it occurs as part of a cloud-native platform despite assurances that cybersecurity procedures are in place.

Well, if there are vulnerabilities everywhere, is everyone simply out of luck? Not so fast. Safeguarding a company's most valuable asset – their data – remains paramount despite the obstacles. Especially as data volumes continue to expand at an unprecedented rate. The challenge therefore is to manage growth while minimizing technological and/or human error to ensure data protection.

The primary goal of backup processes is to guarantee the ability to recover from any data loss or system failure within a predetermined timeframe. This necessitates a robust backup strategy involving automated

processes across various applications, platforms and virtual environments. In the face of increasing ransomware threats, immutable storage has become a vital feature.

Rather than placing all of one's proverbial eggs into a single basket, organizations can strengthen their data storage protection through a hybrid cloud approach that leverages the benefits of the full cloud with the control and security of on-premises solutions. There are several options for ransomware protection including immutable snapshots, S3 object-locking and platforms that provide unbreakable backup. Such solutions offer immutable storage that keeps backup data safe from ransomware attacks, accidental deletions or silent data corruption, while ensuring that backup data remains unaltered and recoverable to provide businesses a reliable defense against evolving cybersecurity threats.

Conclusion

There are many benefits to moving to the cloud – from saving money, to easy scalability and greater reliability – for both IT and end users than on-premises infrastructure. However, security is not one of those benefits. Ransomware has evolved to the point where it is no longer a "will I get hit?" scenario but rather a "when I get hit" one. And, unfortunately, companies rarely see it coming.

For businesses looking for better security of their data, having an immutable backup solution as either a standalone or as part of a hybrid cloud is a more attractive option. This is especially true for organizations with extremely sensitive information, such as healthcare or financial institutions. It can also be ideal for organizations that must comply with regulations that aren't met by public cloud providers.

Want to have the last word in guaranteeing the safety, security and immediate availability of invaluable data? Ignore the public cloud and instead implement an immutable solution that provides the data integrity, ransomware defense, compliance and legal requirements, and historical data preservation that is needed to tell cybercriminals that they are wasting their time.

"That's all, folks!"

About the Author

Judy Kaldenberg has been Championing Channel-Driven Data Storage and Ransomware Defense for many years. Her expertise encompasses all aspects of product and channel marketing with extensive experience in charting out sales strategies and contributing towards enhancing business volumes and growth. Prior to working for Nexsan, she held management positions at Kodak Alaris, Avtex Solutions LLC, The MACRO Group Inc., ACS Incorporation, Gauss Interprise, Optika, and Eastman Kodak Company.

Judy can be reached online at info@nexsan.com and at our company website https://www.nexsan.com/.

Maximizing Security Through Hardware

A Case for Hardware Security Key Deployment Throughout an Organization

By Joe Loomis, Marketing Director, CryptoTrust LLC

Organizations are continually balancing seamless user experiences and implementing robust defenses against evolving threats. Passwords, as the first line of defense, remain a primary vulnerability, often exploited due to poor password management practices. While some multi-factor authentication (MFA) methods and password managers have become common practice, they remain insufficient in countering the sophisticated techniques used by advanced adversaries. Hardware security keys are an underutilized tool that offers substantial improvements in fortifying an organization's defenses against unauthorized access without increasing the burden on end users.

This article delves into the inherent weaknesses of current password management methods and explores how the integration of security keys, either as standalone tools or in conjunction with software password managers, can significantly enhance an organization’s defense-in-depth strategy.

The Pitfalls of Current Password Management Practices

Despite advancements in cybersecurity awareness, many organizations still rely heavily on traditional password-based authentication methods. Unfortunately, common password management practices are fraught with vulnerabilities, leading to breaches that can severely compromise an organization's data integrity.

1. **Weak and Reused Passwords:** Many employees, overwhelmed by the sheer number of accounts and passwords they need to manage, often resort to creating weak passwords or reusing the same ones across multiple platforms. This practice leaves critical systems vulnerable to credential-stuffing attacks, wherein compromised credentials from one platform are used to gain access to others.
2. **Phishing Attacks:** Phishing remains one of the most effective methods for attackers to acquire user credentials. Despite extensive training and awareness campaigns, employees are frequently duped into entering their credentials into fake websites, providing attackers with a direct route into organizational systems.
3. **Password Sharing and Management:** Shared credentials within teams can lead to significant security risks, especially when employees leave the organization or when credentials are stored in insecure locations, such as spreadsheets or emails. This lack of proper management leads to unsecured access points for potential attackers.
4. **Compromise of Centralized Password Managers:** While password managers are a popular tool for improving security, they represent a central point of failure. If an attacker can compromise a password manager, they gain access to all stored credentials, leading to a cascade of breaches. For organizations relying solely on software-based password managers, this presents a significant risk.

Given these issues, relying solely on traditional password management practices exposes organizations to considerable risks. A more robust solution is needed—one that significantly reduces the attack surface while enhancing the overall security posture. This is where security keys enter the equation.

What Are Security Keys?

Security keys are hardware-based devices that provide an additional layer of authentication, often referred to as hardware-based multi-factor authentication (MFA). Unlike software-based MFA methods, such as SMS codes or app-generated tokens, security keys are resistant to phishing, man-in-the-middle (MITM) attacks, and other forms of credential theft. These keys work by using cryptographic protocols to verify the identity of the user and the legitimacy of the website or system they are accessing, without ever exposing sensitive information.

Security keys are typically based on open standards, such as FIDO2, Universal 2nd Factor (U2F), or WebAuthn, making them compatible with a wide range of platforms and services.

The Case for Implementing Security Keys

By integrating security keys into the authentication process, organizations can mitigate many of the vulnerabilities associated with password-based systems and centralized password managers. Here are several use cases where security keys can enhance cybersecurity within an organization:

1. Phishing-Resistant Authentication:

Phishing attacks often succeed because users inadvertently enter their credentials into fraudulent websites. Security keys eliminate this risk by using cryptographic authentication that ties the login attempt to the legitimate website or application. Even if an employee is tricked into clicking on a malicious link, the security key will not transmit any authentication data unless the legitimate domain is matched.

Use Case: Employees who regularly access sensitive systems, such as email or cloud storage platforms, are prime targets for phishing attacks. Requiring a security key as part of their login process ensures that they can only authenticate with the genuine service, significantly reducing the likelihood of credential theft.

2. Further Protection Against Credential Theft:

Unlike passwords, which can be stolen, shared, or guessed, security keys store cryptographic sequences that are never exposed to the user or to attackers. When a login attempt is made, the security key creates a unique cryptographic signature that can only be verified by the legitimate service, rendering stolen passwords or credentials useless.

Use Case: For high-privilege accounts, such as those belonging to system administrators or executives, the use of a security key provides an additional layer of protection. Even if an attacker manages to obtain the account's password, they will not be able to log in without the physical security key.

3. Securing Password Manager Access:

While password managers offer convenience by securely storing credentials, they are not immune to attack. A compromised password manager could give an attacker access to all of a user's stored credentials. Security keys can be used to protect access to the password manager itself, ensuring that even if a user's password is compromised, the attacker cannot gain access to the stored credentials without the security key.

Use Case: Employees can use a security key to authenticate into their password manager, requiring two layers of security (password + key) to access their stored credentials. This greatly reduces the risk of credential exposure in the event of a password manager compromise.

4. Defense-In-Depth for Critical Systems:

For systems that are especially critical to an organization's operations, such as financial systems, proprietary applications, or cloud environments, a defense-in-depth approach is crucial. Security keys can be integrated as an additional layer of authentication on top of existing MFA methods, ensuring that even if an attacker compromises one layer, the security key provides an additional barrier.

Use Case: A security key can be required for accessing sensitive financial systems or proprietary business applications, particularly in industries where regulatory compliance mandates stronger authentication methods. For example, in the healthcare or finance sectors, security keys can provide the extra assurance needed to protect sensitive data.

5. Access Control for Physical Devices:

Security keys are not just limited to online services—they can also be used to authenticate access to physical devices, such as laptops, workstations, or network equipment. By requiring a security key to log in to these devices, organizations can ensure that only authorized personnel can access critical infrastructure.

Use Case: System administrators who manage sensitive network infrastructure, such as servers or routers, can be required to use a security key to authenticate their logins. This adds an extra layer of security, ensuring that only individuals with physical possession of the security key can access the devices.

Best Practices for Security Key Deployment

To ensure a successful implementation of security keys across an organization, CISOs must carefully plan the deployment process. Here are some best practices to consider:

1. **Identify Critical Systems and Users:** Not all systems or users require the same level of security. Begin by identifying the most critical systems (e.g., financial systems, proprietary applications) and users (e.g., administrators, executives) who would benefit most from security key implementation.
2. **Integrate Security Keys with Existing Systems:** Many systems, such as cloud services, identity management platforms, and password managers, already support security key authentication via FIDO2 or WebAuthn. Ensure that your existing systems can integrate seamlessly with security keys, and consider upgrading or replacing systems that do not support modern authentication methods.
3. **Use Security Keys in Conjunction with Password Managers:** Password managers are a valuable tool for improving password security, but they are not foolproof. Encourage employees to use security keys to protect access to their password managers, ensuring that even if a password is compromised, the security key provides an additional layer of protection.

4. **Educate Employees on Security Key Usage:** While security keys are highly effective, they may require a cultural shift within the organization. Ensure that employees are trained on how to use security keys properly and provide clear guidelines on when and where security keys are required.
5. **Implement Redundancy:** Since security keys are physical devices, there is a risk of them being lost or damaged. Ensure that employees can restore their security key data via encrypted backups and that your keys have a mechanism for erasing their data if physically compromised. For sustainability, choose a model that hosts upgradeable firmware to keep it current without the need for outright replacement.

Security keys offer a powerful, phishing-resistant solution that can enhance the security of password-based systems, protect against credential theft, and provide an additional layer of authentication for critical systems and high-privilege users.

By integrating security keys into a defense-in-depth strategy, organizations can significantly reduce their exposure to future cyber threats and strengthen their overall security posture. For CISOs, this implementation represents a valuable opportunity to stay ahead of the limitations of traditional password management practices, creating resilient organization-wide defense systems.

About the Author

Joe Loomis is the Marketing Director for CryptoTrust LLC. He has served in the U.S. Navy as an Information Systems Technician running shipboard network security overseas. Having started and operated several businesses in other fields, he now takes his entrepreneurial passion to the cybersecurity field through writing and content creation. Joe can be reached online at joe@onlykey.io and at our company website https://www.onlykey.io.

Confronting the Ransomware Menace: A Critical Look at Payment Practices and Emerging Strategies

By Usman Choudhary, general manager, VIPRE Security Group

Ransomware attacks remain a significant threat to organizations worldwide, with cybercriminals continuously evolving tactics. Despite long-standing advice from cybersecurity experts against paying ransoms, many businesses still opt to pay, hoping for the safe return of their data. However, this approach often fails and perpetuates the cybercrime cycle, increasing calls for making ransom payments illegal.

Recent data indicates a positive shift: only 34% of organizations now pay ransoms, marking an all-time low. This suggests that nearly two-thirds of targeted businesses refuse to succumb to attackers' demands. While this decline is encouraging, the goal is to reduce ransom payments further.

However, when organizations pay the ransom, they reinforce to bad actors that their tactics are working. Thus, the attacks will continue as the actors, confident in their ability to extort money from victims, continue their efforts. Paying also increases the chances of repeat attacks, marking the organization as an easy target for future extortion.

Paying up is no guarantee that the encrypted data will be restored. Attackers often provide fake decryption keys, demand more money, or simply vanish without fulfilling their promises. This leaves companies worse off, losing their data and money.

Despite the warnings, organizations are still paying. As of this writing, reports indicate that Panera Bread, a US-based restaurant chain, paid a ransom in March. The much-publicized ransomware attack in which Change Healthcare paid a reported $22 million has led to a deluge of similar attacks against other healthcare organizations—more than at any time in the past.

The rationale for paying ransoms is often driven by the urgent need to restore access to critical data. However, cybersecurity professionals strongly advise against this practice, advocating instead for a comprehensive, layered cybersecurity strategy to prevent ransomware attacks from succeeding in the first place. Paying a ransom does not guarantee restored access to data or even quick access to locked data.

To Pay or Not to Pay

Some experts and regulatory bodies propose making ransom payments illegal to deter ransomware attacks. The logic is straightforward: if no one pays, the financial incentive for cybercriminals disappears. Although 34% of targets still pay ransoms, eliminating this option could significantly reduce the profitability of ransomware attacks, discouraging cybercriminals.

Implementing a ban on ransom payments poses immediate challenges for businesses, which may find it difficult to combat ransomware without the option to pay. Recognizing these challenges, the International Counter Ransomware Initiative (ICRI) suggests governments and institutions could provide financial aid and resources to support affected organizations, fostering a collaborative approach to mitigating ransomware risks.

If these initiatives fail, cyber insurance remains a vital option for protecting an organization from the financial loss of such attacks. Cyber insurance politics cover ransomware payments under strict conditions that require insurance approval before any payment is made.

In such instances, insurers can create a lot of red tape, and payment is offered only when all mitigation strategies are exhausted. In such cases, law enforcement involvement is mandated, establishing clear protocols for collaboration during ransomware incidents. While such policies are a proactive measure to reduce financial loss, the legwork to collect on the claim is copious.

Another problem with these policies is that they limit the loss to the policyholder through capped amounts. A policy with a $100,000 limit may not cover ransom demands exceeding this amount, leaving the attacked organization to cover any cost overruns.

Email: Primary attack vector

Ransomware primarily infiltrates systems through email, with 66% of infections stemming from phishing emails and scams targeting unsuspecting employees. As attackers become more sophisticated, they employ tactics such as malicious links, attachments, and QR codes to deploy ransomware. Organizations must educate their staff to recognize these threats and implement robust cybersecurity measures.

Proactive threat detection is necessary in the fight against ransomware. Research from VIPRE Security has found that of more than 7 billion processed emails, as many as 13% were identified as malicious.

Advanced email security systems have been pivotal in identifying and protecting against these threats.

One notable feature is the ability to isolate and analyze links within emails, which has protected users from millions of potentially dangerous clicks. Technology advancements have enabled the detection of nearly half of all malicious emails through content analysis and the other half through link detection.

Further illustrating the sophistication of modern threats, millions of emails have been flagged for malicious attachments, and advanced behavioral analysis has identified numerous never-before-seen threats. Tools that analyze webpage behavior have been particularly effective, ensuring real-time protection without lag.

Implementing rules to detect statistical patterns and indicators related to malware families has also been highly effective. These measures have captured millions of generic malware instances each quarter, with a notable increase in detection towards the end of the year.

Conclusion

The battle against ransomware involves preventive measures, legislative action, and strategic insurance policies. Integrating advanced email security solutions and proactive threat detection further strengthens defense mechanisms.

While the reduction in ransom payments is a positive sign, ongoing efforts are essential to diminishing the threat further. Organizations can better protect themselves against this persistent menace by fostering robust cybersecurity practices, considering legal frameworks against ransom payments, and leveraging cyber insurance.

About the Author

Usman Choudhary is general manager of VIPRE Security Group. You can learn more about VIPRE at https://vipre.com/.

Complexity: The Silent Killer of Cybersecurity

By Jaye Tillson, Field CTO, Distinguished Technologist, HPE Aruba Networking

The cybersecurity landscape is a complex and ever-evolving ecosystem. At its core lies a fundamental paradox: the more tools we deploy to protect our digital assets, the more complex and vulnerable our security posture becomes. This is a challenge faced by security teams worldwide, but it's particularly acute for Chief Information Security Officers (CISOs).

The average CISO juggles a staggering array of security tools – often more than 75 – sourced from a multitude of vendors. Each tool comes with its own unique management interface, update schedule, and potential vulnerabilities. This creates a patchwork quilt of security, where gaps can easily emerge, and threats can slip through undetected. The complexity inherent in managing this sprawling toolset is a significant drain on resources, hindering the team's ability to focus on strategic initiatives and proactive threat hunting.

Studies show that the average number of security tools deployed by organizations has increased by 30% in the past 3 years. This proliferation of tools has led to a corresponding increase in security complexity and operational costs.

Moreover, the different patching and replacement cycles associated with these tools introduce another layer of complexity. Ensuring that all tools are up-to-date with the latest security patches is a daunting

task, requiring meticulous planning and coordination. A single overlooked patch can become a critical vulnerability, inviting cybercriminals to exploit the gap.

This overreliance on such a wide array of tools is counterintuitive to the goal of creating a secure environment. It can inadvertently increase risk. The more tools in place, the greater the likelihood of overlapping functionalities, redundant efforts, and increased operational costs. Additionally, the sheer volume of alerts generated by these tools can lead to alert fatigue, desensitizing security teams to genuine threats.

Experience tells us that a significant amount of security alerts are false positives, leading to wasted time and resources. This highlights the challenge of managing the sheer volume of data generated by modern security tools.

Recognizing this issue, CISOs are increasingly prioritizing consolidation. The trend is clear: fewer vendors, better security. This shift is driven by the desire to simplify operations, reduce costs, and improve overall security posture. However, this is not a new aspiration. IT and security teams have long sought to streamline their toolsets, but the technology simply hasn't been mature enough to support such a consolidation.

The tide is finally turning. Advances in technology, particularly in the areas of cloud computing, artificial intelligence, and automation, are making it possible to achieve the long-sought-after goal of a consolidated security stack. Cloud-based platforms offer the scalability and flexibility needed to integrate disparate security functions into a unified solution. AI and automation can streamline processes, reduce manual intervention, and improve threat detection capabilities.

Forrester has predicted that by 2025, 50% of organizations will have adopted a consolidated security platform. This trend is being driven by the increasing complexity of the threat landscape and the need for more efficient and effective security operations.

Zero trust architecture is another key driver of this trend. By shifting the security perimeter from the network to the individual user, zero trust necessitates a more centralized and integrated approach to security. This architectural shift aligns perfectly with the goal of consolidating security tools. By adopting a zero trust framework, organizations can reduce their reliance on traditional perimeter-based security controls and replace them with more granular, identity-centric protections.

In conclusion, the complexity of modern security environments is a major obstacle to effective threat management. CISOs are leading the charge in addressing this challenge by consolidating their toolsets and moving towards fewer vendors.

While this has been a long-standing desire, recent technological advancements are finally making it a reality. By simplifying their security stacks and embracing emerging technologies like cloud, AI, and zero trust, organizations can significantly enhance their security posture and better protect their valuable assets.

About the Author

Jaye Tillson, Field CTO and Distinguished Technologist – Security at HPE, brings over 25 years of invaluable expertise in successfully implementing strategic global technology programs. With a keen focus on digital transformation, Jaye has been pivotal in guiding numerous organizations through their zero-trust journey, enabling them to flourish in today's dynamic digital landscape.

His passion lies in collaborating with enterprises, aiding them in their strategic pursuit of zero trust. Jaye takes pride in applying his real-world experience to tackle critical issues and challenges faced by these businesses.

As a renowned expert in the field, Jaye has showcased his thought leadership at prestigious industry conferences such as Gartner, VMWorld, Evanta, IDC, and Next. Further validating his expertise, he participates on advisor boards for leading companies including VMware, Nutanix, CIOnet, and Proofpoint.

Jaye is also the co-founder of the SSE Forum and co-host of its popular podcast, 'The Edge,' where he delves into topics such as cybersecurity, the role of the CISO, SASE, SSE, and Zero Trust. This platform allows him to engage with a wider audience, fostering meaningful discussions on industry trends and innovations.

Additionally, Jaye actively contributes as a member of the CSA Zero Trust Working Group, serves as a board member of the CSA UK Chapter, and acts as an Advisor for Infosec.live. For more information, visit his website at https://jayetillson.tech.

How Amazon Prime Day Scams Are Getting Smarter and How Can You Protect Yourself

By Efrat Tabibi, Head of Data Science & Analytics at Guardio

Amazon Prime Day has become a major shopping event, with 2023 setting a record as customers purchased over 375 million items worldwide, up from 300 million in 2022. As more people rush to find deals, scammers are using increasingly advanced tactics to exploit unsuspecting consumers.

What's Different This Year?

The use of AI has significantly changed how scams are created and deployed. Tools like ChatGPT have seen explosive growth, reaching 100 million users in the first couple of months after launch — the fastest-growing consumer application in history. This widespread use of AI tools allows scammers to craft highly convincing emails, fake websites, tones of voice and even deepfake videos that closely mimic legitimate communications. In the first half of 2024 alone, there has been a notable increase in AI-powered scams, such as voice cloning and deepfakes, which impersonate trusted organizations or individuals with unprecedented accuracy.

And it’s not just about mimicking Amazon anymore. Scammers are expanding their targets to include other trusted names such as USPS, Temu and SHEIN. With 54% of Prime Day shoppers comparing prices across multiple retailers before purchasing, scammers see an opportunity to deceive across different platforms, knowing that consumers are less suspicious when they recognize a brand.

Amazon's Package Volume and USPS's Role:

Amazon’s logistics operations have expanded significantly, and in 2023, the company surpassed UPS in U.S. parcel volume, marking a major shift in the delivery landscape. Despite Amazon's growing in-house capabilities, it still relies heavily on USPS for a substantial portion of its deliveries, especially for last-mile services. USPS handled millions of Amazon packages, particularly in rural and remote areas, where its delivery network reaches every address in the U.S. In 2023, U.S. parcel volumes reached 21.65 billion shipments, with USPS playing a crucial role in handling a significant portion of these parcels.

Given USPS's extensive involvement in deliveries, it has become a prime target for scammers. In Q1 and Q2 of 2024, USPS was one of the most frequently imitated brands in phishing scams, as scammers created fake notifications and impersonated its services to trick consumers. Scammers have used this association to craft phishing emails that look like official USPS notifications, including fake tracking updates or delivery failure alerts, exploiting the trust consumers have in USPS.

What Can the Public Do About It?

Traditional Methods Aren’t Enough:

Hovering over a link or checking the sender’s email might have been enough in the past, but today's AI-powered scams are designed to bypass these simple checks. Fake websites can appear high in search engine rankings, so searching for a company's name directly might still lead you to a scam.

Take Safer Actions:

The safest way to check your orders or get customer support is through the official app or by typing the URL directly into your browser. Avoid clicking on links from emails or text messages, even if they appear to come from a trusted source. Scammers are skilled at creating urgency to make you click without thinking.

Utilize Advanced Security Tools:

As the human eye is no longer sufficient to detect today’s sophisticated scams, security tools that provide real-time protection can help detect phishing attempts, block malicious websites and warn you about potential scams before they reach people. As scammers continue to evolve their tactics with AI, having this extra layer of security is crucial.

The reality is simple: as scams become more sophisticated, so must the public’s defenses.

About the Author

Efrat Tabibi is the Head of Data Science and Analytics at Guardio. With over 10 years of experience in data analysis and cybersecurity, Efrat leverages her extensive knowledge to protect users from online threats. Efrat can be reached online at our company website https://guard.io/.

The Multi-Layer Complexity of Cybersecurity for The Automotive Supply Chain

By Austen Byers, Technical Director, Americas, TXOne Networks

Thousands and thousands of components go into the assembly of contemporary vehicles. It is impossible for any original equipment manufacturer (OEM) to produce all these components themselves. The demand for just-in-time delivery and customization for all these parts has created a huge, unusually integrated supply chain.

If even one supplier experiences a cybersecurity breach, the impact can be exponentially damaging for the automotive industry. The weeks of plant downtime not only cause huge production losses for that supplier, but it also creates a ripple effect impacting production and supplier relations further down the chain. Not to mention, the entire supply chain could be exposed to a devastating cyberattack. Most important of all is the potential to jeopardize human safety.

Unfortunately, there are gaps in operational technology (OT) cybersecurity that are growing more common in the manufacturing process of the automotive supply chain. The introduction of increasingly

innovative and powerful systems in the plants, as well as more connectivity across and beyond the vehicles themselves, is widening the gaps.

Plant and security managers are often stunned to discover the range of vulnerabilities that exist under their watch. What actionable steps can they take to make definitive and quick progress in closing the gaps and ensuring protection from supply chain threats?

Automotive manufacturers cannot afford to be merely responsive to cybersecurity events or new regulations that come their way. They need a proactive and practical approach forward to ensure uninterrupted operations and revenues.

Surprisingly Common Security Gaps

The OT environments for most companies in the supply chain are complex and untouchable with a mentality of "if it isn't broken, don't fix it." Many of today's automotive plants contain a variety of hardware and software systems with widely differing ages, operating systems (OSs), and capabilities.

For example, some of the robotic technologies that are being installed in the plants are among the most modern and innovative industrial control systems (ICSs) found in any manufacturing sector globally. They rely on new OSs, which require different patching and firmware levels.

Step over to the next production line in the same plant, and it's common to find assets that are decades old. While such a legacy system could be critical for the manufacturing process, it might still be running an old OS that is no longer being updated or patched by its vendor.

Responsibility for OT maintenance and cybersecurity in the manufacturing process of the automotive supply chain usually falls to traditional information technology (IT) network or OS support. As a result, there is often literally no one who is directly responsible for what is getting plugged into the OT network on the floor. Furthermore, because there is not often a strong relationship between the different worlds, very minimal OT knowledge resides on the IT side of expertise, or vice versa.

The automotive manufacturer is often under the dangerous misperception that both its IT and OT networks are being secured—when, in fact, the company does not have nearly the visibility to protect its own OT processes, much less those of its connected vendors and partners. Indeed, it is usually an OEM's Tier 1 and Tier 2 suppliers whom cyber attackers target in the automotive industry.

Actionable Steps to Seize Control

How can an automotive manufacturer gain visibility across its OT landscape and begin to put in place practical and effective processes? The good news is that there are key strides that can be made in short order to get out in front of the evolving challenges that they will face in the months and years ahead:

- Walk the plant floor and open the cabinets—The first step is often the most eye-opening. Plant personnel and support vendors will do what they need to do in order to get a system up, running

and connected, including remote access points. Often, in the wake of that process, there are wide-open, unsecured internet connections left behind into the manufacturer's network.

- Shore up and lock down—It is crucial to adopt a solid security practice around the maintenance routine across the asset lifecycle of existing equipment and to make sure that there are safe mechanisms for secure file transfer. When they do not have remote access, vendors often bring in unsecure USB sticks to load code or software patches on their equipment. Tightening perimeter security and, as necessary, locking down OT endpoints is a key second step.
- Prioritize the most vulnerable and meaningful gaps—The OT networks in the automotive supply chain are typically flat. A cyber attack on one system often can impact other plants and systems across the network of suppliers and partners. Automotive manufacturers must assess the potential harm of various threats—i.e., if Machine X goes down or Process Y fails, what is the risk of a downward cycle?—and prioritize actions such as network segmentation that would do the most to mitigate damage across the supply chain.

The question is not whether it's necessary to strengthen OT cybersecurity in automotive manufacturing—rather, it's how and where to get started. Plant and security managers cannot afford to be stymied by the complexity and scope of the clear challenges facing them and wait for new events or regulations to force their hands. There are practical, low-risk steps to be taken today in getting started, and they can enable automotive manufacturers to very quickly realize value in an investment in OT cybersecurity.

About the Author

As Technical Director, Americas at TXOne Networks, Austen Byers leads the company's efforts in providing design, architecture, and engineering technical direction and leadership.

Austen is a sought-after thought leader in operational technology (OT) cybersecurity with more than 10 years in the cybersecurity space. He has spoken at numerous industry events as a subject-matter expert to provide insight into the state of industrial cybersecurity, the intricacies of OT breaches, and providing strategies to help organizations keep their assets and environments safe.

Austen can be reached at austen_byers@txone.com and https://www.txone.com/.

The CISO's Myopia

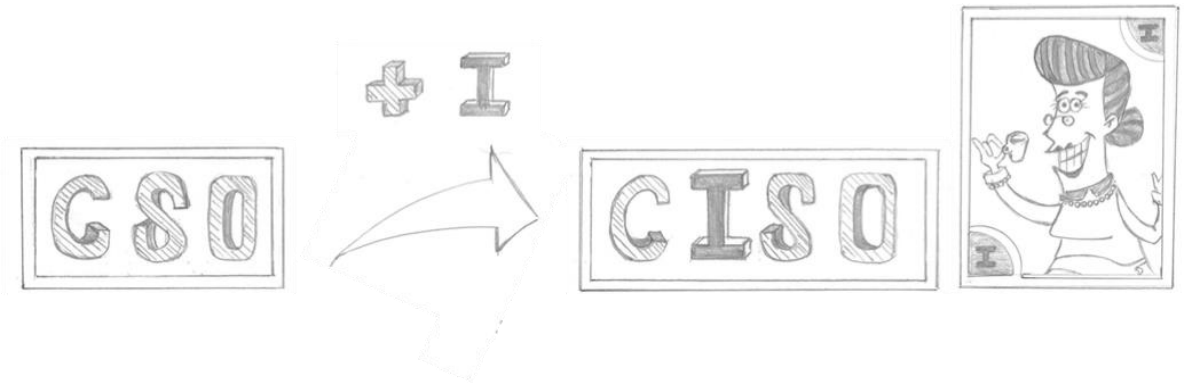
By Jordan Bonagura

Fifteen years ago, I wrote an article entitled "The CSO's Myopia." At the time, I aimed to highlight a critical limitation in information security management. I demonstrated how many information security professionals struggled to manage all the aspects needed to create effective policies and processes. The conclusion I sought to highlight was that this problem is mainly due to an excessively narrow approach to the organization and its usual resources.

Reflecting on what it would be like to run your company without your most important data or, worse still, imagining that all this information could fall into the wrong hands seemed, although obvious, quite alarming. Unfortunately, this uncomfortable reality has become all too common, where data leaks, cyber-attacks, secret breaches, and industrial espionage are frequently reported in the media. At one extreme, threats to national security, such as cyber-warfare, have also further underscored the urgent need for data protection.

Faced with this not-so-new scenario of growing risks, organizational structures need to constantly reinvent themselves. Just a decade ago, the CSO (Chief Security Officer) role was primarily responsible for physical security measures, such as securing facilities, managing personnel security, and overseeing emergency preparedness. Today, the CSO's role has evolved to include new responsibilities, such as enterprise risk management. CSOs are now expected to understand, mitigate, and stay ahead of a wide range of risks, including cyber, physical, operational, and reputational risks. Thus, we can say that this

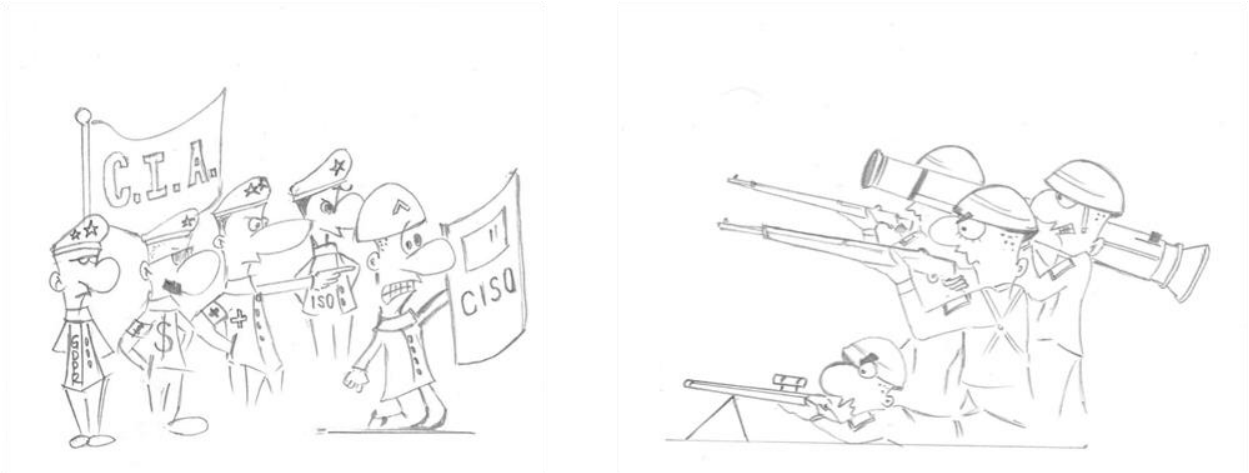
professional has gained, in addition to many new concerns and responsibilities, a new letter to their title: The traditional CSO has been transformed into a new, revamped, and now even busier CISO (Chief Information Security Officer).



The CISO got the Old Maid card.

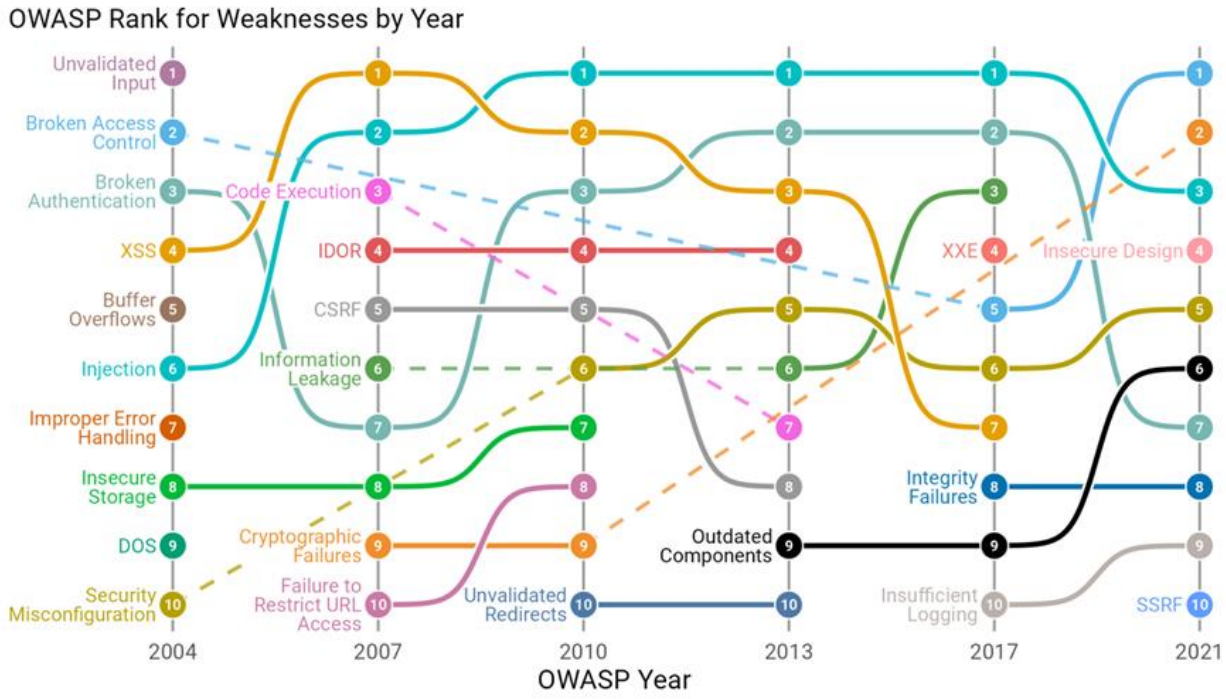
As with many other management positions, the CISO is also the professional responsible for determining the cost vs. benefit ratios of the investments that will be made in the information security area, more specifically, the security and risks vs. the viability of the costs/investments. Obviously, for these decisions, evaluation is crucial, as excessive or misdirected action can derail remediation efforts.

At the same time, the world is committed to seeking solutions for guaranteeing the security triad (Confidentiality, Integrity, and Availability, aka C.I.A.). Numerous regulatory bodies have implemented security norms and standards, such as PCI-DSS, ISO/IEC 27001, and HIPAA, as well as legislation such as the GDPR.



CISO - Compliance and legislation.

As the graph below shows, the types of vulnerabilities recorded over the years continue to be concentrated in very similar main categories. However, the number of occurrences has increased due to the expansion of attack surfaces.



OWASP Rank for Weaknesses by Year - F5 Labs.

Information such as above highlights the critical importance of analysis and tools for a CISO. These tools are essential for improving and updating logical and physical control mechanisms, helping to reduce the risks associated with vulnerabilities that have already been identified and included in organizations' policies.

However, it seems that the "corrective glasses used" now by the new CISO are often not enough to overcome the chronic myopia that plagues the position because the fundamental problem remains unchanged: The constructive process by which companies continue to develop and structure their security policies still uses an "inbox" view that is an internal perspective and, therefore, limited in scope. This "approach" was not, is not, and is unlikely to be sufficient to cover the full range of vulnerabilities in the company.

Companies must consider a new approach since only those who don't experience the day-to-day running of the organization can get far enough away from the heart of the problem to see it from another perspective. As long as CISOs try to base security policies exclusively on their knowledge of the organization and their usual resources, it's improbable that these policies will cover all possible and imaginable gaps. Supported by these policies, many institutions become prisoners of their pseudo-security.

This is the CISO's myopia: believing that building a 100% "made in company" policy can be enough to control all security aspects. This myopia ignores that criminals don't follow the CISO's rules and policies; they think differently and have different experiences, and, at the end of the day, it's many against few.

CISO - "inbox" view.

In this way, the CISO significantly increases the risk of controlling only the aspects covered by this "inbox" view without considering many other real and unforeseen threats that may go beyond their security measures.

The limitation of relying exclusively on the internal policies and knowledge of the CISO and their team highlights the need for an external and specialized perspective to strengthen organizations' security. Specialized professionals and companies can offer more impartial, less biased views.

Pentest services, for example, allow companies to simulate real attacks on your environment, testing the effectiveness of security measures under adverse conditions. Since criminals don't follow the rules established by internal policies, pentesters imitate behaviors and attack techniques real criminals use. This helps to identify weaknesses that could be exploited by external attackers, who operate outside the limits imposed by the company's security policy and often outside the law.

The incorporation of an "outbox" perspective to alleviate problems rooted in the usual "inbox" view, whether in supporting the construction and updating of internal policies or in expanding the knowledge base for consolidating defenses, can help remedy this dangerous myopia that we have been discussing for years.

About the Author

Jordan Bonagura Principal Security Researcher | Information Security Consultant | Cybersecurity Specialist | Professor | Speaker.

If you have any further questions feel free to reach out to him at jordan.bonagura@secureideas.com or you can find him on LinkedIn.

White Paper: Advancing Cybersecurity Through Kernel Immunization

By Patrick Houyoux LL.M. ULB, Brussels,Trinity College, Cambridge, UK. President – Director PT SYDECO

PT SYDECO, an innovative Indonesian company specializing in IT security committed to pushing the boundaries of cybersecurity through cutting-edge solutions adapted to modern threats, presents a revolutionary approach to cybersecurity: immunization of the operating system kernel, inspired by biological immune systems.

Introduction

The digital landscape is continuously evolving, with cyber threats becoming increasingly sophisticated and challenging to detect. Traditional methods of cybersecurity, such as reactive patching and signature-based detection, struggle to keep pace with the dynamic nature of advanced persistent threats (APTs) and kernel-mode rootkits. This white paper introduces a revolutionary approach to cybersecurity: the immunization of the operating system kernel, inspired by biological immune systems.

The Problem with Current Cybersecurity Measures

Current cybersecurity solutions often rely on a reactive approach—detecting vulnerabilities after they are exploited and deploying patches to mitigate the damage. This method leaves a critical window of exposure between the discovery of a threat and the application of a fix, during which systems remain vulnerable to attack.

Moreover, the sophistication of modern threats, particularly those targeting the kernel, demands a more robust and proactive defense mechanism. Kernel-mode rootkits, in particular, can operate with high levels of privilege, making them difficult to detect and remove without significant system disruption.

The Vision: Kernel Immunization

Our proposed solution is a paradigm shift in cybersecurity: the concept of kernel immunization. By drawing parallels with the human immune system, which can recognize and neutralize pathogens before they cause harm, this approach aims to equip the kernel with the ability to defend itself autonomously against threats.

Key Objectives:

- **Immunization Against APTs and Rootkits:** By fortifying the kernel against APTs and kernel-mode rootkits, we aim to create a self-defending system that can neutralize threats at their inception.
- **Autonomous Intrusion Defense:** The immunized kernel would possess the capability to resist any form of unauthorized intrusion, preventing the installation of malicious programs and ensuring system integrity.
- **Elimination of Patch Dependency:** One of the most transformative aspects of kernel immunization is the potential to eliminate the need for traditional patching. This would close the window of vulnerability associated with patch development and deployment, ensuring continuous protection without the risk of data loss or server compromise.

The Benefits of Kernel Immunization

1. **Proactive Defense:** By immunizing the kernel, systems would no longer rely solely on reactive measures. Instead, they would proactively neutralize threats before they can exploit vulnerabilities.
2. **Reduced Downtime:** With no need for patching, systems can remain operational and secure without the disruptions typically associated with updates and fixes.
3. **Enhanced Security Posture:** The kernel's ability to autonomously defend against the most sophisticated threats would significantly enhance the overall security posture of any organization.

Conclusion

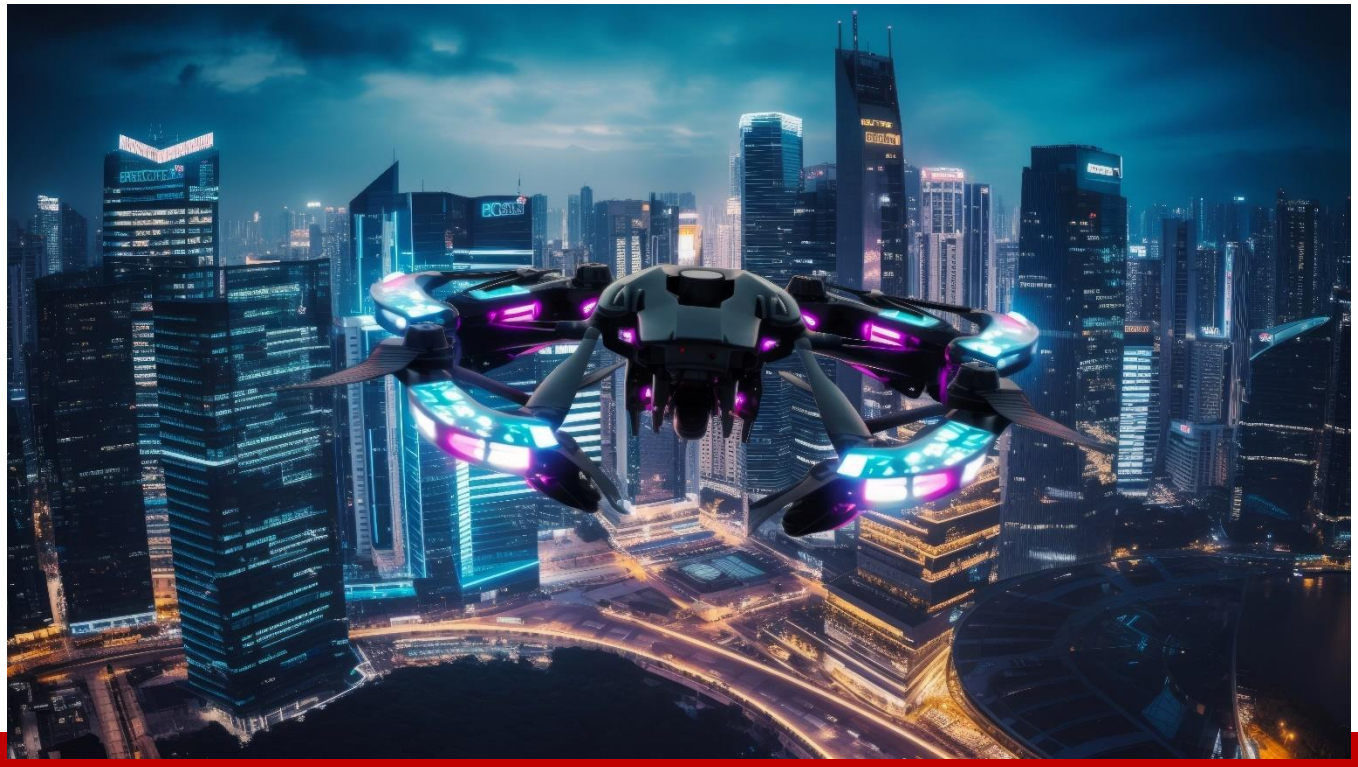
The concept of kernel immunization represents a bold step forward in the field of cybersecurity. While still in its conceptual stages, the potential benefits of such an approach are clear: increased resilience, reduced dependency on reactive measures, and a more secure digital environment. As cyber threats continue to evolve, so too must our methods of defense. Kernel immunization offers a promising avenue for achieving a future where systems are not only protected but immune to the most dangerous cyber threats.

Next Steps

The **PT SYDECO** team is determined to transform the cybersecurity landscape with this innovative technology and is actively seeking partners and collaborators to realize this vision, further develop and refine this concept. Interested parties are invited to contact us info@sydecloud.com to explore potential synergies and contribute to what could be the next big breakthrough in cybersecurity.

About the Author

Patrick Houyoux, Master in Law, Brussels University; Diploma in Comparative Legal Studies, Trinity College, Cambridge University; 3rd Cycle Solvay Business School Brussels University; Research assistant Faculty of Law, Brussels University; Judge of Appeal for the Chamber of Cinematography in Belgium; International Arbitrator; Lawyer; Jurisconsult; President of the Chamber of Commerce Wallonia – Indonesia. President - Director of PT SYDECO.



SWARM: Pioneering The Future of Autonomous Drone Operations and Electronic Warfare

Adaptive Communication for Military Drone Swarms

By Adam Gazdiev, Full Stack Developer

Modern unmanned technologies are experiencing rapid growth, encompassing both civilian and military applications. Autonomous vehicles, delivery drones, and unmanned aerial vehicles for rescue and firefighting services have become an integral part of contemporary infrastructure. However, these technologies are particularly significant in the military sphere, where they set standards and direction for future civilian applications.

Historically, military developments have often outpaced civilian ones, paving the way for the adaptation of the latest technologies. Today, a key direction in the evolution of unmanned systems is their integration into groups or "swarms," which require specialized software to coordinate and synchronize the actions of numerous devices. These systems must not only be autonomous but also capable of functioning effectively under active countermeasures, including electronic warfare (EW).

Group Drone Operations: Modern Requirements and Challenges

Modern combat operations demand a high degree of autonomy from unmanned systems, the ability to adapt to changing conditions, and real-time coordination of actions. When developing software that supports Swarm technology for military purposes, it is important to consider a range of requirements that ensure not only functionality but also security, resilience to interference, and high autonomy. Below is an example list of requirements that could be presented by a potential customer:

General Requirements

- Reliability and Resilience: The protocol must be resistant to software and hardware failures and able to recover quickly. This is particularly crucial in conditions of active countermeasures, including EW.
- Security: The protocol must ensure a high level of protection against unauthorized access, including data and command encryption. It is important to provide adaptive protection that automatically strengthens in response to detected threats.
- Modularity and Scalability: The software should be modular and easily scalable, allowing for the addition of new functions and integration with various types of drones and other weapon systems.
- Performance: The protocol must provide high performance, ensuring coordination and synchronization of actions during high-intensity combat operations.

Functional Requirements

- Autonomous Decision-Making: The protocol must enable each drone to make independent decisions within the parameters of the mission.
- Swarm Coordination: The protocol must effectively distribute tasks among drones and coordinate their actions without constant operator intervention.
- Adaptation to Changes: The protocol must be capable of adapting to changing mission conditions and the environment.
- Scenario-Based Management: The protocol must provide operators with the ability to configure mission parameters and action scenarios through an intuitive user interface.

Technical Requirements

- Communication Interfaces: The protocol must support various communication standards and protocols, ensuring reliable and secure communication.
- Data Processing: The protocol must integrate sensor data from various drones to form a complete mission picture and analyze the current state.
- AI Algorithms: The protocol must include artificial intelligence algorithms for data analysis and decision-making based on machine learning.

Operational Requirements

- Resistance to EW: The protocol must have built-in protection against electronic warfare and be able to operate under active countermeasures.
- Energy Efficiency: The protocol must be optimized to minimize drone energy consumption.
- Support and Maintenance: The protocol must provide the ability for easy updates and support throughout the system's lifecycle.

Technical Overview of the SWARM Protocol

The SWARM protocol was developed as a concept to address all these challenges. It includes innovative solutions that provide stable and adaptive communication between drones, ensuring their coordination and autonomy even under active EW countermeasures.

Operating Modes

The SWARM protocol is designed with various usage scenarios in mind, allowing it to adapt to different mission conditions. The primary operating modes include:

- Standard Mode: This mode is intended for everyday operations where a moderate level of encryption and an average data exchange rate are required. The protocol utilizes FIFO algorithms to process data in the order it arrives, ensuring a balance between performance and resource consumption.
- Combat Mode: In combat situations, the protocol activates enhanced encryption and increases the frequency of data exchange. The use of priority queues ensures that critically important data is processed first, which is essential for timely decision-making and rapid response.
- Silence Mode: For covert operations, the protocol minimizes data exchange while using a high level of encryption. WFQ algorithms are actively employed in this mode to fairly distribute limited communication channel resources among different data streams, maintaining their confidentiality and integrity.
- Protection Mode: The protocol creates electronic interference to counter enemy UAVs and protect ground forces. In this mode, LIFO queues are used, which prioritize the most recent data, allowing for quick responses to new threats and the implementation of necessary measures.

Adaptive Encryption

The SWARM protocol includes adaptive encryption mechanisms that automatically select the level of data protection based on current conditions. In high-threat environments, such as combat operations or electronic warfare (EW) countermeasures, AES (Advanced Encryption Standard) is used. This method provides a high degree of security through the use of symmetric keys and complex encryption algorithms.

In less critical situations, such as standard or training missions, Fernet is used—a symmetric key encryption method that requires less computational power. This ensures faster data processing while maintaining an adequate level of security.

The protocol dynamically switches between encryption methods, analyzing threats in real time using predictive machine learning algorithms. This allows the system to maintain a balance between data transmission speed and security, especially in the presence of active electronic countermeasures.

Dynamic Network Topology

In rapidly changing combat situations or during complex missions, the SWARM protocol supports the dynamic formation and restructuring of network topology. This enables drones to automatically adapt their connections, ensuring a reliable and resilient network even when the swarm's composition changes or individual nodes fail.

The NetworkX library is used for creating and managing network topology, allowing for efficient graph management and the execution of complex computational operations, such as finding the shortest paths and restructuring the network in real time.

When changes in the network are detected, such as the addition of new drones or the failure of existing ones, the topology is automatically updated. This not only ensures network resilience but also optimizes data transmission routes, minimizing delays and improving communication reliability.

Multi-Channel Transmission

The SWARM protocol supports simultaneous data transmission across multiple communication channels, including RF, Wi-Fi, Li-Fi, and optical channels. This provides high flexibility and reliability in communication, particularly in the presence of active interference or channel congestion.

The protocol includes an automatic channel-switching mechanism that adapts to current communication conditions. This allows it to bypass interference by changing the frequencies used or switching to alternative channels, such as Li-Fi or optical, which is especially important when countering electronic warfare attacks.

Context-Aware Routing

In modern combat or complex mission scenarios, the SWARM protocol utilizes context-aware routing, which takes into account various mission parameters when selecting optimal data transmission routes.

Machine Learning Models: The protocol includes trained models that analyze parameters such as network load, signal strength, response time, and communication channel type. These models predict the optimal routes for data transmission, minimizing the risk of data loss and delays.

The use of context-aware routing enables the protocol to adapt to changing mission conditions, increasing the efficiency and reliability of data transmission even in complex and dynamic environments.

Incident Detection and Response Protocols

The SWARM protocol includes advanced mechanisms for the automatic detection and response to hacking attempts or unauthorized access. These mechanisms ensure a high level of security and system resilience under active countermeasures.

Machine Learning Models: The protocol uses Isolation Forest algorithms to detect anomalies in system performance and RandomForestClassifier for incident classification and threat level determination. These algorithms are trained on extensive datasets, enabling them to effectively identify and respond to potential threats.

When an anomaly or intrusion attempt is detected, the system automatically activates backup communication channels, switches to more secure encryption algorithms, and implements other measures to protect the network and data.

Disaster Recovery System

In the context of intense combat or critical missions, the disaster recovery system is an integral part of the SWARM protocol. It ensures network operability during failures, including switching to backup communication channels and restoring data.

The system includes network monitoring, which is carried out using machine learning methods. This allows for the timely detection of potential failures and the implementation of preventive measures, including self-healing and automatic switching to backup resources.

Packet Accounting System

During various tasks and missions, the SWARM protocol utilizes a packet accounting system that supports several queue types for managing data flow. This allows for the optimization of data transmission based on task priority and current conditions.

Queue Operation Modes:

- FIFO (First-In-First-Out): This packet processing mode implies that packets are processed in the order they arrive. This approach is most effective in situations where all data has the same priority, and it is important to maintain processing sequence. FIFO is used in standard operations where uniform resource allocation is required.

- LIFO (Last-In-First-Out): In this mode, the most recently received packets are processed first. LIFO is used in situations where the most current information must be processed immediately, while older data can be deferred. This is useful in critical scenarios where the latest changes in system status or mission conditions are important.
- Priority Queue: In this mode, packets are processed based on their priority. High-priority packets are processed first, allowing for a prompt response to critically important events. This mode is ideal for combat conditions, where certain data, such as alarms or instructions, must be processed immediately.
- WFQ (Weighted Fair Queuing): This mode uses weighted queues to fairly distribute resources among different data streams. Each stream receives a certain share of bandwidth, which minimizes delays for critical data and ensures balanced information transmission. WFQ is especially effective in resource-constrained environments, such as radio frequencies or power-intensive communication channels.

The choice of queue processing mode is determined by the type of mission and current conditions. The SWARM protocol can automatically switch between modes or combine them to ensure optimal performance and minimal delays in data transmission.

Drone Synchronization

To successfully execute missions, the SWARM protocol ensures the synchronization of drone actions, achieved through consensus algorithms such as Raft. This is critically important for maintaining decision consistency and executing synchronized actions across the network.

The protocol provides distributed consensus, allowing drones to make collective decisions and coordinate actions even in the event of a loss of connection with the central command point. This is particularly important in combat situations, where rapid and reliable decision-making is required.

Autonomy and Self-Organization

Drones operating under the SWARM protocol possess a high degree of autonomy, enabling them to make independent decisions based on current data and mission context. Self-organization algorithms allow drones to adapt to environmental changes, restore connections, and coordinate actions with other drones.

The protocol includes self-organization and consensus algorithms, allowing drones to operate both independently and as part of a swarm, ensuring network resilience and mission execution in the face of connection losses and other unforeseen circumstances.

Response to Attacks and Coordination of Drone Actions in Combat Conditions

In combat situations, the SWARM protocol supports the coordination of drone actions, including the automatic distribution of tasks and interaction between drones. This includes functions such as automatic channel switching, activation of interference generation modes to counter enemy UAVs, and real-time task distribution among drones.

The protocol ensures flexibility and adaptability in executing combat tasks, enabling drones to effectively respond to attacks, coordinate their actions, and ensure the safety of both the drones themselves and the ground forces they protect.

The Significance and Future of the SWARM Protocol

The SWARM protocol, even in its conceptual development stage, holds significant potential to influence future military operations and technology. In a world where unmanned aerial vehicles (UAVs) are becoming a critical component of military strategies, the development of such protocols is essential for maintaining global competitiveness.

Global Leaders in Swarm Drone Technology

The United States and China continue to lead the world in the development and application of swarm drone technologies. These countries are actively competing for dominance in this field, reminiscent of a modern-day arms race, but with more advanced and flexible technologies. The U.S. focuses on developing sophisticated software solutions, integrating artificial intelligence to coordinate and manage hundreds of UAVs simultaneously. China, on the other hand, emphasizes mass production of cheaper drones that can be deployed in large-scale attacks.

Ukraine and Russia: Practical Experience and Innovations

In recent years, Ukraine has emerged as a key player in unmanned technology, using drone swarms in real combat situations. This experience allows Ukraine to not only actively implement new developments but also adapt these technologies to perform complex combat tasks. Despite the strongest countermeasures from electronic warfare systems, Ukraine demonstrates high efficiency in using drone swarms, making it one of the leaders in this field.

Russia is also actively developing unmanned technologies, with a focus on electronic warfare and counter-drone measures. The Russian military employs both offensive and defensive UAV systems, emphasizing the importance of a comprehensive approach to modern warfare, where drones play a crucial role.

Joint Military Exercises and International Cooperation

Joint military exercises between the United States, the United Kingdom, and Australia, conducted under the AUKUS program, have been a significant step in testing and integrating swarm drone technologies. These exercises, held in the United Kingdom, allowed participating countries to exchange advanced AI models and jointly test UAV systems in conditions as close to real combat as possible. This cooperation clearly demonstrates that the future of these technologies will be determined by the countries that can most effectively integrate and develop drone swarms within their armed forces.

Global Challenges and the Importance of SWARM

As swarm drone technologies evolve, so do the challenges associated with their effective use and countermeasures. Countries including the U.S., China, Russia, and Ukraine are actively developing both offensive and defensive systems, creating a need for comprehensive solutions. Even in its conceptual phase, the SWARM protocol is already playing a significant role in this context. Its further development can greatly enhance military capabilities, contribute to security and technological leadership on the international stage, and open new perspectives for civilian applications.

Thus, SWARM not only addresses current challenges but also sets the direction for the future development of swarm drone technologies. In the global race for dominance in this field, every new development—whether in hardware or software—has enormous significance for the future of military and civilian applications.

About the Author

Adam Gazdiev is a Full Stack Developer who recently completed a comprehensive Full Stack Development course at SyntraPXL in Belgium. He has developed strong foundational skills in software development, including frontend and backend development, databases, RESTful APIs, and more.

In addition to his technical training, Adam holds a Master's degree in International Relations from RUDN University in Moscow, graduating with high honors.

His diverse background in public service, business, journalism, and project management equips him with the ability to approach technical challenges from a multidisciplinary perspective. This unique combination of experiences enables Adam to analyze problems not only from a technical standpoint but also with a broader understanding of strategic, operational, and human factors.

Adam can be reached via email at a.gazdiev@gmail.com, or through his website https://gazdiev.dev/. You can also connect with him on LinkedIn or explore his projects on GitHub.

The Journey Toward Modern Cryptography

Bringing Clarity Through an Inventory of Cryptography

By Dr. Taher Elgamal, Co-Founder of InfoSec Global and Partner at Evolution Equity Partners

Cryptography has been the backbone of security in our digital world, and it continues to grow in importance as more services, capabilities, and our lives become ever more digital. Cryptography increases in importance daily as we see new reports about cyber-attacks. Hospitals, retail stores, businesses of all sizes, governments - all are under constant threat of attack to exfiltrate data, disrupt critical systems, or other nefarious purposes.

Today's cryptography is very strong against the capabilities of current computers. Indeed, data breaches, for example, are not successful because they break cryptography. Rather, successful attackers mostly obtain digital identities and masquerade as authorized entities to gain access to data and systems. Consequently, we operate on the well-founded belief that the cryptography used to protect our digital lives is, in fact, very secure.

A new threat – quantum computing – is challenging that belief. Cryptographers have known for decades – in fact, well before the development of quantum computers began – that a quantum computer of sufficient power would be able to break some of the most important cryptographic algorithms we depend on today. Significant advances in quantum computing are being announced every few months, putting pressure on organizations to prepare for their arrival.

To counter the threat of quantum computing, organizations worldwide face the challenges of moving from a small set of well-known, traditional cryptographic algorithms to a larger set of new algorithms specifically developed to withstand quantum computing. These new algorithms are known as post-quantum cryptographic algorithms.

Examining the past to chart a course for the future

It is difficult to think of any area of an organization's digital landscape that isn't touched by cryptography. Every user login and machine authentication, such as a Web server identifying itself to a browser, requires cryptography. Securing data in transit and at rest requires cryptography.

With such widespread use of cryptography today, the transition to post-quantum cryptography will take time. Organizations will only succeed in that transition by first understanding where and how they use cryptography today. Each organization owns the overall security posture of its own digital environment, although the organization may not have a complete understanding of their cryptographic assets.

Organizations need a comprehensive cryptography inventory and management. This inventory provides insight into the algorithms, keys, protocols, and software libraries in use today and where they are used. Underscoring its fundamental importance, US federal government agencies are currently mandated to generate a full cryptography inventory. Similarly, organizations processing credit card data must produce a cryptography inventory by March 2025 to meet industry compliance standards.

Only with a comprehensive cryptography inventory can organizations truly understand their cryptography landscape and prioritize which areas to tackle first in their journey to post-quantum readiness.

The critical role of crypto agility

The US National Institute of Standards and Technology (NIST) is currently standardizing a family of new algorithms capable of withstanding the threats of quantum computing. These new algorithms present significant differences from the traditional algorithms they are intended to replace. There is uncertainty over which post-quantum algorithms will stand the test of time and, of course, we should expect more post-quantum algorithms to be developed and standardized over time, as well. Consequently, unlike the past, software and hardware security solutions will need to offer customers a set of cryptographic algorithms together with the ability for customers to easily select and subsequently change the selection of the algorithms in use by specific applications.

When considered at the scale of large organizations, selecting and later modifying the selection of cryptographic algorithms for applications needs to be manageable. This means that organizations need to be able to change the cryptographic algorithms used by applications in a timely, policy-driven manner without requiring changes to the applications themselves. Simply put, this is the definition of agile cryptography, often referred to as "crypto agility".

There is no stopping progress in the digital age, and there is no uncertainty about cryptography's importance to that continual progress. A post-quantum future enabled by crypto agility will be a better, more manageable place for organizations to benefit from cryptography's essential capabilities.

The first step to that future is organizations capturing a full inventory of their cryptography to better understand their digital landscapes. Step two leverages that inventory to create a prioritized plan for transitioning applications to agile, manageable cryptography.

About the Author

Dr. Taher Elgamal is a Visionary Leader in the field of Cybersecurity, widely recognized as the "father of SSL" – the internet security standard, Secure Sockets Layer. His contributions over four decades span entrepreneurship, investment, and technical leadership, shaping the landscape of online security.

Taher's career is marked by innovation. He is a prolific inventor, holding numerous patents in data security, payments, and data compression. He has founded several successful companies, including InfoSec Global, NokNok Labs, and Securify. His tenure as Chief Technology Officer, Security at Salesforce.com further solidified his reputation as a leading expert.

Taher's dedication to the field is reflected in his numerous accolades. He is the recipient of the RSA Conference 2009 Lifetime Achievement Award and the 2019 Marconi Prize, a testament to his lasting impact on the industry.

Taher can be reached at www.linkedin.com/in/taherelgamal/ and at www.infosecglobal.com.

Future-Proofing IoT: Security Measures for Enterprises and End-Users

By John Linford, Security Portfolio Forum Director, The Open Group

As the Internet of Things (IoT) continues to expand, its impact on the business world is profound, offering transformative capabilities across various sectors. From enhancing operational efficiencies in manufacturing with industrial sensors to revolutionizing healthcare with wearable technology, IoT devices are at the forefront of modern innovation. They enable real-time data collection and analysis, facilitating smarter decision-making and the creation of new business models.

However, this widespread adoption of IoT technology also introduces significant cybersecurity challenges. The sheer volume of data generated and transmitted by these devices makes them prime targets for cyber threats. For businesses, this necessitates a proactive approach to cybersecurity, focusing on robust strategies to protect sensitive information and maintain the integrity of IoT ecosystems. By addressing these risks head-on, enterprises can harness the full potential of IoT while safeguarding their operations and customer trust.

Navigating IoT Security Challenges

Despite the benefits of automatic security upgrades, trusting IoT devices is increasingly risky in today's environment. Vulnerabilities can lead to unauthorized access, data breaches, and exploitation of personal information, particularly since many IoT devices do not encrypt data by default. Insecure interfaces and lack of physical security measures make these devices susceptible to malware and other cyberattacks.

Brute-force attacks exploit weak passwords and lack of multi-factor authentication to breach IoT devices. Distributed denial-of-service (DDoS) attacks, driven by botnets, can overwhelm and disrupt unsecure devices. Attackers can also exploit unpatched security flaws in IoT firmware and software to gain unauthorized access or impede operations. Ransomware attacks target critical devices, especially in industrial or infrastructure settings, to block access to systems.

With the proliferation of IoT devices and increasingly sophisticated attack methods, network protection alone is insufficient. Businesses must implement comprehensive cybersecurity strategies, including robust IoT device management, advanced threat detection, and rigorous data encryption, to safeguard their operations and sensitive information.

Applying Zero Trust Principles to IoT

IoT devices like cooling systems, smart TVs, and security cameras can often be overlooked, leading to security gaps. To address this, organizations should adopt a comprehensive Zero Trust strategy that includes all Internet-connected devices. This involves clearly assigning departmental responsibility for hardware and identifying where operational technology (OT) and physical security can be reinforced with Zero Trust principles.

Zero Trust assumes no device is inherently secure, applying continuous security measures rather than granting blanket access. A crucial step is creating an accurate inventory of all assets, particularly IoT devices, to develop policies that account for these often-overlooked vulnerabilities. Given the complexity of large organizations, security teams should also plan for potential gaps in asset inventories.

To effectively implement Zero Trust, the industry needs to standardize best practices, ensuring IoT devices are defended against evolving cyber threats. This proactive approach is essential for protecting networks and the data they carry.

AI-Driven Security Measures

To enhance IoT security, businesses must look beyond foundational strategies like Zero Trust and embrace advanced technologies. Artificial intelligence (AI) and machine learning (ML) play a crucial role in this effort. These technologies can analyze vast datasets to detect patterns and anomalies, enabling real-time threat detection and response. AI-driven security tools can monitor and manage IoT networks more effectively, speeding up the identification and mitigation of potential threats. However, AI should complement, not replace, a multi-layered security strategy.

Blockchain technology offers another layer of protection for IoT networks. Its decentralized structure can secure data exchanges between devices, creating a tamper-proof environment and reducing the risk of unauthorized access or data breaches. Blockchain solutions can enhance the overall security framework by ensuring data integrity across connected devices.

Biometric authentication methods, such as fingerprint and facial recognition, further strengthen IoT security. When used alongside strong passwords, these techniques add a robust layer of protection, minimizing the risk of unauthorized access and ensuring that only verified users can interact with critical systems.

While IoT devices bring significant benefits, the associated security and privacy challenges are substantial. By integrating AI, blockchain, and biometric authentication with foundational practices like Zero Trust, businesses can create a more secure and resilient IoT environment. This comprehensive approach is paramount for protecting sensitive data and ensuring that the full potential of IoT can be safely realized in today's interconnected world.

About the Author

John Linford is The Open Group Security Portfolio Forum Director, responsible for facilitating the creation and delivery of standards and certification programs from the Security Forum, Open Trusted Technology Forum (OTTF), and Assured Dependability Work Group. These groups comprise the cybersecurity and supply chain security SMEs in The Open Group.

The Open Group is a global consortium that enables the achievement of business objectives through technology standards. As Forum Director, John supports the leaders and participants of his Forums and Work Group in utilizing the resources of The Open Group to facilitate collaboration and follow The Open Group consensus-based Standards process to publish their deliverables.

Hacking Cybersecurity Leadership

How effective leadership fosters individual and system-wide resilience

By Daniel Shore, Co-Founder and Social-BehaviouralScientist at MultiTeam Solutions

Cybersecurity is an infinite game being played by teams and multi-team systems of individuals with finite capacity. Alongside this, the unpredictable nature of the cyber industry leaves many things outside of the defenders' control. While leaders readily invest in technology to maximise human capacity, we have to remember that the use of technology is still a human task. New technology can be useful, however we must put more emphasis on human capital. Businesses should be investing more time into their people, their development, and well-being, or else they risk their cybersecurity professionals burning out and quitting the so-called "infinite game."

MultiTeam Solutions conducted research into stress and burnout amongst nearly 175 cybersecurity professionals, where burnout was generally defined as "no longer having the motivation to do one's job effectively." The research found that over 50% of individuals believe they will burn out in the next year, with 35% of this group admitting they anticipate burning out within the next 6 months. Another 25% accept that it will happen in the next 2-3 years. Not only does this show that 80% of respondents acknowledge

they will be less effective in the foreseeable future (and some very soon), but also that burnout and stress are a known and expected part of working in cybersecurity.

Stress and burnout, in many respects, are challenges that present themselves at an individual level. All too often, though, the bureaucratic nature of cybersecurity operations maintains its focus on general performance rather than the individuals involved. Naturally, for high-level strategic decisions, there is merit in taking a generalised perspective, particularly in larger organisations. This approach is not sufficient for addressing stress and burnout.

While leaders are leading teams, multi-team systems, and entire organisations, they—and especially direct supervisors—must pay attention to the individuals who compose those larger groups. If not addressed at an individual level, then stress and burnout will undermine motivation and affect cohesion across cybersecurity ecosystems—contributing to a vicious cycle of unaddressed issues and lower morale. Hence, the principles guiding any new leader-driven initiative aiming to improve mental health and well-being in cybersecurity needs to be rooted in the individual's experience.

There are various practical strategies that leaders can take to help reduce the attack surface of stress and burnout for the people they lead. An important framework to incorporate in any new initiative addressing this issue is the "ABC" framework for motivating individuals: Autonomy, Belonging, & Competence. Motivation serves as one of the best adversaries for stress and burnout.

Autonomy

Leaders can look for opportunities to provide those they lead with a sense of autonomy through ownership and choice. Often, ownership and choice are viewed at a macro level, where a person oversees a task or project simply because it aligns with their role or title—while this contributes to autonomy, it can limit the number of opportunities. By taking a more nuanced perspective, leaders can readily provide and recognise more of these types of opportunities.

At a more micro-level view, leaders can home in on specific tasks or projects that align with an individual's strengths or areas interests, where ownership will come more naturally. For example, if there is a team member with a strong interest and skillset in network security and traffic analysis, the leader can assign this individual the task of enhancing the organisation's Intrusion Detection System (IDS).

This gives the individual a sense of ownership and allows them to manage decisions across various processes including strategically upgrading rules, optimising alerts, and reducing false positives. In this scenario, the leader provides a range of decision-making opportunities, cultivates ownership, and leverages the team member's expertise, which also builds on a sense of competence.

Belonging

Cybersecurity culture often fosters a sense of individualism that lends itself to operating in isolation—individual interest in areas of cybersecurity lead to individually-driven projects, individual certifications, etc. That being said, being siloed is not a sustainable mode of operation. For most cyber professionals,

the challenges are too complex to resolve individually and negative experiences (failure, shame, guilt, embarrassment, etc.), when experienced alone, are likely to take an even greater toll than when those experiences are shared with others.

Leaders can find opportunities to build connectivity through initiatives at multiple levels–the individual, team, multi-team system, and across the organisation. For example, helping to connect goals across these levels can help people understand that they are part of something bigger than themselves. Helping individuals see how their goals fit into those of the team and setting wider objectives that envelope individual aims are all relatively straightforward ways to create a sense of belonging in a professional setting. Similarly, guiding teams to see how their goals fit into the multi-team system, contributes to a sense of belonging at the next tier up of what is known as the goal hierarchy.

Another possibility is supporting employees to start formal groups (e.g., affinity groups) within an organisation in order to bring together individuals with shared identities, interests, or experiences. One example of this would be standing up a “women in cybersecurity” group for the purpose of regularly gathering, sharing experiences, and supporting each other’s career advancement. Successfully organising or contributing to such groups can also build on one’s sense of autonomy and competence.

Competence

In order to boost a sense of competence at the individual level, leaders need to create a learning-oriented environment that provides opportunities for individuals to explore, gather, and practice applying new information. There are specific strategies to build or strengthen these aspects of the work environment.

For example, leaders can support individuals by providing both time and financial resources for professional development opportunities, such as new certifications. An added layer of precision that will further build motivation is identifying how these opportunities support not only their role in the organisation, but also their specific area(s) of interest. Not to mention that the opportunity for individuals to choose to gain expertise in a specific area of interest builds one’s sense of autonomy, and if that area fits within their team’s work, then an increase in sense of belonging (via future contributions) can be part of the outcome, too.

Leaders can also embrace a growth-mindset culture whereby mistakes do not equate to failures; rather, mistakes are repositioned as learning opportunities to develop and grow. This allows individuals to safely explore and practice various aspects of their work. It’s important to note that this approach also requires a shift toward more developmental, rather than punitive or evaluative, feedback.

A necessity, not a nicety

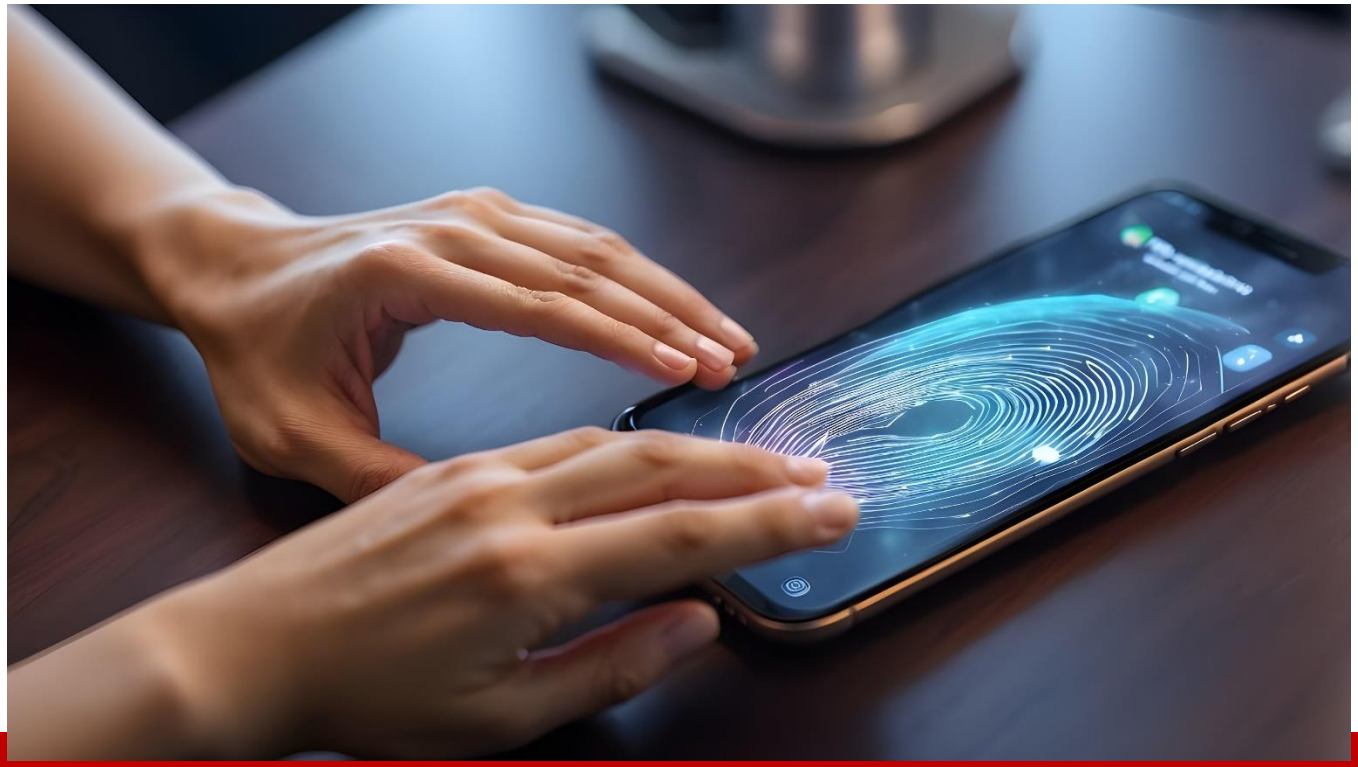
As cybersecurity continues to increase both in complexity and pressure, prioritising the mental health and well-being of professionals is essential to protecting the workforce. By taking a human-centered approach to combating stress and burnout at the individual level, leaders will overcome a common deficiency of large organisations and bureaucracies. Leaders who invest in the ABCs of motivation—and especially

use this model to motivate direct supervisors to support individual team members—will cultivate a productive and adaptive workforce that is more resilient individually and collectively.

About the Author

Dr. Daniel Shore is an expert in Workplace Psychology. He focuses on teams, multi-team systems, and leadership with a human-centered approach to fostering connections within and between teams. He is the Co-Founder of the Integr8 training program, which is built on 5 years of US- and European-government funded research.

Daniel can be reached online on LinkedIN and at our company website MultiTeam Solutions | Leadership & Effective Teamwork Strategies.



How Behavioral Biometrics Protects Against Identity Theft

By Zac Amos, Features Editor, ReHack

It seems like there's news of a new massive data breach daily. Many consumers are on edge, wondering whether their Social Security number, birth date and address are a part of the attack. Conventional security tools are lacking and identity theft is rising, so companies must act sooner rather than later. Could behavioral biometrics be the solution they need?

The Role of Behavioral Biometrics in Identity Verification

Behavioral biometrics falls under the "something you are" authentication factor. It applies physical and digital actions to statistical models or analytics software to distinguish between genuine account holders and fraudsters. It is a type of passive verification that runs in the background as an individual interacts with their device.

Examples of behavioral biometrics include mouse movement, keystroke and scroll speed. On mobile, it tracks device orientation, swiping pattern and touch pressure. Someone's eye movement, signature style, reading speed and gestures can also contribute to their profile.

Despite how complex tracking behavior may seem, this type of biometrics is highly accurate. In one study on identity verification via mobile devices, this tool achieved a 96.47% true acceptance rate and a 0.1% false acceptance rate. Despite only evaluating touch screen and sensor data, its error rate was minimal.

Even if a fraudster has legitimate credentials or knowledge, this tool exposes them for who they really are. Unlike personally identifiable information (PII) — which includes birth dates, names and addresses — behaviors cannot be reliably mimicked.

Why People Need Behavioral Biometrics for Protection

Behavioral biometrics gives people a way to detect and prevent identity theft. They need it because many conventional detection systems become virtually worthless when an attacker has legitimate credentials. As long as someone logs into their account with the correct password and knows the answer to the security question, those tools don't raise the alarm.

Bad actors don't typically steal a person's identity and immediately take out loans or open new credit cards. Instead, they test the waters by logging in a few times to ensure everything works and they've gone unnoticed.

That said, thanks to modern technology, it doesn't take a sophisticated cybercriminal to get away with identity theft. Cracking basic security to steal legitimate credentials has become easier than ever. For instance, using artificial intelligence, a hacker only needs one second to bypass an eight-character password.

Lately, identity theft frequency has been rising. Experts estimate there is a new victim every 22 seconds, meaning 33% of adults in the United States will have their identity stolen within their lifetime. Behavioral biometrics may be the only way to address this issue.

Why Standard Biometrics Aren't Good Enough Anymore

Authentication factors cover something a person has, knows or is. For a while, the latter was considered the best type of security because it couldn't be stolen. Just a few years ago, iris and fingerprint scans were considered the best identity verification measures.

As this technology evolved, face and speech identification became standard. However, with the emergence of AI-powered deepfakes, any hacker with access to a generative model can steal a person's voice and look. Behavior is the only thing this tool can't consistently replicate on a large scale.

Moreover, unlike other biometrics that require a camera, second device or optical scanner to function, behavior biometrics doesn't need any special tool. It functions regardless of device because companies can tweak their process to align with whatever hardware is available.

How This Biometric Protects Against Identity Theft

Behavioral biometrics can protect people against identity theft in several ways.

1. Identify Fraudulent Accounts

Determining whether new accounts are fraudulent is challenging since there's no history. However, companies that track behavior could use the individual's setup actions to verify their identity immediately, protecting existing customers.

2. Develop Personal Risk Profiles

Behavioral biometrics lets businesses develop risk profiles for customers. What they do online tells a lot about how prone they are to identity theft. For example, reusing passwords or visiting sites that don't use HTTPS can compromise their PII.

Decision-makers can use these details to determine their risk level. In response, the information technology (IT) team can develop personalized recommendations or require at-risk users to adopt additional security tools.

3. Expose Account Takeovers

Account takeover is difficult to track with traditional security measures because the access is legitimate. However, the attacker's behavior is often starkly different from the typical habits of the legitimate account holder. The IT team can use this data to freeze and restore the profile.

4. Uncover Synthetic Identities

This tool lets businesses intervene in real time, enabling them to protect against synthetic identity theft. Detecting them becomes difficult when criminals use a combination of real and fake PII. Any activity on their end legitimizes their account, making tracing challenging.

Equifax — one of the big three credit bureaus — reports one out of every three supposed false positives it detects is a synthetic identity. With behavioral biometrics, they could quickly identify subtle discrepancies and close fraudulent accounts.

5. Unmask Cybercriminals

IT teams can track every account's behavior — not just potential victims. This way, they can expose the fraudsters, money mules and hackers who use their platform to steal, sell, transfer and use PII for identity theft long before they target victims.

Balancing the Benefits and Drawbacks of Integration

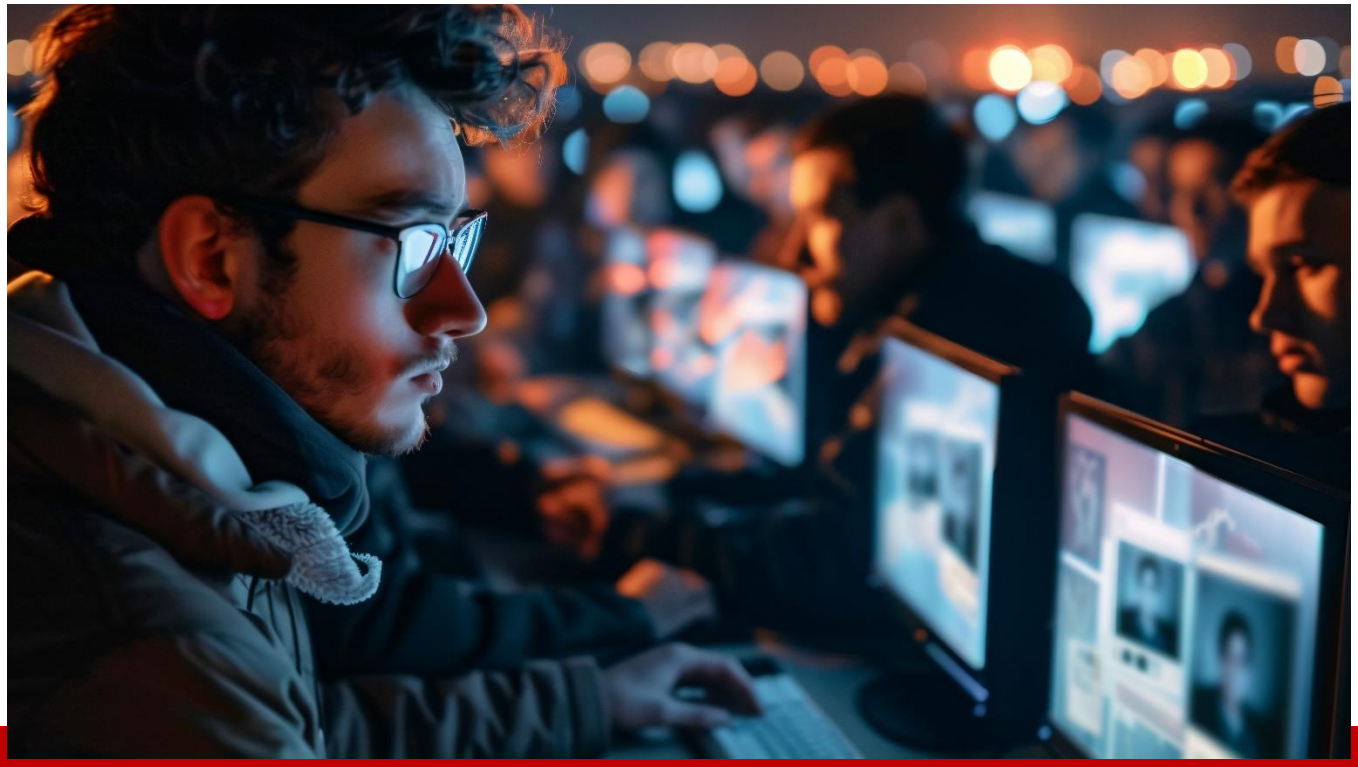
Behavioral biometrics passivity is convenient but lacks privacy. Will business leaders sell that data to third parties? How long will they store it? Is at-rest encryption an option or will it take up too much storage

space? Navigating regulations and alleviating consumers' fears should be a priority for any company seeking to implement this tool.

Security is another potential issue. As much as this wealth of data helps the IT team, it could also help cybercriminals if it falls into the wrong hands. Companies must secure these datasets to ensure detailed sensor, behavioral, location and activity information isn't fed to a malicious botnet or algorithm.

About the Author

Zac Amos is the Features Editor at ReHack, where he covers cybersecurity and the tech industry. For more of his content, follow him on Twitter or LinkedIn.



How Streaming Platforms and Content Producers Can Combat Digital Piracy

By an Executive at Mutin.ee

Streaming platforms and content producers have long faced the challenges of digital piracy, especially as the industry continues to grow into a multi-billion-dollar sector. As technology evolves, so do the tactics employed by criminals to exploit this market. IPTV piracy, in particular, has become one of the most sophisticated methods, providing illegal access to live-streaming services and on-demand content. To preserve the integrity of the streaming market, it's essential to understand the tools and techniques available to combat this ongoing issue.

The Scale and Impact of IPTV Piracy

IPTV piracy poses a significant threat to both streaming platforms and content producers by offering unauthorized access to premium content at minimal cost. This illegal activity undermines legitimate businesses, drains revenue from creators and broadcasters, and contributes to economic losses that affect industries globally. According to some estimates, the illegal IPTV market costs the entertainment industry billions annually in lost revenue. Beyond financial losses, these platforms also evade taxes, depriving governments of essential revenue that could be reinvested into public services.

One of the most significant impacts is on sports leagues and the movie industry. Live sports, especially football, are often illegally streamed through IPTV services, undercutting the value of broadcasting rights. Similarly, movie studios experience diminished returns on their productions as pirated copies flood the internet soon after a film's release, sometimes even before it hits theaters. This depletes the funds available for future content creation.

Technologies to Combat Piracy

To counteract the growing sophistication of IPTV piracy, advanced technological solutions are required. These solutions must detect and disrupt unauthorized streams while simultaneously working within the legal frameworks of multiple countries.

Mutin.ee, a leader in anti-piracy technologies, offers a comprehensive suite of tools designed to effectively disable illegal IPTV services. Key to this effort is the *SpreadKey* technology, which overloads pirate IPTV servers by acquiring and sharing access credentials to weaken their ability to provide consistent streams during high-traffic periods. This disrupts user access and degrades the quality of illegal streams.

Additionally, *ServerSweep* identifies and shuts down pirate servers through reverse engineering techniques and close monitoring of IP addresses. By tracing the source of illegal streams to the load balancers, this technology ensures that the backbone of pirate operations is systematically dismantled. Collaborations with content delivery networks (CDNs) and ISPs allow for swift takedowns, ensuring minimal downtime for legitimate services.

Real-Time Monitoring and Disruption

Real-time detection is crucial for shutting down unauthorized streams before they can gain significant traction. Mutin.ee's system monitors network traffic, analyzes suspicious behaviors, and employs machine learning to detect illicit streams as they emerge. Through rapid response mechanisms, these streams are often taken down within minutes, ensuring that pirated content is not widely disseminated.

The ability to act swiftly is critical during high-profile live events, such as sports championships or exclusive movie premieres, where the demand for illegal streams surges. Through partnerships with local authorities and global rights holders, Mutin.ee coordinates real-time actions, leading to immediate disruptions in service and the prevention of widespread piracy.

Legal and Collaborative Efforts

While technology forms the backbone of anti-piracy efforts, legal and regulatory frameworks also play a vital role in ensuring the continued protection of intellectual property. Companies like Mutin.ee operate within the legal confines of international treaties such as the Berne Convention and the TRIPS

Agreement, which obligate member states to take action against copyright violations. However, these frameworks must be continuously updated to keep pace with the rapid evolution of piracy techniques .

Collaboration between rights holders, service providers, and legal entities is crucial. Many countries have enacted specific laws to address the issue of IPTV piracy, and Mutin.ee works closely with authorities in regions such as the UAE, Qatar, and the European Union to ensure compliance and strengthen enforcement. Notable success stories include partnerships with organizations like BeIN Sports to combat unauthorized sports streaming, highlighting the effectiveness of public-private collaborations in tackling piracy.

The Future of Anti-Piracy Efforts

As streaming platforms continue to expand, the future of anti-piracy efforts will likely revolve around predictive and preemptive strategies. Emerging threats such as deepfake technology, which could be used to create convincing counterfeit content, and encrypted networks that shield piracy activities, will require even more advanced solutions. Anti-piracy technologies will need to evolve to become more proactive, using AI to predict piracy behaviors and prevent them before they occur.

Blockchain may also play a role in securing content rights, providing immutable records of content ownership and distribution, making it harder for pirates to manipulate and distribute illegal content. As digital ecosystems become more complex, companies like Mutin.ee are preparing for these emerging challenges by enhancing their AI algorithms and building more robust, adaptive systems.

Conclusion: The Vital Role of Anti-Piracy Service

The continued success of streaming platforms and content producers depends heavily on the effectiveness of anti-piracy measures. Without the protection provided by technologies like those developed by Mutin.ee, the industry would face significant losses that could threaten its long-term viability. From real-time monitoring to international legal collaborations, the fight against piracy is multifaceted and ever-evolving.

As the battle against online piracy continues, the development and deployment of advanced anti-piracy technologies will remain critical to preserving the integrity of the digital content market. By disrupting illegal streams, securing digital content, and collaborating with authorities, companies can ensure the continued growth and sustainability of the streaming industry.

About the Author

An executive from Mutin.ee.

Mutin.ee can be reached online at Argh@mutin.ee and at our company website https://mutin.ee.

Modern Infrastructure Has a Severe Access Problem

By Ev Kontsevoy, CEO, Teleport

Modern DevOps and cloud infrastructure has exploded in complexity, and with that complexity comes a big access problem. Today's computing infrastructure has evolved so fast that it's the main attack target, with roughly 85% of data breaches in 2023 involving servers.

Unfortunately, cybersecurity approaches to managing secure access have not scaled in lockstep with modern infrastructure. What works for traditional IT – perimeter security with VPNs, shared secrets, Privileged Access Management (PAM), IGA, etc. – is incompatible with modern infrastructure, where the ever-changing, ephemeral nature of resources and multiple cloud solutions have vanquished the static network perimeter.

Nothing is static in modern infrastructure. Everything is defined by code. Every access is a privileged access, meaning an attacker gaining access to a DevOps credential can breach and pivot to other infrastructure resources and sensitive corporate data. In the absence of new strategies, the blast radius can include the deployment pipelines or other sensitive privileges held by the engineers who build and maintain the infrastructure-as-code pipeline.

To stop data breaches, enterprises must enforce Zero Trust at the application and workload layer, not

just the network level (where Zero Trust has already played a material role in securing perimeter-less environments).

Achieving this, however, will require enterprises to embrace a new cybersecurity paradigm that enables unified access control and is based on cryptographic identity, rather than built on unified access controls and cryptographic identity rather than credentials.

Bad actors exploit complexity to move laterally across infrastructure

Let's first put things into perspective. The amount of computing resources needing protection today is immense: physical servers, virtual servers, cloud provider accounts, containers, Kubernetes clusters, CI/CD pipelines, DevOps dashboard, IoT, mobile platforms, and now Generative AI, too.

These have all expanded enterprises' capabilities greatly, but with a big asterisk. Every resource has its own remote access protocol, its own need for encryption, its own identities with credentials, policies, and need for auditing. If you need bespoke domain expertise to secure and manage every single resource, that places significant operational stress on IT teams. The explosion of resources means an immeasurable number of credentials lie distributed among numerous identity silos, and crucially, access policy silos, which expand attack surfaces.

This makes fertile ground for social engineering attacks. Indeed, software vulnerabilities are not the root cause of data breaches (they're only 5% of breaches). Human error is the real problem. It's why roughly half of breaches involve credentials.

A typical identity attack follows a pattern of leveraging identification and authentication failures (e.g. phishing, weak passwords, ineffective or missing MFA, credential stuffing), followed by lateral movement. In other words, attackers don't just directly attack a single target – they navigate through various interconnected systems using the compromised credentials to gain access to different resources. That's how attackers access sensitive data or systems that might otherwise be protected. How can enterprises stop this from happening? This is where zero trust access comes into play.

Access protocols aren't nearly unified enough

The goal of zero trust access is to stop attackers from moving laterally, effectively stopping them at a single compromised resource, reducing the blast radius. You can expose every resource to public network access, removing the distinction between the corporate network and public networks, bypassing and eliminating the need for firewalls and VPNs.

But to achieve zero trust access, enterprises must either remove insecure access protocols or provide a secure wrapper (tunnel) around those protocols. What most enterprises are missing is a unified access mechanism that acts as a front-end to all the disparate infrastructure access protocols. In practice, organizations should only ever be granting access based on tasks, and they should only be

granted the minimum required privileges to finish said task. Not every engineer needs root access, and if they do, they don't need it all the time. Unified access with automation plays a big role in provisioning access with short-term privileges that expire when a task is completed.

Unfortunately, many organizations are still behind on adopting unified access control for authentication and authorization. Visibility is poor, too, as the cybersecurity sector learned recently through the mistaken assignment of dangerous GKE permissions to the 'system: authenticated' user group. It's a telling reminder that software teams often have no idea who has access to which applications or workloads across their infrastructure. This, sadly, is a symptom of access management having become far too complicated and fragmented across silos.

'Developers should never have access to production data' is a rule every tech company should be able to easily enforce across all protocol and resource types. Yet, for most cybersecurity professionals today, that's a sci-fi concept, and that could mean potentially dire consequences if, after a data breach, engineers are unable to trace all access relationships attributed to a user or resource.

A new paradigm for modernizing secure access to infrastructure

Unified access control, paired with zero trust, is the foundation for modernizing secure access, though there are other considerations. To make infrastructure immune to human error, every enterprise needs to make phishing-resistant passwordless (cryptographic) authentication mandatory. While traditionally, strong authentication applies to human users, organizations should also authenticate every system and resource in the infrastructure to be able to grant the appropriate privileges. This also prevents attackers from deploying their own rogue malicious systems.

But how do you implement cryptographic authentication for non-human systems and accounts? You assign a unique identity to every system or resource that's able to be cryptographically authenticated using public key infrastructure (PKI) with hardware security modules (HSM) and trusted platform modules (TPM). Granted, this can be challenging to implement manually in dynamic, ephemeral environments such as Kubernetes, where systems are automatically instantiated as needed. Thus, automating processes here is critical.

This isn't just a new paradigm for a select few organizations to embrace. Any enterprise with operations governing business applications and customer data should see themselves as having a vested interest in properly enforcing zero trust, along with eliminating credentials and standing privileges. After all, modern infrastructure isn't getting any less complex in the next few years, and nobody wants to be in a position where nobody knows who's got access to their data.

About the Author

Ev Kontsevoy is Co-Founder and CEO of Teleport. An engineer by training, Kontsevoy launched Teleport in 2015 to provide other engineers solutions that allow them to quickly access and run any computing resource anywhere on the planet without having to worry about security and compliance issues. A serial entrepreneur, Ev was CEO and co-founder of Mailgun, which he successfully sold to Rackspace. Prior to Mailgun, Ev had a variety of engineering roles. He holds a BS degree in Mathematics from Siberian Federal University, and has a passion for trains and vintage-film cameras. Follow Ev Kontsevoy on LinkedIn and Teleport at https://goteleport.com/.

One Day – Two Conferences

Two independent conferences to be held on one day - or concentration of forces

By Erwin N. Schnee, Founder, ICB Infosec community Builder GmbH

One Day – Two Conferences

On Tuesday, May 20, 2025, the third IoT / OT Security Conference will take place. This conference is dedicated to the theme “Optimally Protecting IoT / OT Enterprise Devices and Networks.” In addition to two keynote speeches and your personal selection from eight breakout sessions, there will be numerous opportunities to exchange knowledge with other professionals. How can the integration of traditional IT with operational technology (OT) infrastructure be achieved while ensuring robust protection against cyberattacks?

While traditional IT has been a target for cybercriminals for years, with corresponding measures taken to protect infrastructure and data, operational technology has only recently been discovered as a lucrative playground for cybercriminals. Consequently, defense measures are less sophisticated.

It is expected that attacks on operational infrastructures will increase significantly in the future. While many professionals are aware of this situation, there is a lack of willingness at the C-level to engage with this issue. How can you create more awareness in your organization? Which areas are well protected, and where is there a need for action? The IoT / OT Security Conference will address these and other challenges related to IoT / OT from 8:00 AM to 1:15 PM. This conference is tailor-made for all those who deal with IoT, IIoT, IoMT, OT etc.

On the same day, from 1:00 PM to 5:30 PM, the eleventh InfoSec Healthcare Conference will take place. The challenges in healthcare are becoming increasingly complex, and information security is gaining more importance. In addition to two keynote speeches and your personal selection from eight breakout sessions, there will be numerous opportunities to exchange knowledge with other professionals on the topic of information security in healthcare.

Whether a targeted attack on a healthcare facility or a random victim of a cyberattack, the consequences can be devastating, and the number of incidents is steadily increasing, even in healthcare. Therefore, the following questions arise: How can you create more awareness in your organization? Which areas are well protected, and where is there a need for action? This conference is customized for hospitals, clinics, medical technology, consultants ...

On May 20, 2025, these two conferences will be held together in Cham (Zug) Switzerland for the first time.

What's New?

- **Two Conferences in One Day:** Attendees can choose to attend one conference or participate in both with our combo ticket.
- **More Exclusive Breakout Sessions:** Fewer slots, but more focus and deeper insights.
- **Cross-Selling Opportunities:** As a sponsor, take advantage of the unique opportunity to reach the entire participant mix in one day.

Why These Changes? We listened to your feedback! More compact events mean:

- More Time Savings for Participants.
- More Efficient and Targeted Contact Opportunities for Sponsors.

Our Expectations for 2025:

- Similar number of participants as in 2024: around 300 attendees.
- Sponsorship slots will fill up faster due to more exclusive offers.
- Higher traffic and improved networking opportunities for sponsors.

What Remains Unchanged?

- Separate websites: www.infosec-health.ch and www.infosec-iot.ch
- Proven processes and a focus on networking and knowledge exchange.
- Access to recordings of the presentations, which have been extensively used in the past.
- Interested in being part of this groundbreaking event? For more information, contact the Organizer.

About the Author

Erwin N. Schnee, Founder ICB Infosec Community Builder GmbH. He has been an independent entrepreneur for over 30 years with a focus on B-to-B and durable consumer goods focusing on market development and customer acquisition as well as their support.

In the ICT industry, he has looked after various companies from small to global companies under his leadership. Occasionally he looked after the following companies and their development in the Swiss market. Novell, Cisco, Adobe and BusinessOne from SAP. In addition, he has supervised projects by Swisscom, HP, Commodore, Apple, 3com Unisys, etc.

Erwin sees himself as a bridge builder between supply and demand with a strong focus on information and cyber security. In this context, he has also launched the InfoSec Healthcare and IoT / OT Security Conference. He can be reached at e.schnee@infosec-cb.ch and www. Infosec-cb.ch, https://www.linkedin.com/in/erwin-schnee-79902941**/.**

People, Not AI, Will Ensure Security in an AI Environment

By Michael Cocanower, Founder and Chief Executive Officer, AdviserCyber

As I walked across the wide expanses of the vendor hall during the annual Black Hat USA event in early August, I searched and searched for a vendor booth without referencing artificial intelligence.

I couldn't find one.

That worries me. As cybersecurity professionals, we know that no system — not a single one — is infallibly secure. Yet, as one company after another rushes to incorporate AI-powered tools in cybersecurity products, we're encouraged to believe that AI will answer all of the security problems that confound us.

The truth is AI also opens a whole new world of potential cybersecurity issues, particularly for industries such as financial services. However, the human factor will remain the most important element of any effective cybersecurity effort, no matter how much AI power is deployed in the battle.

The first challenge arrives

For many organizations, the first great challenge is with the fast adoption of Copilot, the Microsoft generative AI chatbot rolled out just over 18 months ago.

As Copilot is integrated into Microsoft 365 applications, it speeds the creation of documents and presentations, captures action items from Teams meetings, summarizes email discussions, and provides insights on spreadsheet data.

Only 12 months after Copilot was launched, Microsoft revealed that the platform has been used by 50,000 organizations — including more than half of the Fortune 500 — and about 1.3 million paid users. Larger organizations are taking a further step with the creation of custom Copilot applications, but this pace of adoption also demonstrates that small and medium-sized enterprises also are adopting the AI tool.

It's evident, too, that the application is being well-used. When Copilot was launched, Microsoft cited internal research that found that 70 percent of people would like to delegate as much as possible to AI to lessen their workload. There's no way of knowing how much work is being shifted to Copilot and other AI tools, but this increased adoption shows work is being completed via AI at an astounding rate.

Copilot and the deep pool of data

Here's the problem: The foundation of Microsoft 365 applications is data. Copilot taps into that data to create content. But sensitive data — personal identifying information of customers for example — must remain secure. But as Copilot snags data, it risks revealing information that should be secure.

Copilot can create lots of sensitive data on its own, drawing from the deep well that's available to users of Microsoft 365. Those newly created documents don't always carry the same security tags as the source file.

A marketing team, for instance, might use Copilot to help analyze recent customer survey data. Some of the customer comments in the survey files might be confidential. The analysis developed with Copilot might not recognize that these comments are confidential, the analysis could be uploaded to a company server with wide access, and sensitive customer data would spill out.

It's fair to assume any new file — whether it's created with the help of AI or not — is going to end up somewhere it doesn't belong.

A survey this spring by Concentric AI highlighted the risks. It looked at more than 550 million data records and found that the average organization has more than 800,000 files at risk due to oversharing. According to the study, 16 percent of an organization's critical data is overshared, 17 percent of at-risk files are overshared with third parties and 90 percent of documents considered "business critical" are being shared outside of the executive suite.

The Dark Cloud: Intruders

As troublesome as oversharing may be, far more serious issues will arise as intruders learn how to exploit Copilot to gain access to data and systems.

Already, cybersecurity professionals at Blackhat demonstrated numerous ways that bad actors within an organization as well as outsiders could use Copilot to access internal company information, manipulate it, or steal it.

Essentially, Copilot — or any similar AI-powered assistant — is just another user on the network. Its access privileges can be exploited just like those of any other user.

Microsoft's security focus

Microsoft, as expected, paid close attention to security in the development of this powerful AI tool. Copilot adheres to security and compliance standards, it relies on encrypted data transfer, it uses its Entra ID tool to authenticate access and it doesn't allow third-party sharing by default.

This is all good. But it's critically important to note that Copilot relies on existing permissions and policies. In their rush to meet the demand of workers and efficiency-minded executives for fast deployment of Copilot, cybersecurity professionals may not take the time to look as closely as they should at existing permissions in their organization's systems. This should be audited at least annually, but that's a heavy lift for small and midsized organizations where employees are already likely wearing multiple hats.

And the security that Microsoft has built into Copilot crumbles into sand when users store sensitive information in much less secure locations — notably, their personal OneDrive accounts, or don't classify the data appropriately according to company policies.

AI security tools and more

Copilot, of course, is only the most visible of the AI-powered tools whose development and deployment will challenge the cybersecurity profession.

It's not surprising, then, that technology entrepreneurs have identified AI-focused cybersecurity as a growth market. The long rows of vendors at Blackhat, each with their take on the improvement of cybersecurity in an AI environment, speak volumes about the direction the profession is taking.

Many of the cybersecurity products that are pouring into the market address real needs. Many of them provide clever and efficient solutions — often relying on AI-powered tools to battle cybersecurity threats in the AI environment.

But AI itself won't provide all the solutions for AI security. Cybersecurity professionals who limit themselves to the deployment of technological tools will be crushingly disappointed if they don't simultaneously build a good cybersecurity culture, a culture that recognizes the importance and best practices of cybersecurity across the organization.

Practical steps for staff

First, and most importantly, every person in the organization needs to understand that cybersecurity is an organization-wide responsibility. It is not the job of the cybersecurity team. Rather, good security depends on each individual. This message needs to be part of Day One onboarding, and it needs to be driven deep into the organization's culture.

Second, the requirement of personal responsibility is particularly important when users rely on Copilot or other AI-powered assistance. Good cybersecurity trainers will help them understand how AI tools can tap deep into the organization's files, and trainers will emphasize again and again the danger that arises when files incorporated into AI-assisted documents don't carry the same security tags as they did in their original home.

Third, cybersecurity teams within organizations must ensure they are putting as many guardrails into place as possible when deploying CoPilot or enabling users with add-on tools like CoPilot Studio. At a minimum, those responsible for cybersecurity (whether in-house or outsourced) should be familiar with the types of exploits demonstrated at Blackhat and other security conferences, and enable as much protection as possible when rolling out these tools.

Fourth, cybersecurity leaders must remember that not everyone in the organization understands the meaning of security tags. Staff members almost certainly will understand that Social Security numbers must be kept secure. However, they may not exercise the same caution with the terms of a vendor contract or results of a customer survey. From the executive suite to the desk where the interns sit, everyone needs to be on the same page.

Fifth, if everyone is to be on the same page, cybersecurity leaders need to ensure that common nomenclature is used across the organization. Is "secure" the same as "confidential"? Remove any doubt with standard terminology.

Practical steps for cybersecurity leaders

While security is an organization-wide responsibility, good cybersecurity executives create an AI environment that allows the organization to thrive.

First, they refuse to let themselves be rushed into poorly vetted decisions about AI tools. To be sure, competitive pressures and the rapid adoption of AI tools by organizations large and small require timely decision-making. But cybersecurity executives need to understand the risks that any AI tool brings — and they all carry some risk. This understanding needs to be shared across the C-suite.

Before AI tools such as Copilot are deployed, organizations should carefully review their data classification and access policies, especially related to sensitive data. The standard always will be "need to know" first followed by "least privilege." These standards become eroded over time, however, as more and more people argue that they need to know. Adoption of AI tools should be accompanied by a review and reset of permissions.

Finally, cybersecurity leaders need to battle against a philosophy of “set it and forget it” when they deploy AI tools. Training programs must be ongoing. Access-control policies must be reviewed and revised regularly, especially in organizations that are growing rapidly or expanding their use of AI tools.

These are big jobs requiring heavy lifting by cybersecurity professionals. They’ll get some help from the many products that are arriving in the market. But success ultimately will depend on the ability of cybersecurity professionals to motivate, train, and support the people who are the cornerstones of any successful security effort.

About the Author

Michael Cocanower is Founder and Chief Executive Officer of AdviserCyber, a Phoenix-based cybersecurity consultancy serving Registered Investment Advisers (RIAs). A graduate of Arizona State University with degrees in finance and computer science, he has worked more than 25 years in the IT sector. Michael, a recognized author and subject matter expert, has earned certifications as both an Investment Adviser Certified Compliance Professional® and as a Certified Ethical Hacker. He is frequently quoted in leading international publications and has served on the United States Board of Directors of the International Association of Microsoft Certified Partners and the International Board of the same organization for many years. He also served on the Microsoft Infrastructure Partner Advisory Council.

Resilient Cyber Infrastructure on Limited Budgets

Top-tier Cybersecurity Without Breaking the Bank

By Solemar Bottcher, Founder, S NEXT Cybersecurity

The cybersecurity trends for 2025 demonstrate that nothing new is emerging, but rather that the demands of 2023 and this year are being amplified, highlighting the opportunity to discuss the challenges that companies worldwide encounter when it comes to securing their assets, and maintaining their reputation, whether through budget constraints or selecting the best solutions. In many cases, CISOs and IT teams are frequently under a lot of pressure to complete these tasks, which can result in errors and further delays to the process.

Let's get straight to the point: no piece of technology will replace the responsibility of a human employee or user. An organization can invest a million dollars, but if it does not establish a daily safe and proactive culture, the broken workflow will find a way to throw that money right in the trash.

Before allocating resources, it's crucial to understand your organization's specific security requirements. Every company needs awareness and training, but not necessarily an expensive NDR solution.

I've already demonstrated this with projects in which our clients were able to build a solid infrastructure simply by beginning with the primary value, as previously stated, people. Begin strategic planning for the human element, documentation, and current infrastructure. This first phase requires little expenditure and, if done right, will provide such security that it will drive the following technology investment by helping to prioritize areas where the money is used efficiently.

Social Engineering

Cultivating a security-conscious culture is critical. The organization as a whole gains when workers emphasize security at all levels. Security begins here, fostering a culture in which everyone is accountable for maintaining security.

Social engineering remains the most significant threat, corresponding to 74% of all breaches, according to Verizon. Rather than taking advantage of technological flaws, it plays on human psychology. The likelihood of successful social engineering attacks can be considerably decreased by investing in user education and awareness initiatives. Employee vigilance can be maintained by routine training and simulated phishing activities.

Search for Alternatives

The digital security landscape has transformed dramatically. Initially, simple firewalls and antivirus programs were enough, but as cyber threats grew more sophisticated, so did the required defenses. Today, organizations must contend with advanced persistent threats (APTs), ransomware, social engineering attacks, and an extra truckload of risks. This evolution calls for a more comprehensive and layered security approach.

With budget limitations, exploring alternative solutions becomes essential. When it comes to the technology and equipment side, especially in a non-profit environment, work with recycled parts can be very useful, it can be with parts that are stored in the shelf, collected on recycle centers, or even found at the bin itself. It is up to use as long as it can accomplish the task at hand with a decent performance.

Open-source tools also offer several advantages, including cost savings, transparency, and community support. These softwares can be customized to meet specific needs and often benefit from regular updates and a collaborative development model. Some proprietary solutions often have free tiers that provide essential functionalities without the associated costs. Notable examples are Snort for intrusion detection and OpenVAS for vulnerability scanning.

The Cloud (aka someone else's computer)

Independently of the company's size, recently we've been hearing about Shadow AI, referring to AI tools and solutions implemented without formal approval, which can pose significant risks. A note to take here is that, it is not only AI, but all Software as a Service (SaaS) tools and cloud instances, it's essential to maintain visibility and control over all deployments to ensure they align with security policies and do not increase the attack surface of an organization. A new phrase resuming it all is "get breached without being breached".

Wrapping Up

Moreover, the best investment that can be done is gathering knowledge. Worldwide accepted cyber standards such as NIST CSF and PCI DSS are freely available for reading and learning. Staying informed about current trends and emerging threats is also vital, by following cybersecurity forums, blogs, and social media channels, can provide insights into cost-effective solutions, community-driven security practices and helps in making informed decisions, staying ahead of potential threats. Well, you must understand, because here you are, reading Cyber Defense Magazine!

About the Author

Solemar Bottcher is the Founder and CEO of S NEXT Cybersecurity. With a degree in Computer Science and specialization in infrastructure security, Solemar dedicates his career to protecting the digital landscape through innovation and ethical practices. He believes in the power of continuous learning and proactive approach to cybersecurity. He is also a strong advocate for regular employee training. Beyond his professional achievements, Solemar is a man of diverse passions, including racing, retro items, road trips, classic cars, and 80s rock music. Additionally, his Christian faith is a cornerstone of personal and professional commitment, guiding him in his mission to make the digital world a safer place.

Solemar can be reached online at solemar@snext.com.br and at our company website https://www.snext.com.br/.

Locking Down Your Digital World: Mobile Security Best Practices

By Nicole Heron, Marketing Manager at Salt Communications

In today's hyper-connected world, our smartphones have become indispensable tools for both personal and professional use. These mobile devices now hold sensitive company data, critical contacts, confidential emails, information shared via instant messaging platforms and vital financial information. This convenience brings a significant responsibility: the need for robust mobile security measures. Ensuring the security of these devices is crucial to protecting your digital world from potential threats and vulnerabilities. Here are essential practices to help you secure your smartphone and safeguard your valuable information against cyber threats.

1. Use Strong Passwords and Biometric Security

The first line of defence for your mobile device is a strong, unique password. Users should avoid using simple, easily guessable combinations like "1234", "password", or even your birthday (as everyone rushes to change their passcode). Instead, they should opt for a complex password that includes a mix of upper and lower-case letters, numbers, and symbols to enhance security. Additionally, many smartphones now offer advanced biometric security features such as fingerprint scanning, facial

recognition, or even iris scanning. These features provide an extra layer of protection, making it more difficult for unauthorised users to access your device. Combining a strong password with biometric authentication significantly reduces the risk of unauthorised access and helps safeguard your personal and professional information.

2. Enable Two-Factor Authentication (2FA)

Two-factor authentication (2FA) enhances your account security by adding an extra verification step beyond just a password. This means that even if an unauthorised person manages to obtain your password, they still can't access your account without the second form of verification. This additional layer of security often involves a one-time code sent to your mobile device, or it can be a prompt in an authenticator app. By requiring both something you know (your password) and something you have (your mobile device or another verification method), 2FA significantly increases the difficulty for attackers to breach your accounts, offering robust protection against unauthorised access.

It is probably useful to not have your only 2FA system on the same phone which may have fallen into the wrong hands. Multi-layers or options for 2FA would be most beneficial to protect your important information.

3. Keep Your Software Updated

Software updates frequently contain essential security patches designed to protect your device from emerging threats and vulnerabilities. These updates address known issues and enhance the overall security of your operating system and applications. By regularly updating both your operating system and apps, you ensure that your device has the most current defences against malware, phishing attacks, and other security threats. Keeping your software up-to-date is a proactive step in safeguarding your data and personal information, reducing the risk of exploitation by attackers seeking to exploit outdated software weaknesses.

4. Be Wary of Phishing Attempts

Phishing scams are becoming increasingly sophisticated, making it more challenging to identify and avoid them. Cybercriminals use various tactics to deceive individuals, often creating messages that appear legitimate. Be particularly cautious of unsolicited emails, text messages, or phone calls asking for personal or financial information. Always verify the sender's identity through a separate, trusted channel before clicking on any links or downloading attachments. Look for signs of phishing, such as unusual URLs, spelling errors, and generic greetings. Additionally, ensure that your security software is up to date to help detect and prevent these malicious attempts. Stay informed about common phishing techniques to protect yourself and your organisation's information.

5. Manage App Permissions

Regularly review the permissions granted to your apps and limit access to only what is necessary for their functionality. For example, a weather app typically doesn't need access to your contacts, camera, or microphone. Reducing unnecessary permissions minimises the risk of data breaches and unauthorised data usage. By restricting app permissions, you help protect your personal information from being accessed or exploited by potentially malicious software. Take the time to go through your device settings periodically to ensure that each app only has access to the data and features it genuinely requires to operate. This practice not only enhances your privacy but also contributes to the overall security of your device.

6. Back Up Your Data

Regularly back up your data to a secure cloud service or an external device to safeguard your valuable information. By doing so, you ensure that even if your phone is lost, stolen, or compromised by malware, you can recover your important files, photos, contacts, and other data without significant disruption. Opt for reputable services that offer robust security features, such as encryption and two-factor authentication, to protect your backups from unauthorised access.

Additionally, consider maintaining physical backups on external devices like hard drives or USB sticks for an extra layer of security. Consistent data backups are a critical component of a comprehensive digital security strategy, providing peace of mind and ensuring continuity in the face of unexpected incidents.

7. Remote Wipe Capability

Enable the remote wipe feature on your device to enhance your security measures. This functionality allows you to remotely erase all data from your phone if it is lost or stolen, ensuring that your personal and sensitive information does not fall into the wrong hands. To set this up, use the built-in options available in your device's operating system, such as Find My iPhone for Apple devices or Find My Device for Android devices. Make sure to familiarise yourself with how to activate the remote wipe feature quickly and efficiently in case of an emergency. Enabling remote wipe adds an essential layer of protection, giving you peace of mind knowing you can safeguard your data even if your device is physically compromised.

8. Educate Yourself

Stay informed about the latest security threats and trends by actively educating yourself. Awareness is a powerful tool in protecting your digital world, as it helps you recognise and respond to potential risks effectively. Follow reputable tech blogs, subscribe to security newsletters, and participate in online forums dedicated to cybersecurity. These resources provide valuable insights, tips, and updates on emerging threats, best practices, and technological advancements. Additionally, consider taking online courses or attending webinars to deepen your understanding of cybersecurity. By staying proactive and

continuously enhancing your knowledge, you can better defend against cyber threats and make informed decisions to protect your digital life.

9. Secure Your Communications

By investing in secure messaging technology and fostering a culture of cybersecurity awareness, organisations can significantly reduce the risks tied to transmitting sensitive information via insecure systems. This proactive approach not only protects the integrity of corporate networks but also ensures the trust and confidence of customers, employees, and stakeholders when sharing important information through a trusted instant communications platform. In doing so, organisations can safeguard their valuable data assets and maintain their reputation in an environment where consumer messaging systems are insecure and actively being used as a route onto consumer devices causing data breaches and cyberattacks that can have severe consequences.

Best Practices for Mobile Security

By following these best practices, organisations should also consider integrating a Mobile Device Management (MDM) solution into their operations, to allow them to significantly enhance the security of their mobile devices and protect the professional data being managed.

In a world where digital threats are constantly evolving, taking proactive steps to secure your mobile operations is essential. This includes using strong passwords, enabling two-factor authentication, keeping your software up to date, and being cautious of suspicious messages or links. MDM solutions offer centralised control and monitoring of your mobile devices, ensuring compliance with security policies, remotely wiping data if a device is lost or stolen, and automatically deploying security updates. Regularly review and adjust your security settings, including MDM configurations, to ensure optimal protection.

Lock down your digital world today and enjoy the peace of mind that comes with knowing your information is safe. Implementing these security measures not only protects your personal and professional data but also helps prevent unauthorised access and potential breaches. Stay vigilant and proactive to maintain a secure and trustworthy digital environment.

Contact Salt Communications today to explore how our expertise can help your organisation secure its sensitive communications effectively – email info@saltcommunications.com or visit our website saltcommunications.com

References:

https://www.keepsolid.com/authenticator/help/security/strong-password-or-biometric-authentication

https://www.ncsc.gov.uk/guidance/phishing#:~:text=Business%20Guide%20beforehand.-,What%20is%20phishing%3F,can%20sabotage%20systems%20and%20organisations

https://www.techtarget.com/searchmobilecomputing/definition/remote-wipe

About the Author

Nicole Heron is Marketing Manager at Salt Communications. Nicole has been working within the Salt Communications Marketing team for several years and has played a crucial role in building Salt Communications reputation. Nicole implements many of Salt Communications digital efforts as well as managing Salt Communications presence at events, both virtual and in person events for the company.

Nicole can be reached online by emailing nicole.heron@saltcommunications.com and at our company website https://saltcommunications.com/.

Security Breaches Are Expensive: Your Company Needs a Culture Overhaul

Centralized Security Teams Might Not Be Enough

By Manish Sinha, Software Engineer Lead, Facebook

In today's rapidly evolving digital landscape, we can no longer rely on a centralized security team as the sole gatekeeper of our organizations' digital strategy. The traditional model of relegating security to compliance is no longer sufficient.

Instead, security must become an integral part of your company culture, woven into every decision and action taken by employees at all levels. There needs to be a leadership buy-in and be part of every significant technical discussion.

The Problem

In recent years, there has been a surge in high-profile security breaches, each serving as a reminder that inadequate security measures can have devastating consequences. These breaches result in financial losses, cause long-term damage to a company's reputation, invite regulatory oversight, and hurt customer trust.

If personally identifying information is breached, it can lead to customers suffering from identity theft. The Department of Justice released their report - Data Breach Notifications and Identity Theft, 2021. The key findings were

1. In 2021, 12% of all persons aged 16 or older were notified that an entity with their personal information experienced a data breach in the prior 12 months (figure 1).
2. Victims of identity theft (24%) were twice as likely as non-victims (11%) to learn that an entity with their personal information experienced a data breach in the past year.1
3. Victims of multiple types of identity theft (32%) were more likely than victims of existing credit card (25%), bank (16%), or email or social media account (23%) misuse to learn that an entity with their personal information experienced a data breach.

Consider the 2017 Equifax breach, which exposed the sensitive personal information of 147 million people. The company faced a staggering $700 million settlement and suffered immeasurable damage to its reputation.

Similarly, the SolarWinds supply chain attack in 2020 affected thousands of organizations worldwide, including multiple U.S. government agencies. The full extent of the damage is still being assessed, with estimates running into billions of dollars.

As we can see, the impact is significant, and there is a critical need for an approach that scales, is comprehensive, and focuses more than checking checkboxes on compliance forms.

Centralized Security Team - Pros and Cons

Traditionally, organizations have relied on centralized security teams to manage their cybersecurity needs. While this approach has merits, it also has significant limitations.

Criteria	Centralized	Distributed
Consistency and Coherency	Consistency in security practices across the organization	Potential disconnects from broader security practices
Responsibility and Accountability Model	Centralized oversight and governance. Risk being perceived as overbearing	Individual teams have more flexibility and are given more leeway to determine specialized policies to suit their needs. Considered less overbearing.

Scalability	Efficient Allocation of resources. Difficulty in scaling a single team for the entire company	Duplication of resources, but possible to scale up for an entire company

As highlighted in the IANS Research article, a hybrid approach that combines centralized oversight with decentralized execution can offer a balance. This model involves creating a service-oriented security organization that provides essential security functions while allowing flexibility and responsiveness to individual business unit needs.

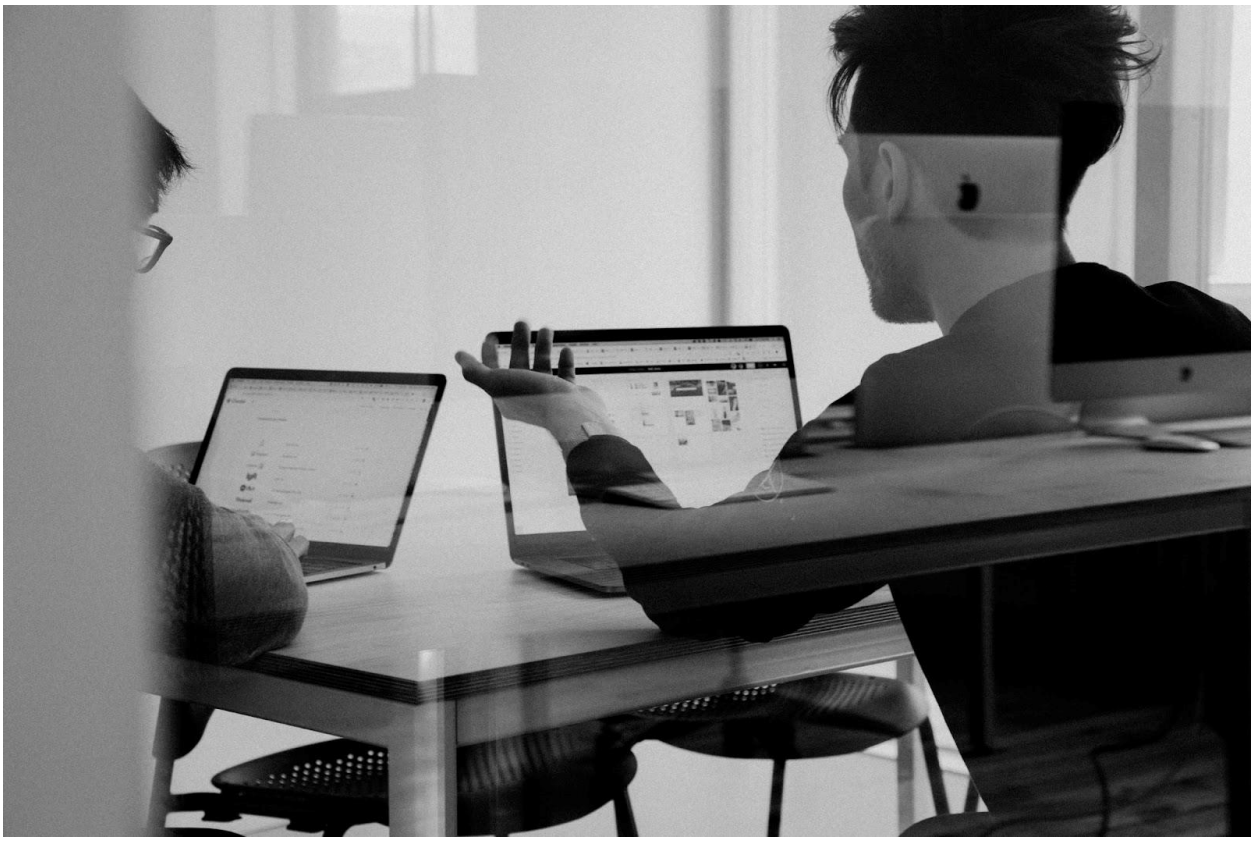
One shortcoming of the above research article is that it assumes security is one size fits all, which can be checked off with checklists. Security is a process and a culture where nuanced decisions must be made. This means the distributed security structure is critical, as the individuals working closely with the product better understand the intricacies and threat model.

Adoption of a new culture

It is crucial to instill a new cultural mindset that integrates security into the very fabric of the organization. This shift in culture entails:

1. Making every individual accountable for security, not solely relying on the central security team
2. Promoting transparent discussions about security issues and occurrences
3. Cultivating a mentality of continuous growth and adaptability in light of advancing threats
4. Acknowledging security achievements and gleaning insights from setbacks without assigning blame

This cultural transformation necessitates unwavering leadership support, consistent communication, and concrete steps that demonstrate the organization's dedication to security.



Central team vs individuals - separation of responsibilities

While shifting towards a security-conscious culture, it's crucial to delineate responsibilities between the central security team and individual employees. There should be no overlap or ambiguity.

Central Security Team	Individuals
Developing and maintaining security policies and standards	Following security best practices in their daily work
Providing specialized security services (e.g., threat hunting, incident response)	Identifying and reporting suspicious activities or potential security incidents by analyzing their product usage
Offering guidance and support to business units	Receive guidance and participate in security programs

Conducting security assessments and audits	Considering security implications in their decision-making processes

Fund an Internal Security University Program

Unfunded mandates are a slow-ticking time bomb. If the company considers security crucial and mandates that everyone play their part, it needs to fund a training and support program.

The best way to start is to invest in a comprehensive security education, which they can call “Security University” within the company. The company should ensure that each individual who needs to be trained has time allocated to go through the learning exercise and an opportunity to put it into practice.

This "Security University" should:

1. Offer role-specific security training
2. Provide hands-on labs and simulations
3. Keep employees updated on the latest threats and mitigation strategies
4. Foster a community of security champions across the organization

Lastly, the company should have some support resources for individuals to fulfill their responsibilities. Examples could be an internal community, groups, or Q&As with experienced security engineers.

Properly align incentives

The Majority of U.S. employees say incentive-based pay motivates them at work. This should not be surprising, as work isn’t the only thing we value in our lives.

It's well-established that incentive-based pay motivates employees. Harvard Business School released a study reinforcing this idea - Do Bonuses Enhance Sales Productivity? A Dynamic Structural Analysis of Bonus-Based Compensation Plans. Organizations should leverage this insight to align their incentive structures to promote security-conscious behavior.

This could include:

- Incorporating security metrics into performance evaluations
- Offering bonuses for identifying and reporting security vulnerabilities
- Recognizing and rewarding employees who go above and beyond in promoting security
- Tying executive compensation to the organization's overall security posture

Organizations can ensure security becomes a priority at all company levels by properly aligning incentives. Everyone can play their tiny part so that they all add up.

Putting it all together

Transforming security from a mere compliance checkbox to a fundamental part of company culture requires a comprehensive approach. This involves reconsidering organizational structures, investing in education, aligning incentives, and fostering a mindset where security is everyone's responsibility.

This transformation won't happen overnight. It demands sustained effort, commitment from leadership, and patience. However, the benefits – including improved resilience against threats, enhanced customer trust, and potentially significant cost savings from avoided breaches – make this journey worthwhile.

In an era where digital assets are often a company's most valuable resources, treating security as a cultural imperative rather than a necessary evil is not just smart – it's essential for long-term success and sustainability.

About the Author

Manish Sinha is an accomplished Software Engineer currently working at Meta. He specializes in Security and Performance, including the intersection of the two. With over 13 years of industry experience, he has previously worked at Amazon and Microsoft, gaining extensive experience and handling significant software and services used by millions daily. At Amazon, he was the company's security certifier, reviewing and approving many applications that handled critical customer data.

Manish Sinha can be reached online at contact@manishsinha.me and https://www.linkedin.com/in/manishsinha27/ and at his website https://manishsinha.me.

Security Post CISA Secure by Design Pledge

By Ram Movva, CEO of Securin and Kiran Chinnagangannagari, Co-Founder, Chief Product & Technology Officer, Securin

Tech leaders recognize that there has never been a more crucial time to begin incentivizing routine security practices and across industry transparency. This is especially apparent to those that were among the first to sign CISA's Secure by Design pledge, that select group of cybersecurity professionals are also cognizant of the importance of how we address and discuss the vulnerabilities and weaknesses that lie within software that is widely used.

Most of the vulnerabilities being exploited today are ones that could have been avoided. Below are some examples:

The Challenges of Weaknesses and Vulnerabilities

1. Putting all of your focus and security efforts onto the MITRE Top 25 can leave you vulnerable to a less known, highly weaponized weakness that's relevant to your specific systems. Relying solely on the Top 25 based on CVSS scores is missing the big picture considering that our industry calls out for risk-based prioritization. For example, across CISA KEVs, eight of the Top 25 weaknesses are outside the MITRE Top 25. The same can be seen with the MITRE Top 25 list where nine out

of the Top 25 weaknesses across ransomware-exploited CVEs are absent. This is starting to be remediated with MITRE itself acknowledging the gap and releasing its Top 10 CISA KEV Weaknesses in 2023.

2. There is also the harsh reality that older vulnerabilities that have been around for a while are not out of commission. This can be seen with XSS (cross-site scripting), developers are coding-in the same errors to web applications repeatedly. This is not done out of laziness or spite, but because modern web applications are often complex, with numerous interconnected dependencies and components.

3. We must equip developers with the knowledge they need if we want secure coding practices that have a greater focus on eliminating repeatedly exploited software weaknesses. The question that follows is typically, 'how can developers know which class of weaknesses display these hazardous patterns?' The answer lies within Known Exploitation Insights, which the five main types of weaknesses developers should work on addressing are:

a) Access Control
b) Improper Input Validation
c) Injection
d) Memory Safety
e) Resource Lifecycle Management

The bottom line is that many of the vulnerabilities that we know all too well that are listed in the Top 25 can be quelled through the implementation of better and more secure coding practices.

The stakes within the cybersecurity industry have never been higher than they are currently. This point is emphasized by CISA Director Jen Easterly:

"They [cyber attackers] are able to get into our critical infrastructure because of flaws and defects in our technology. But we have the power to change this. We can achieve long-term security through fundamentally more secure software. Building more secure software is the only way to catalyze more secure critical infrastructure."

This is why CISA's Secure by Design is so important and why Securin is proud to be a part of it. Secure by Design places secure practices at the core of everything pertaining to software and how we use it. Its seven pledges highlight the need for a holistic approach to mitigation and how there needs to be a more expansive view of risk.

To be precise: we need proactive cybersecurity.

Below are the Seven Secure by Design pledge goals – and the rationale behind them:

1. **Increase multi-factor authentication (MFA) use:**

The greatest defense against password-based attacks such as credential stuffing and password theft is MFA. Multi-factor authentication (MFA), in any configuration, has proven to greatly diminish the success rate of these attacks.

2. **Reduce default password use:**

Universally shared passwords – or default passwords – continue to be the catalyst for damaging cyber attacks. Replacing default passwords with more secure methods of authentication, such as MFA, is recommended to better protect yourself from these attacks.

3. **Reducing entire classes of vulnerability:**

The majority of exploited vulnerabilities today are due to classes of vulnerabilities that can often be prevented at scale via SQL injection, XSS, etc. Software manufacturers can reduce risk for their customers is by working to reduce classes of vulnerabilities at scale across their products.

4. **Increase installation of security patches:**

In addition to taking vulnerabilities out at source, software manufacturers can make it easier for customers to install security patches, such as by offering support and enabling automatic update functionality (by default, where appropriate).

5. **Publish a vulnerability disclosure policy:**

Coordinated vulnerability disclosure is a mutually beneficial norm for engaging with security researchers. In addition to a clear channel to report vulnerabilities, Security researchers receive authorization for testing under the policy. Software manufacturers benefit from receiving help from the security research community that can allow them to better secure their products.

6. **Transparent vulnerability reporting (including accurate CWE and CPE fields in every CVE record):**

In addition to serving as a standardized way to communicate actions that customers should take to protect against vulnerabilities, timely, correct, and complete CVE records allow for public transparency in vulnerability trends over time. This benefits individual companies and their customers alike, and the software industry more generally, by allowing software developers to better understand the most pressing classes of vulnerabilities over time.

7. **Evidence of intrusions logs to facilitate customers in breach detection and prevention:**

It is a necessity for organizations to detect cybersecurity incidents that have occurred and understand what happened. Software manufacturers can enable their customers to do so by providing artifacts and capabilities to gather evidence of intrusions, such as a customer's audit logs. By doing this, software manufacturers embody the Secure by Design principle of taking ownership of their customers' security outcomes.

Now What?

Cybersecurity is becoming part of the day-to-day software development and there is a new generation of software developers emerging that are tasked with operating in this newly converged IT/Security world. It is pleasing to see developers being encouraged to reduce the number of vulnerabilities in their products, because so often the conversation revolves around remediating vulnerabilities, when in actuality many vulnerabilities can be prevented on the assembly line before a product leaves the shop. To include the wider community and customers to aid in the security process, taking measures like including the vulnerability disclosure policy and security patch initiatives are great measures to take.

That is why CISA plays such a significant role in keeping the United States safe from cyberthreats, and it is our job as security leaders to recognize this and continue to sign pledges like Secure by Design that support the integrity of our critical infrastructure systems.

About the Authors

Kiran Chinnagangannagari is the Chief Product and Technology Officer at Securin. He is a highly accomplished and experienced executive with extensive experience in key leadership roles at major multinational companies. Kiran was the Co-Founder, President, and Chief Technology Officer at Zuggand, an Amazon Web Services Advanced Consulting Partner. Before Zuggand, Kiran was the Chief Technology Officer of the state of Arizona, where he was instrumental in advancing IT strategy and enabling efficient, innovative, and sustainable services. Passionate about helping people find solutions that make their lives easier, Kiran brings a deep understanding of leveraging technology to solve business challenges. Kiran can be reached online via LinkedIn and at https://www.securin.io/.

Ram is the Chairman and Chief Executive Officer of Securin Inc. Through his visionary approach and strategic decision-making, he has played a crucial role in establishing Securin Inc. as a reputable and pioneering figure in the cybersecurity domain. With a wealth of experience spanning more than two decades, Ram co-founded Cyber Security Works and RiskSense and held prominent positions at TIBCO Software. His educational background includes a Bachelor of Engineering degree from the Manipal Institute of Technology and a Master of Engineering degree with a specialization in Systems Engineering from the Georgia Institute of Technology. Recognized as a transformational leader at the WCRC Leaders Asia—The CEO Awards India 2022-2023, Ram's passion for philanthropy is evident through his active support of community-impacting initiatives. Ram can be reached online via LinkedIn and at https://www.securin.io/.

Segmentation is Key in U.S. Air Force's Zero Trust Strategy – How Other Agencies Can Follow Suit

By Gary Barlet, Public Sector Chief Technology Officer, Illumio

The U.S. Air Force recently released its Zero Trust Strategy, outlining strategic goals and objectives that enable Air and Space Forces to operate using Zero Trust in the future.

One focus of the strategy – Objective #5.4 – is expanding segmentation capabilities. It states that segmentation is the practice of breaking a unified system into smaller, isolated segments to apply more granular visibility and access controls to each segment. It highlights that the U.S. Air Force must evolve from network-based segmentation to data center, host-based, and micro-service level segmentation to provide the strongest controls.

As the U.S. Air Force and other Department of Defense (DoD) agencies work to meet the FY 2027 Zero Trust deadline, and federal agencies work to meet this year's September 30 Zero Trust architecture deadline, it is vital that robust measures to achieve the most secure environments possible are in place.

How the U.S. Air Force Has Already Begun Their Segmentation Journey

According to research by Gartner®, "By 2026, 60 percent of enterprises working toward a Zero Trust architecture will use more than one deployment form of microsegmentation, which is up from less than 5 percent in 2023." The U.S. Air Force is among the agencies already advancing their segmentation journeys.

For example, the U.S. Pacific Air Forces has used segmentation tools on their Zero Trust architectures to segment their users and networks to a more refined level. This granularity grants users access to only the data they need from anywhere connected to the cloud – protecting their data against adversaries. Additionally, the U.S. Air Force has leveraged segmentation to gain visibility into network communications and insights into potential vulnerabilities.

Reducing An Attack's Impact with Zero Trust Segmentation

Other agencies should follow the U.S. Air Force's lead on segmentation methods. Zero Trust Segmentation (ZTS), segmentation using Zero Trust principles, is a crucial technology measure within the Zero Trust framework. By adhering to the principle of "least privilege" access and continuous visualization of all communication patterns and traffic between workflows, devices, and the internet, ZTS constantly verifies connections and creates granular policies that permit only essential communication. In the event of an attack, ZTS isolates on and offline assets dynamically and enhances visibility across networks and traffic – limiting lateral movement and containing the attack's impact.

Implementing ZTS not only puts methods in place that will minimize the impact of an attack, but also reduces the blast radius of cyberattacks within an organization by 66 percent, ultimately saving organizations $1.8 million annually by decreasing overall risk exposure.

Starting the Zero Trust Segmentation Journey

To start their ZTS journeys, agencies should adopt an "assume breach" mindset, recognizing that cyberattacks are inevitable in today's expanding threat landscape. Adopting an "assume breach" mindset actively encourages agencies to put measures in place to minimize an attack's impact. It is not possible to prevent all attacks, but steps can be taken to detect and mitigate the spread.

Next, agencies must determine their security objectives and prioritize progress over perfection. Start small and focus on what's most pressing, then build up from there. Key security objectives should include:

- **Enhance Real-Time Visibility:** Agencies can't protect what they can't see. Identifying which high value assets – data, applications, systems, services and anything else that's both digital and mission critical – are most important to their security object is crucial and should be segmented. Agencies can bolster their visibility efforts through application dependency mapping, which helps agencies locate these assets within environments and understand traffic flows reaching them.
- **Understand Vulnerabilities:** Application dependency mapping also shines light on security policies that are monitoring and controlling the traffic flows, revealing potential vulnerabilities.

Through visibility, agencies can understand their risks, like high-risk pathways, and other vulnerabilities, and build out their ransomware containment efforts.

- **Block Known Ransomware Points:** As agencies segment their assets and block their most vulnerable ports after identifying them, enhanced real-time visibility will proactively reduce the blast radius and block known ransomware points – leading to a small, "quick win" for agencies.
- **Build a "Containment Switch":** This allows agencies to stop an in-progress incident from spreading. Controlled manually by the security team or as part of a script, the switch isolates the attack at the entry point. While the attacker is isolated, an application dependency map ensures vital operations continue.

These steps enable ZTS to establish the rules and policies for what's allowed and what's not. If an attack does occur, combining all these steps with ZTS guarantees minimum impact, regardless of where an attack originates – whether it's on an endpoint device, a vulnerable network, or a compromised cloud environment – and ensures operations can continue even while an agency is under active attack.

By preparing for and implementing ZTS, agencies can ensure that everyday attacks don't escalate into mission-impacting breaches – allowing them to focus on mission readiness and protecting the nation.

Gartner, Market Guide for Microsegmentation, Adam Hils, Rajpreet Kaur, Jeremy D'Hoinne, 12 June 2023

About the Author

Gary Barlet is the Public Sector Chief Technology Officer at Illumio, where he is responsible for working with government agencies, contractors and the broader ecosystem to build in Zero Trust Segmentation as a strategic component of the government Zero Trust architecture. Previously, Gary served as the Chief Information Officer (CIO) for the Office of the Inspector General, United States Postal Service. He has held key positions on several CIO staffs, including the Chief of Ground Networks for the Air Force CIO and Chief of Networks for the Air National Guard CIO, where he was responsible for information technology policy and providing technical expertise to senior leadership. He is a retired Lieutenant Colonel from the United States Air Force, where he served as a Cyberspace Operations Officer for 20 years. He can be reached at gary.barlet@illumio.com.

Sensitive Data Here, There, Everywhere – SaaS Security Beyond Core Apps

By Zehava Musahanov, Content Manager, Adaptive Shield

Organizations often focus on protecting sensitive data within their core applications — such as Salesforce, Microsoft365, ServiceNow, and Google Workspace — assuming these are the exclusive repositories of critical information. However, this mindset creates a dangerous and rather large blind spot for bad actors to exploit. Sensitive data doesn't just reside in core applications; it is spread across the entire digital ecosystem in lesser-known apps, unsanctioned apps, and interconnected third-party apps.

Expanding Beyond Core Applications

The misconception that sensitive data exists solely in core apps stems from the traditional approach to data management. Once upon a time, core applications were considered the primary holders of valuable information. However, as organizations adopted cloud services, integrated third-party applications, and

automated workflows, sensitive data began spreading into a wide variety of “non-core” apps. In recent years we’ve seen an increasing amount of breaches from non-core apps, targeted through various vulnerabilities and attacks.

One example is the breach at Snowflake, which led to the exposure of personally identifiable information (PII), including names, email addresses, physical addresses, and even partial credit card numbers. Similarly, Sumo Logic experienced a breach where compromised credentials were used to access the company’s Amazon Web Services account.

The long tail of smaller SaaS applications is also highly susceptible to breaches. In 2022, HubSpot suffered a breach when malicious actors compromised an employee account used for customer support, allowing them to access and export customer contact data from several HubSpot accounts. In another case, a misconfiguration in the JIRA collaboration tool exposed the internal data of major corporations and even NASA to potential leaks.

These breaches show that threats often originate from both simple security oversights and complex attack methods, highlighting the need for a proactive approach to SaaS security.

Which Applications Should be Monitored and Secured?

The challenge for organizations that adopt a strategy of monitoring only their core apps while leaving all their other apps to periodic manual audits is determining which applications require monitoring.

Almost every security professional would agree on the need to secure HR information, customer data, product roadmaps, go-to-market strategies, and legal documents. Applications that interact with sensitive databases would also require monitoring.

Despite that universal agreement on the need to secure that data, many organizations rely on manual audits to secure Adobe Sign (legal document repository), DropBox (company resources), Looker (business intelligence containing sensitive data), HiBob and Bamboo HR (HR applications with sensitive employee data), Chorus and Gong (applications containing sensitive customer data), and PowerApps (LCNC app builder with access to sensitive databases).

Nearly every SaaS application contains data that needs to be protected. Relying on a “core apps” strategy means leaving terabytes of sensitive data exposed to misconfigurations, configuration drifts, and poor access controls.

How Shadow Apps Increase Risk

Shadow apps, which are SaaS applications that the security team is unaware of, extends the issue further. This typically happens when employees adopt tools that simplify their workflow and are often not done so maliciously by employees. These tools, however, lack enterprise-level security measures, making them targets for cyberattacks. Without centralized oversight and monitoring, it becomes nearly impossible to control where sensitive data might end up.

Take a Full Stack Approach

To truly secure corporate data, security teams need to start from the premise that every application must be secured. Securing the full SaaS stack requires investment in a SaaS Security Posture Management (SSPM) platform and commitment from app owners and the security team to collaborate on SaaS security. While it can be challenging to introduce full-stack SaaS security, failure to do so will simply leave too much sensitive data exposed.

About the Author

After completing her BA in Communications, Zehava began her career diving into the world of content writing. She recently joined Adaptive Shield as Content Manager, bursting with ideas to create engaging discussion around SaaS security and the rapidly developing world of SSPM. She also does portrait drawings.

Zehava can be reached online at her LinkedIn and at our company website https://www.adaptive-shield.com/.

Get the Kickstarting a SaaS Security Program Guide now.

The Ripple Effect of National Data Breaches: A Wake-Up Call for AI-Era Security

By Sharat Ganesh, Senior Director, Product Marketing | Head, Cloud Security at Qualys

The Ripple Effect of National Data Breaches: A Wake-Up Call for AI-Era Security

It was just another Tuesday morning. With a steaming cup of coffee in hand, I settled into my routine of scanning the latest cybersecurity news. But then, I stumbled upon a headline that made my heart drop: a massive national public data breach. After fifteen years in this field, you'd think I'd become desensitized to such news. Yet, this one struck a chord—it felt like a glaring reminder of the vulnerabilities we face in this rapidly evolving, AI-driven paradigm. I couldn't help but think back to Equifax in 2017 and SolarWinds in 2020. Each time, we collectively gasp, make promises to improve our defenses, and then... life continues as usual. But should it? As I dug deeper into the details of this latest breach, I realized how our eagerness to adopt AI and digital acceleration might be leaving us more exposed than ever. I'll admit, I'm not immune to these pitfalls. Just last month, I found myself about to reuse a password for a new online account. Old habits die hard, right? That moment was a stark reminder: in today's hyper-connected world, my data isn't just mine. It's a potential gateway to my company's network, my family's finances, and even national security.

So, what steps can we take as individuals? Here are a few essentials: First, use a password manager. Ditch the post-it notes and let a password manager do the heavy lifting. Second, enable two-factor

authentication. Yes, it adds an extra step, but it's a small price for enhanced security. Third, think before you share. That seemingly innocent quiz about your first pet's name? It could be a goldmine for hackers. Finally, stay informed. Follow reputable cybersecurity news sources. Knowledge is your best defense.

While individual actions are crucial, they're just part of the equation. Organizations must also step up, especially as we dive deeper into an AI-first world. AI and machine learning are double-edged swords. They offer powerful tools for enhancing cybersecurity—think real-time threat detection and automated responses—but they also open new doors for attackers. Imagine AI models trained on compromised data; it's like handing a master key to a burglar. After years in the trenches, I believe organizations need a proactive, holistic approach to cybersecurity.

Continuous monitoring and assessment are essential; annual audits are outdated. We need real-time visibility into our security posture. A zero-trust architecture is also vital—in a world where the perimeter is blurred, trust no one and verify everything. Data minimization is key; if you don't need it, don't collect it. And if you do, encrypt it like your business depends on it—because it does. Lastly, employee education is crucial. Your team is your first line of defense. Make cybersecurity training as routine as coffee breaks.

A few weeks ago, I caught up with some CISO friends who shared a thought that resonated with me: "In this AI era, data isn't just an asset—it's a liability." Those words echo in my mind daily. We're at a crossroads. The potential of AI and digital transformation is immense, but so are the risks. It's like building a digital city—exciting and full of opportunities, but we must ensure our infrastructure is secure. This latest breach isn't just a wake-up call; it's a blaring alarm. Whether you're an individual user, a small business owner, or a corporate executive, it's time to reassess. Are you doing enough to protect your data—and by extension, the data of those who trust you? Remember, in cybersecurity, we're all connected. One weak link can compromise the entire chain. For me, this breach has rekindled my passion for cybersecurity. It's a reminder of why I entered this field: to help make our digital world a safer place, one byte at a time. What steps will you take today to secure your digital future? Let's work together to turn this wake-up call into action.

About the Author

Sharat Ganesh is a Cybersecurity Expert, and Senior Director of Product Marketing for Cloud Security at Qualys, where he plays a key role in shaping and promoting the company's cloud security solutions. With a strong background in cybersecurity and product management, Sharat has established himself as a leader in the field, particularly in areas related to cloud security and security operations. He is also a member of the prestigious Forbes Technology Council, product executive in residence at Mighty Capital, and a mentor/advisor at Data Security Council of India.

Sharat can be reached online at Linkedin and at our company website https://www.qualys.com/.

The Rise in Phishing Scams

By Marcelo Barros, Global Markets Leader – Hacker Rangers

As cybersecurity platforms have become more effective, cyber attackers have shifted their strategy. Rather than challenging defense applications to identify weaknesses, they are now increasingly focused on exploiting human behavior. Their primary method for enacting this updated strategy is phishing.

Phishing attacks have increased at an alarming rate in recent years, with reports showing a 58 percent increase in global phishing attacks from 2022 to 2023. The most probable reason for the increase is that phishing remains remarkably effective. Nine out of ten organizations report that they fell prey to phishing attacks in 2023, with nearly seven out of ten employees saying they contributed to the attacks' success by knowingly taking risky actions such as handing over credentials to untrustworthy sources.

Why does phishing continue to work?

One of the main reasons phishing continues to be effective is its focus on deep-rooted human emotions. Rather than seeking to overcome cyber defenses with computing power or zero-day exploits, it overcomes them by exploiting fear, greed, and empathy.

For example, due to security upgrades such as password generation and multi-factor authentication, breaking passwords has become much more difficult for cybercriminals. With phishing, however, cybercriminals can leverage fear to gain access to passwords. Falsified messages informing employees that their corporate expense account has been compromised and requesting login credentials to fix the problem count on those employees being afraid that the alleged breach will result in greater losses.

Greed is another powerful tool cybercriminals use to empower phishing attacks. A text or email promising access to an exclusive deal, for instance, can quickly prompt a greedy person to hand over sensitive information. According to Verizon's 2024 Data Breach Investigations Report, the median time it takes for someone to fall victim to a phishing attack — from receiving a phishing email to taking the requested action — is 60 seconds.

Phishing also continues to be effective because we are doing more online than ever before. When remote work skyrocketed in the wake of the COVID-19 pandemic, phishing attacks leveled at remote workers increased by 600 percent. As workplaces became distributed, it became more time-consuming and inconvenient to confirm that a text or email message actually came from a manager, opening the door for cybercriminals to exploit the new normal.

The rise of AI is yet another reason for the increased use of phishing attacks. Generative AI makes it much easier for cyber attackers to develop phishing campaigns. The power AI provides to create deepfakes also empowers new variations of phishing, such as vishing attacks that use AI to generate voice calls mimicking a boss or other person in authority.

How can organizations better repel phishing attacks?

Providing effective training is the most important step organizations can take to better repel phishing attacks. The training should provide a general understanding of how phishing works, how to identify it, and how to report it when it is suspected. It should also be updated regularly to include the most recent phishing strategies.

Every stakeholder in an organization should receive training on phishing. Because phishing is focused on exploiting an organization's employees rather than its security framework, it can be leveled against any employee — from the CEO to the newest entry-level hire — so excluding anyone from training creates a dangerous vulnerability.

Organizations that want to better repel phishing attacks should also help employees to prioritize cybersecurity. Cyberattackers often rely on victims overlooking telltale signs of a phishing attack because they are too busy or weary from an overwhelming workload. If employees don't feel empowered to take

appropriate steps to detect and repel phishing, even when it compromises their productivity, the organization will suffer.

An effective cybersecurity strategy must address the ongoing threat posed by phishing attacks. An organization's best defense will be employees who understand the threat and know how to repel it. Organizations that fail to empower employees create a vulnerability that cybercriminals will be quick to exploit.

About the Author

Marcelo Barros, Global Markets Leader of Hacker Rangers, is an IT veteran who has played an instrumental role in delivering cutting-edge cybersecurity solutions and services to clients around the world. His passion for cybersecurity led him to join the team at Hacker Rangers, a leading gamification company that makes cyber awareness fun and engaging for organizations worldwide.

Marcelo can be reached online at https://www.linkedin.com/company/hacker-rangers-security-awareness/ and https://www.instagram.com/hackerrangers.en and at our company website https://hackerrangers.com/.

What US Organizations Need to Know About EU's Digital Operational Resilience Act (DORA)

By Nikos Vassakis, Head of Consulting Services, SECFORCE

The Digital Operational Resilience Act (DORA) is an EU regulation many US firms may need to comply with.

After DORA comes into effect in January 2025, US financial entities that have EU customers and third-party providers will need to comply with DORA. The alternative is potentially prohibitive fines.

This means that any US-based but EU-facing hedge fund, broker (including crypto platform), bank, fintech, or any other kind of financial entity will soon have a new set of regulations to keep—though there are some exceptions.

Here's a quick breakdown of everything US companies need to know about DORA.

What Is DORA?

The Digital Operational Resilience Act (DORA) is the widest scope of EU financial sector cyber regulation to date. Much like the General Data Protection Regulation (GDPR) previously, DORA will put new obligations on companies that want to access the EU marketplace.

In practice, DORA is a cybersecurity-focused regulation. It aims to make financial institutions (FIs) take responsibility for the business risk (to their customers and the sector as a whole) created by cybersecurity incidents.

Anyone familiar with US regulations like PCI DSS, Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley Act (SOX), and frameworks like NIST CSF 2 will recognize DORA's requirements, which center around forcing FIs to get better at identifying and reporting security incidents and preventing them in the first place.

Summed up in a word, DORA is a "resilience" regulation.

DORA has five pillars of compliance. These are:

- Establishing robust ICT risk management frameworks.
- Managing third-party risks.
- Conducting regular digital operational resilience testing.
- Complying with strict incident reporting guidelines.
- Sharing threat intelligence with other financial entities.

These are the core themes of DORA's requirements, though numerous exhaustive obligations exist within these themes. You can read the full list of requirements on the official DORA website.

For some larger firms, DORA's demands may align with their current practices. The act's operational resilience requirements are stringent, but nothing really new.

For others, especially smaller financial firms, DORA brings new challenges around risk management, threat detection and incident reporting, and testing.

A big part of DORA compliance is introducing a level of offensive security into your security program. DORA introduces a new regulatory requirement for "threat-led penetration testing." Within its Resilience Testing pillar, DORA requires FIs to do testing every three years. However, "advanced penetration testing" is a bit of a misnomer. DORA testing requirements are more akin to the open-ended style of offensive security known as red teaming.

DORA Is Likely to Apply to a Wide Range of US Organizations

Almost every kind of financial institution is covered by DORA, including:

- Credit institution
- Investment firm
- Insurance or reinsurance undertaking
- Fintech company
- Payment institution
- Electronic money institution
- Central securities depository
- Crypto-asset service provider.
- Central counterparty
- Trading venue or repository
- Crowdfunding service provider
- Asset management company
- Data reporting service provider.

A select collection of financial institutions is exempt from DORA. You can see a list of who is exempt here.

DORA also applies to organizations that European Supervisory Authorities (ESAs) determine to be a critical ICT third-party service provider (CTPP). These organizations are not financial services organizations but provide critical services to the EU financial services industry. For example, a cloud services provider that several large banks rely on.

Deciding whether or not an organization is a CTPP is pretty complicated (and done on a case-by-case basis), but generally speaking, most big IT services providers with financial services clients, like Google Cloud (who have written about their approach to DORA recently), are likely to fall into this category.

Smaller US Firms Might Be Surprised By DORA

DORA is an extremely broad piece of legislation. Most financial services organizations will be covered regardless of turnover or business size.

However, DORA's requirements change based on the size and risk of the company. For example, microenterprises must only review their risk management frameworks periodically (instead of yearly - as required for larger organizations).

There Could Be Steep Penalties for US Organizations

Failing to comply with DORA will cost organizations 1% of daily global turnover for up to six months. It will severely hamper a firm's ability to access the EU market and its business reputation.

Based on what happened with the GDPR, DORA fines will likely be a) enforced heavily and b) increase with time.

DORA May Affect Existing Contracts with EU Clients

A core DORA focus area is contract management and third-party risk.

DORA will likely require US third-party providers to change parts of their contracts with any EU financial entity or other impacted businesses. For example, they might need to agree on new risk management and reporting standards.

Also, if a US business is deemed a critical third-party ICT service provider (CTTP) to EU clients, they might need to sign up for more new service level agreements (SLAs). These should include provisions for backup providers and compliance with additional regulatory standards.

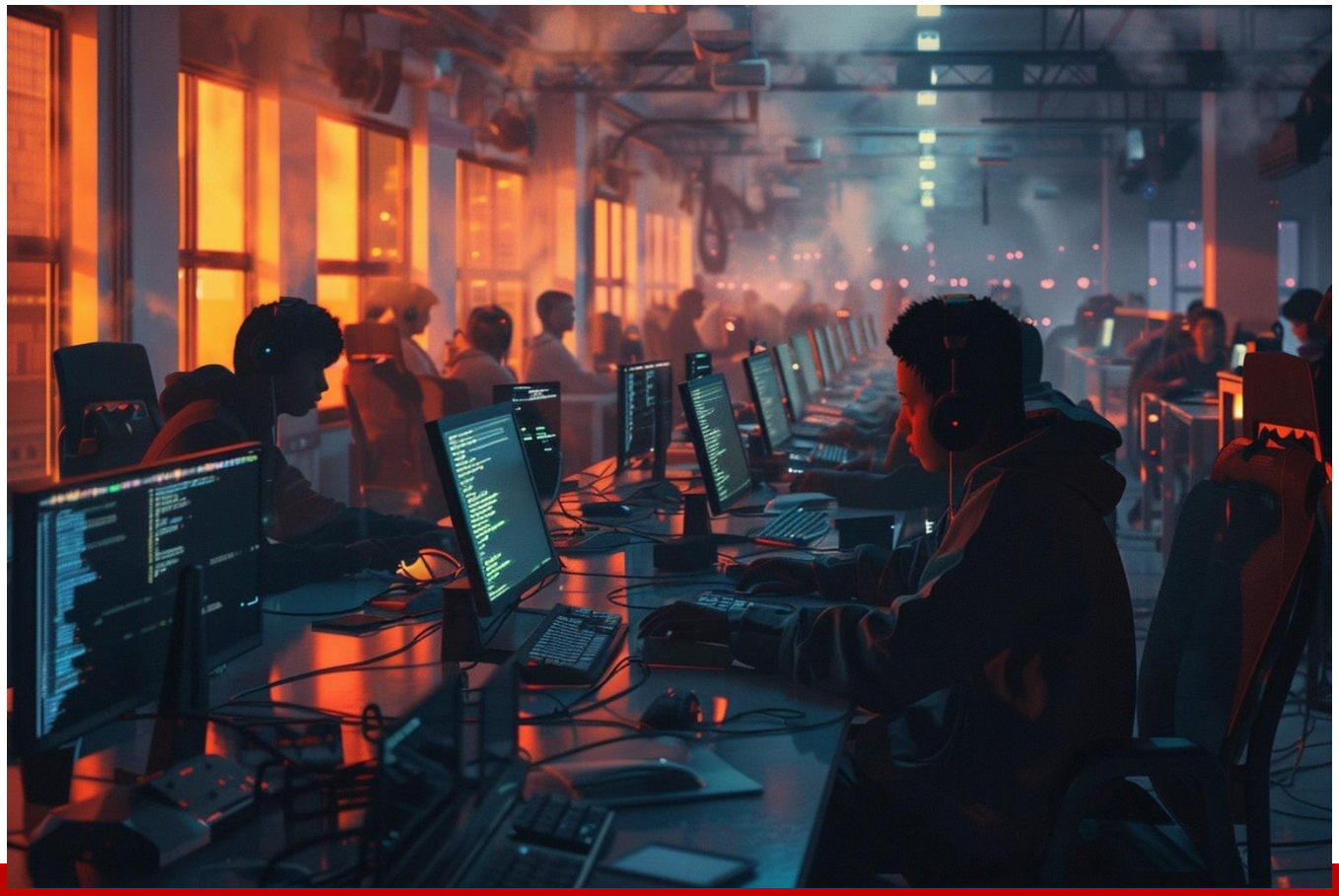
What Now?

The key DORA takeaway for US businesses is to check if you are covered and take action to comply as soon as possible. DORA noncompliance fines are unlikely to be a problem for the next 12 months, but they are coming.

About the Author

Nikos Vassakis is a seasoned Cybersecurity Professional with over a decade of experience and a Master's degree in Information Security. Starting as a penetration tester, he progressed through roles at several security consultancies, managed security services for a global financial institution, and an internal security team at a leading UK bank. These experiences have given him a deep understanding of the unique challenges faced by large-scale enterprises. His diverse background spans penetration testing, risk assessment, compliance, and strategic security planning. Currently, Nikos leads the security consulting practice at SECFORCE LTD, leveraging his extensive experience to guide organizations in strengthening their security posture across various industries and scales of operation.

Nikos can be reached at https://www.secforce.com/.



Why Crowdstrike's Single Point of Failure Wouldn't Happen with an API-based Solution

By Maor Dahan, Chief Technology Officer, Trustifi

Now that the industry has survived the largest IT outage in history, it begs the question: How could such a disaster be propagated by a security company that's used by more than half of all Fortune 500 businesses? How could such a well-known brand so easily trigger such a vulnerability in Microsoft's operating system?

As we've seen, one of the things that brought down CrowdStrike (and approximately 8.5 million Windows workstations) is the intrinsic level at which this solution interacts with Microsoft's core system. A traditional SEG-based (secure email gateway) software package like CrowdStrike interconnects with Microsoft's "kernel," which directly oversees management of system resources including memory, processing, and things as basic as input and output operations.

From the perspective of email cybersecurity, CrowdStrike's email data filters are embedded along the same path that the email data itself travels, within a network's security gateway. Surprisingly, many of

the market's largest cybersecurity brands are SEG-based, providing email security that is embedded within a network's email server, and with accompanying access to Microsoft's kernel—including other cybersecurity behemoths like Proofpoint.

This approach is in direct contrast with an API-based (application programming interface) cybersecurity solution. An API is more along the lines of a plug-and-play integration, which does not impede the user company's core operating systems.

"When the application code crashes, the application crashes," began David Plummer, a former Microsoft Windows developer, in a recent CrowdStrike outage video. "When kernel mode crashes," he continues, "the system crashes." Therefore, traditional SEG-based solutions—many of which are household-name software providers—are creating a susceptibility that API-based software simply doesn't produce.

An API allows system administrators to disable the program with a simple click, at the interface level. Which means if a patch or an update were to go wrong with an API-based, specialized cybersecurity solution, the issue could be nipped in the bud by disabling the application.

The Falcon Update was a Single Point of Failure

As an industry, we should consider the CrowdStrike Falcon update fiasco as a single point of failure scenario. Email security solutions that extend through the security email gateway make it more difficult, if not impossible, for end-user administrators or even managed services providers to override or disable that solution in such scenarios. However, API-based email security doesn't require an inline deployment. A more flexible API-based security integration therefore provides a better course of defense during a single point of failure situation.

In the case of a compromised update, disabling the API would have terminated the "endless reboot loop" created by the erroneous bit of Falcon code, which led to countless non-functional blue screens across the globe. Yet the huge institutions that control our global infrastructure—hospitals, airlines, banks, and government offices—depend on traditional SEG-based solutions, not realizing that next-generation, API-based security may provide greater advantages.

On top of all the malicious threats that are flooding the market, it's unfortunate that end-user companies now need to worry whether their branded security providers are positioning them for widespread system failures. Acknowledging this flaw, Microsoft has announced it is "prioritizing" a reduction of kernel-mode access by third-party software, to improve resilience. Although, the ability to divorce these conventional solutions from kernel access may be limited, due to how these existing solutions are designed. Without a fundamental shift in security architectures, Microsoft can only create so many protections in this case.

The CrowdStrike breakdown is reminiscent of what the industry feared would happen with Y2K, when the Millennium turned-over and date ranges within computer systems worldwide needed to be readjusted. But global failures never came to pass. Maybe just having the foresight to prepare is what kept us all from falling into the blue screen of death back then. Having the foresight to depend on API-based software may help in light of this new potential for system failures as well.

About the Author

Maor Dahan is Chief Technical Officer at Trustifi, a cybersecurity firm featuring solutions delivered on a software-as-a-service platform including sophisticated AI-driven tools. Trustifi leads the market with the easiest-to-use and deploy email security products providing both inbound and outbound email security from a single vendor. Maor can be reached through Trustifi or through LinkedIn.


EVENTS

GITEX GLOBAL

14 - 18 OCT 2024
DUBAI WORLD TRADE CENTRE

MON	TUE - FRI
11 AM - 5 PM	10 AM - 5 PM

THE LARGEST TECH & STARTUP EVENT IN THE WORLD

Global Collaboration to Forge a Future

AI ECONOMY

6,700+ Exhibitors | **187k** Visitors | **1,800+** Speakers

Where the visionaries and policy makers meet.

#GITEXGLOBAL
gitex.com

Scan the QR code to
SECURE YOUR PASS

ORGANISED BY
مركز دبي التجاري العالمي
DUBAI WORLD TRADE CENTRE

SECTOR

October 22-24, 2024

METRO TORONTO CONVENTION CENTRE

SecTor 2024 will celebrate its 18th annual conference with a live, in-person three-day program from October 22 to October 24 at the Metro Toronto Convention Centre in downtown Toronto.

As Canada's largest cybersecurity conference, SecTor provides an unmatched opportunity for security professionals to connect with their peers and learn from their mentors. SecTor is one of the global events in Black Hat's portfolio, and has expanded with new content programs and features. Today, SecTor includes Briefings, an expanded Business Hall, the Black Hat Arsenal program, Summit Day, and much more.

SecTor 2024 highlights include:

- Join thousands of cybersecurity professionals ready to network and share ideas, while bringing the latest in security education to Toronto.
- Explore the Business Hall and connect with expert cybersecurity practitioners, over 120 cutting-edge solution providers, discover new open-source tools at Black Hat's Arsenal, and learn from the pros in free-to-attend Business Hall sessions.
- Hear from experts as they present their ground-breaking research, new vulnerabilities, open-source tools, zero-day exploits, and more in 45 Briefings sessions.
- Participate in 40 Arsenal open-source tool demos and six labs revolutionizing the cybersecurity landscape.
- Engage with industry leaders during a full day of Summits on Tuesday, October 22. Summit programming includes the Executive Summit, The AI Summit at SecTor, and the Cloud Security Summit. Summits each require individual Summit passes to attend.
- Discover the Features Schedule which all pass holders can access, and includes Arsenal, Bricks & Picks, and more.

For more information on SecTor 2024 registration and event week details, please visit www.blackhat.com/sector/2024.

Black Hat is the cybersecurity industry's most established and in-depth security event series. Attendees can find Black Hat events in the United States, Canada, Europe, Middle East and Africa, and Asia.

#SECTORCA

FOLLOW US

11th Cyber & SCADA Security in Energy Sector 2024

prospero
EVENTS GROUP

Embark on a transformative journey with Prospero Events Group. This conference represents the pinnacle of Energy Sector Security Excellence, offering an immersive exploration into safeguarding critical infrastructure against evolving cyber threats.

REGISTER NOW

DATE:
28TH - 29TH OCTOBER

VENUE:

NH Amsterdam Zuid
Van Leijenberghlaan 221
1082 GG Amsterdam, Netherlands

www.energy-prospero.com info@energy-prospero.com +420 255 719 045

prospero
EVENTS GROUP

11th Cyber & SCADA Security in Energy Sector 2024

28 - 29 OCTOBER 2024 | AMSTERDAM

SPEAKER PANEL

DAMIEN PLOIX
Driving Cybersecurity Service Manager,
ENEDIS

MARIANO BUCCO
Cybersecurity Senior Manager,
TENARIS

GAETANO SANACORE
Group Security & Cyber Defence - OT Security Manager,
A2A

RONNY DE JONG
Security Technology Specialist,
MICROSOFT

ALI LARIBI
Founder & IT/OT Cyber Security consultant,
FORTRESS PLUS

DR. YMIR VIGFUSSON
CTO & Co-Founder,
KEYSTRIKE

QUSAI ALRABEI
Senior OT Cybersecurity Leader Global,
SCHNEIDER ELECTRIC

MARTA MAJTENYI
Director of Cyber Security Services, IT Governance, Risk, Compliance,
NORSK HYDRO

TJEERD ZWIJNENBERG
Sales Director Europe,
WATERFALL SECURITY SOLUTIONS LTD

KENNETH TITLESTAD
Director OT Cybersecurity,
SOPRA STERIA

BAS KRUIMER
Business Director Digital Systems & Grid Operations,
DNV

RYAN DAVIDSON
Principal Engineer for Cyber Security & Digital Grid Operations,
DNV

CLIFTON MONTGOMERY
Lead Cyber Security Architect and Engineer,
HONEYWELL

PRATEEK ARORA
Cybersecurity Sr. Expert,
ENGIE LABORELEC

SHARON CARO
Marketing Executive,
SALVADOR TECHNOLOGIES

IAN CUTHBERTSON
Director of Global System Engineering,
CYOLO

JEROEN WIJNANDS
OT Security lead,
ORANGE CYBERDEFENSE

MORE INFO

SPONSORED BY

waterfall
Cyolo
keystrike
SALVADOR TECHNOLOGIES

MEDIA PARTNER

CYBER DEFENSE MAGAZINE

18th Edition

CONNECTED BANKING

West Africa

" EMPOWERING SUSTAINABLE BANKING THROUGH DIGITAL INCLUSION AND INNOVATION "

November 19th and 20th, 2024

Accra, Ghana

Conceptualized and Organized by ICSA

Scan For More Details

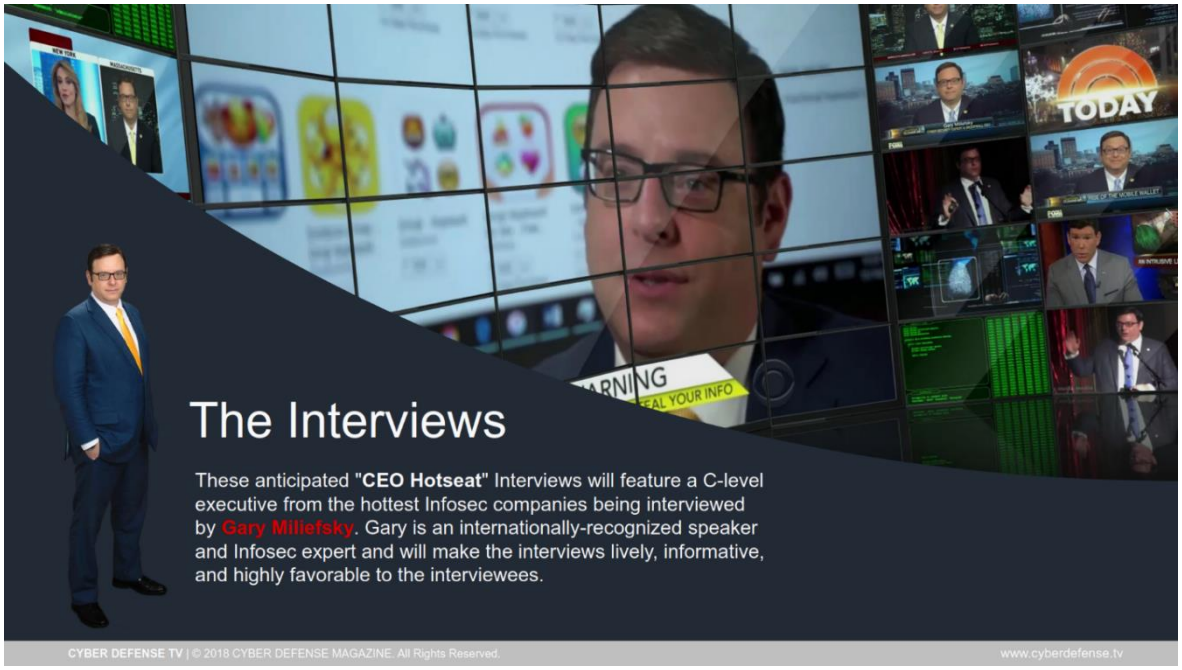
CYBER DEFENSE TV

INFOSEC KNOWLEDGE IS POWER

CyberDefense.TV now has 200 hotseat interviews and growing…

Market leaders, innovators, CEO hot seat interviews and much more.

A division of Cyber Defense Media Group and sister to Cyber Defense Magazine.



Free Monthly Cyber Defense eMagazine Via Email

Enjoy our monthly electronic editions of our Magazines for FREE.

This magazine is by and for ethical information security professionals with a twist on innovative consumer products and privacy issues on top of best practices for IT security and Regulatory Compliance. Our mission is to share cutting edge knowledge, real world stories and independent lab reviews on the best ideas, products and services in the information technology industry. Our monthly Cyber Defense e-Magazines will also keep you up to speed on what's happening in the cyber-crime and cyber warfare arena plus we'll inform you as next generation and innovative technology vendors have news worthy of sharing with you – so enjoy. You get all of this for FREE, always, for our electronic editions. Click here to sign up today and within moments, you'll receive your first email from us with an archive of our newsletters along with this month's newsletter.

By signing up, you'll always be in the loop with CDM.

Cyber Defense Magazine

276 Fifth Avenue, Suite 704, New York, NY 1000

EIN: 454-18-8465, DUNS# 078358935.

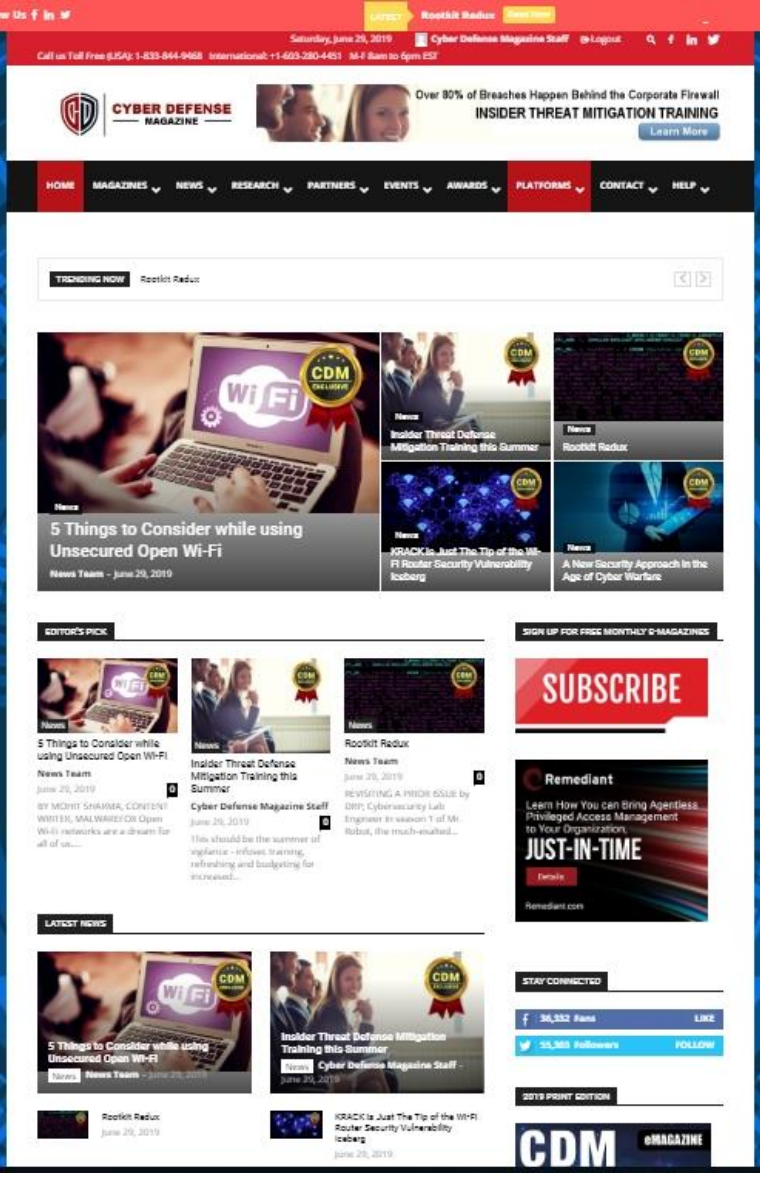
All rights reserved worldwide.

marketing@cyberdefensemagazine.com

https://www.cyberdefensemagazine.com/

NEW YORK (US HQ), LONDON (UK/EU), HONG KONG (ASIA)

Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 10/01/2024



Books by our Publisher: [Amazon.com: CRYPTOCONOMY®, 2nd Edition: Bitcoins, Blockchains & Bad Guys eBook : Miliefsky, Gary: Kindle Store] (with others coming soon...)

12 Years in The Making…

Thank You to our Loyal Subscribers!

We've Completely Rebuilt CyberDefenseMagazine.com - Please Let Us Know What You Think. It's mobile and tablet friendly and superfast. We hope you like it. In addition, we're past the five nines of 7x24x365 uptime as we continue to scale with improved Web App Firewalls, Content Deliver Networks (CDNs) around the Globe, Faster and More Secure DNS and CyberDefenseMagazine.com up and running as an array of live mirror sites. We successfully launched https://cyberdefenseconferences.com/ and our new platform https://cyberdefensewire.com/

CYBER DEFENSE MAGAZINE

WHERE INFOSEC KNOWLEDGE IS POWER

www.cyberdefensewire.com
www.cyberdefensetv.com
www.cyberdefenseradio.com
www.cyberdefenseawards.com
www.cyberdefenseconferences.com
www.cyberdefensemagazine.com

*** with help from writers and friends all over the Globe.**