CYBER DEFENSE
MAGAZINE

eMAGAZINE

JULY
2024

In This Edition

The Value of Trust: How Companies Can Harness Data Responsibly to Drive Growth

Who's Minding the Store?

Safeguarding The Backbone: The Critical Imperative to Protect Operational Technology (OT) Devices

...and much more...

MORE INSIDE!

`

CONTENTS

@MILIEFSKY

From the

Publisher…

TOP INFOSEC INNOVATOR NOW OPEN CYBER DEFENSE MAGAZINE 2024

Rise Above the Noise!

Following our recent announcement, we would like to remind our readers that The Black Unicorn awards program is now part of the Top InfoSec Innovator awards program. Please see detailed information at the Conference and Awards website:

https://cyberdefenseawards.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.

World's First Cyber Defense Genius™

For those readers who have not yet accessed this new facility, we are also pleased to remind you that Cyber Defense Magazine has launched the World's First Cyber Defense Genius™ the world's first AI GPT trained specifically on over 17,000 pages of infosec expertise and learning more, daily. It is now available on our home page at https://www.cyberdefensemagazine.com/ on the ride side of the screen. We welcome your comments and feedback as you take advantage of this excellent professional resource.

Cyber Defense Magazine Builds on History of over 12 Years… Looking Ahead

We continue to see growth in cyber threats and responses, including larger and more pervasive criminal attacks and corresponding larger cyber defense budgets in organizations across the board. We see many hundreds of billions in damages, potentially trillions in the coming years. We note the weaponization of artificial intelligence, data theft and the hundreds of billions of records, and 3500 cybersecurity companies and managed security service providers on the horizon with new and innovative ways to defend against the latest threats. The landscape continues to evolve but the fundamentals never change: managing your risk and increasing cyber resiliency are critical for any business to operate successfully in this heated cyber climate.

Our mission is constant - 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

http://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 July 2024 Issue

From the Editor-in-Chief

We continue to experience a broadening of important topics covering the practical needs of cyber professionals and non-technical users alike. Over the past year, coming across the Editor's desk, we have seen an increase in both the scope and number of articles addressing the growth of cyber-dependent activities.

Of the approximately 50 articles we receive, edit, and publish each month, we note the expansion of some themes and the appearance of new ones. Health care, from both providers and payments systems, continues to grow in frequency and scope. The expanded use of "patient portals" has introduced a new factor in cyber vulnerabilities: the internet-based access to sensitive patient files by consumers, who are by-and-large untrained in online security measures.

Financial institutions are experiencing a similar challenge, with both technical and social engineering exploits being perpetrated against bank customers. While the hacked data from the medical sector is usually monetized in the dark web market, bank customer exploits are designed to get direct access to depositor accounts.

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. With appreciation for the support of our contributors and readers, we continue to pursue our role as the premier provider of news, opinion, and forums in cybersecurity.

Wishing you all success in your cybersecurity endeavors,

Yan Ross

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

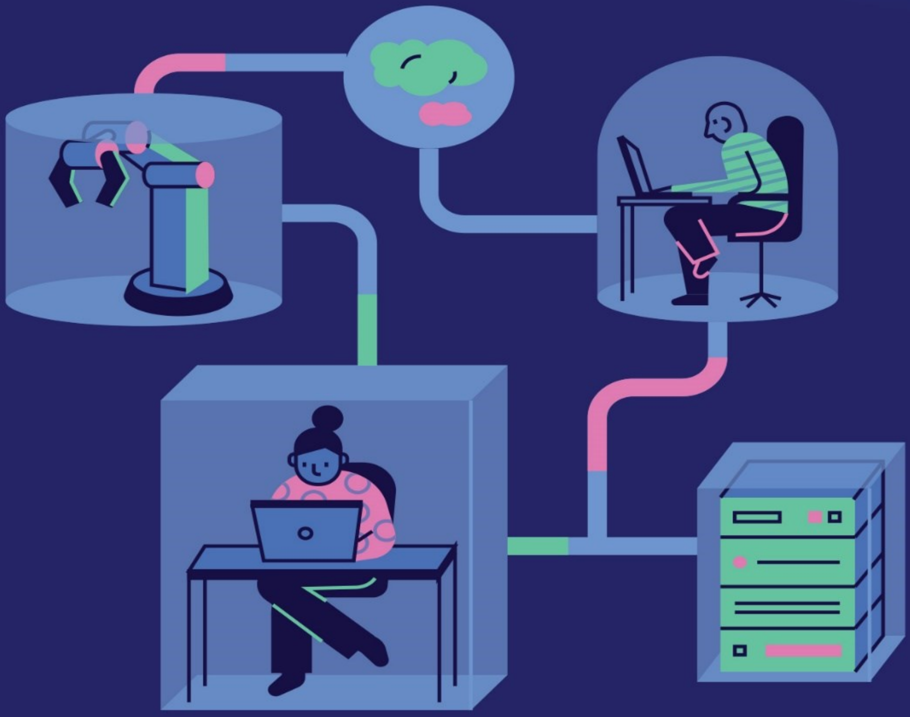
INVEST

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

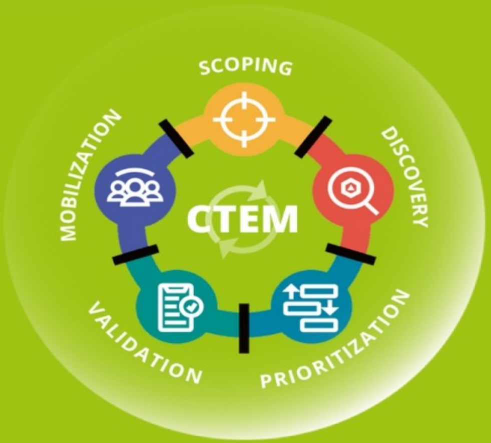
ACCELERATE

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

www.nightdragon.com



20
95
2
6
1
1
466


SCOPING
DISCOVERY
PRIORITIZATION
VALIDATION
MOBILIZATION
CTEM

Gartner Cool Vendor

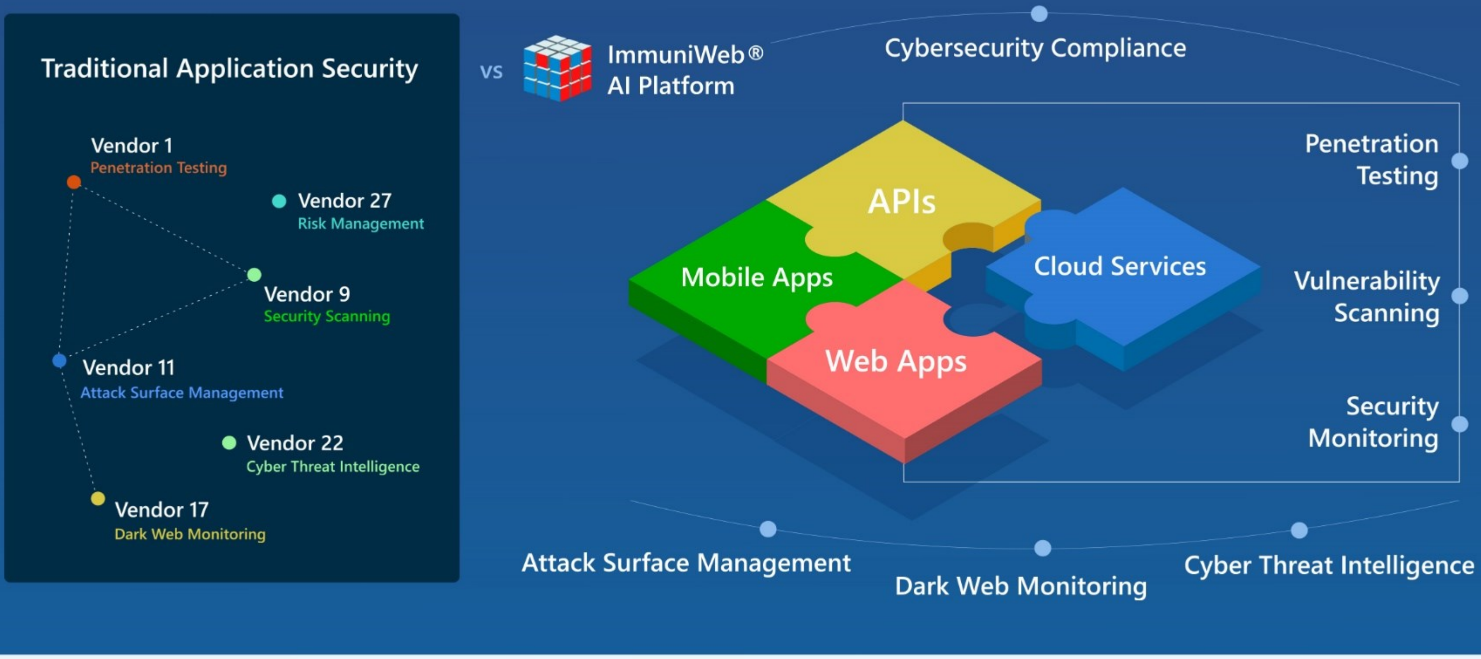
SC 2023 awards Europe highly recommended

IDC Innovator

ImmuniWeb®
AI for Application Security

Gartner peer insights ★★★★★ 4.9 out of 5

Risk-Based and Threat-Aware Application Security Testing (AST)



ebay · next bank CRÉDIT AGRICOLE · ITU · BDO · SIX · haymarket · unirisc group · Swissquote THE SWISS LEADER IN ONLINE BANKING

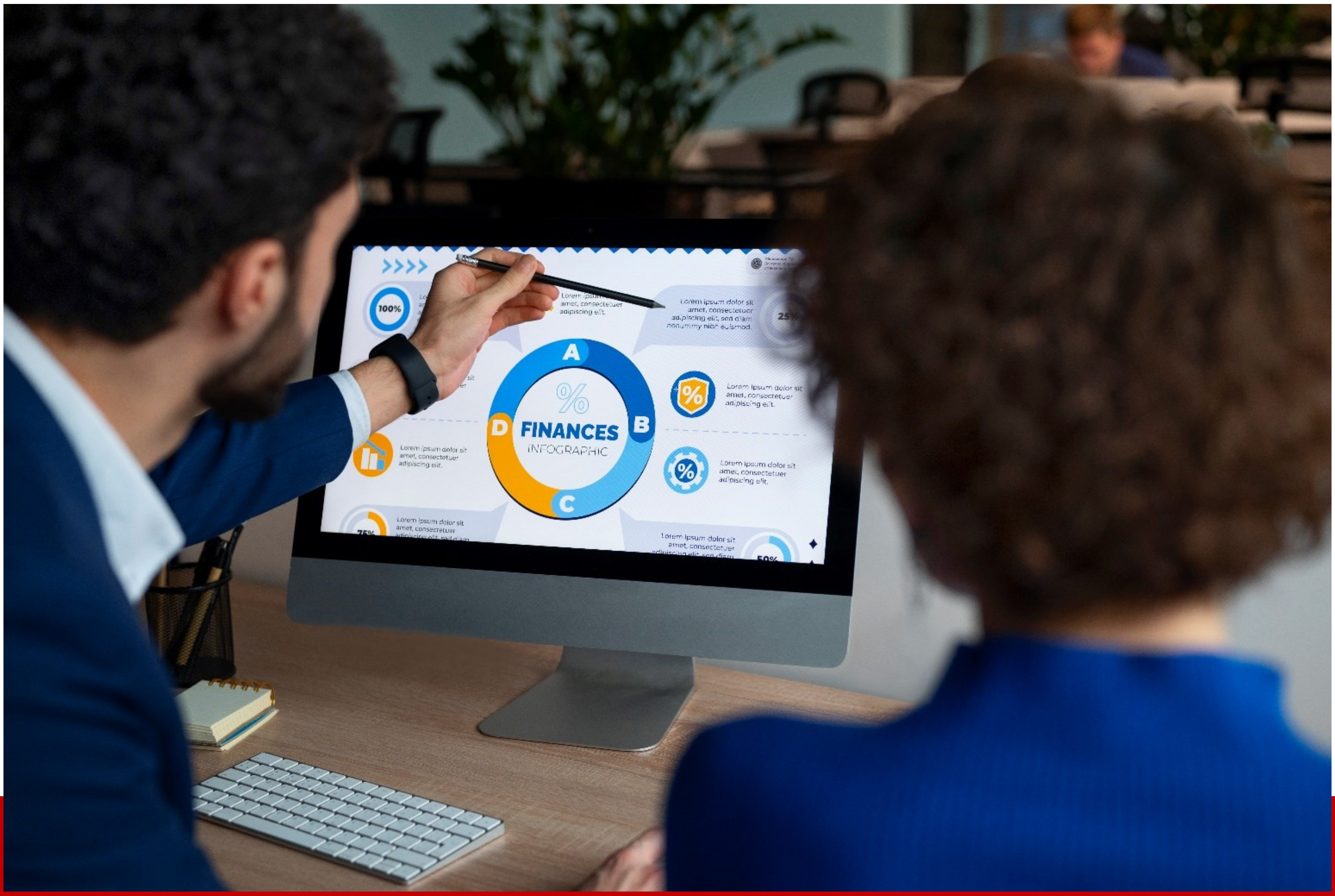
Award-Winning Technology. 20 Use Cases.

- Web Penetration Testing
- Third-Party Risk Management
- Cloud Security Posture Management
- Mobile Penetration Testing
- Attack Surface Management
- Red Teaming Exercise
- Dark Web Monitoring
- API Penetration Testing
- Web Security Scanning
- Cyber Threat Intelligence
- Continuous Penetration Testing
- API Security Scanning
- Continuous Automated Red Teaming
- Mobile Security Scanning
- Network Security Assessment
- Digital Brand Protection
- Phishing Websites Takedown
- Cloud Penetration Testing
- Software Composition Analysis
- Continuous Breach and Attack Simulation

One Platform. All Needs. **www.immuniweb.com**

CREST ACCREDITED · SGS · ISO/IEC 27001 SGS · UKAS MANAGEMENT SYSTEMS 005

ARTICLES



The Value of Trust: How Companies Can Harness Data Responsibly to Drive Growth

Data security and consumer trust go hand-in-hand in our evolving digital world

By Alasdair Anderson, Vice President for Europe, the Middle East & Africa, Protegrity

There’s no doubt that data is a catalyst of growth, forcing companies to increasingly rely on it to drive innovation and enhance consumer appeal. However, companies must focus on leveraging data for growth and ensure the protection and ethical use of consumer information. Establishing a strong foundation of trust with consumers is essential, particularly in light of increasing concerns over data breaches and privacy. As the cornerstone of data’s value, companies must have a strong social contract prioritizing data security to gain consumers' trust in supplying organizations with their data.

Crisis of Confidence Among Consumers

We have entered an era where consumer confidence is waning. According to a recent Cisco survey, 76% of consumers said they would not buy from an organization they did not trust with their data. This sentiment is echoed by the 81% of respondents from the same survey who agreed that how an organization treats its data indicates how it views and respects its customers. As privacy concerns escalate and data breaches become more prevalent, it is imperative for companies to forge a robust social contract that places the protection of consumer data at the forefront.

The absence of such a social contract can lead to dire consequences, including a significant erosion of consumer trust, which is the cornerstone of any successful business relationship. Moreover, companies are liable to legal and compliance repercussions in the event of data breaches, which can have long-lasting negative impacts on their reputation and financial standing.

Companies must embrace a privacy policy written in plain language. It should be obvious to the reader what data a company collects, uses, shares, and discloses about them. Transparency builds trust with consumers and trust delivers loyalty. The irony being that “loyalty” programs are some of the worst offenders, in terms of, a lack in transparency to their consumers. Practical steps can make a difference without much effort. Privacy policies easily found on website landing pages. Use plain language that is easily accessible and understandable for consumers. By doing so, companies can demonstrate their commitment to data responsibility and build consumer trust, an asset in building deeper brand relationships.

Recent Data Breaches

Businesses today thrive on a global infrastructure through the exchange of data. They collect, store, and share massive amounts of sensitive information like customer emails, addresses, and Social Security numbers, aiming to ensure the best customer service is maintained while also adhering to data protection and privacy laws.

However, the recent cyberattack on Change Healthcare serves as a reminder of the importance of harnessing data responsibly. This breach, poised to become the largest health data compromise in U.S. history, was precipitated by unauthorized network access. The attackers exploited an application used by staff for remote system access, deploying ransomware that ultimately led to credential compromise.

This breach highlights how thin of a line these businesses walk as the attack has impacted 129 million individuals and 67,000 pharmacies globally, including all our military hospitals around the world.

Enhancing Data Security and Consumer Trust

To enhance data security and foster consumer trust, organizations must strike a delicate balance between harnessing data for business growth and upholding ethical standards. Organizations must develop frameworks that not only enable data sharing but also adhere to stringent data protection regulations. The act of sharing data unlocks collaborative growth opportunities with external partners and supply chains, catalyzing economic gains.

To mitigate data-related risks, companies must transition from traditional tools to innovative solutions that meet industry compliance and enhance data accessibility. For instance, strategically leveraging third-party vendors is essential for harnessing cloud-managed data warehouses, applications, and analytical tools, allowing for the responsible extraction of business value from data.

Further, the industry needs to radically shift their thinking in the way they approach the sensitive data problem. Two questions, do I have high risk data like social security numbers? More importantly, how many people in your company should see that data in clear text?

The first question is a security question. The second question is a data consumption one. If the answers to the questions are “yes” and “very few” then why protect data at every request by the 99.9% of users? Invert the security model and the natural security state for this type of data is protected. Using tokenization techniques obfuscates the value for a reader but maintains 100% of the data utility for analytics. By implementing this model, only .1% of the requests require transformation to clear text. It markedly improves security posture, widens access to high value customer data, and accelerates it to the teams thirsty to innovate.

Harnessing Data Responsibly

Organizations must judiciously select solutions that not only comply with legal standards but also safeguard sensitive data types such as Personal Identifiable Information (PII), Protected Health Information (PHI), Payment Card Industry (PCI), and Intellectual Property (IP). Tokenization is a recommended approach by the regulatory bodies because it is an effective, principled approach that in the case of PCI renders systems out of scope for audit.

Zero trust principles applied to applications, users, and servers is a growing trend in security because when executed well it is particularly effective for cloud environments. Microsoft summarized the three principles of Zero-Trust as Assume Breach, Verify Explicitly, and Use Least-Privilege Access. By implementing tokenization, organizations are applying Zero-Trust directly to data. Minimizing risk throughout the data’s lifecycle from collection to its final application. This proactive approach to data security is essential.

In 2023 the security industry was $185 billion and grew 14% year-over-year yet data compromises are up 78%. It maybe is stating the obvious, but those numbers don’t add up for consumer privacy. Accenture estimates that by 2030 businesses will unlock $3.6T in data value. The value of data for businesses cannot be overstated. By investing in data security, embracing transparency, and adopting a Zero Trust approach, companies can protect sensitive data and maintain the loyalty of their customers.

As we look to the future, the responsibility lies with businesses to continually adapt and innovate in their data management practices, safeguarding the privacy and integrity of consumer data in our evolving digital world.

About the Author

Alasdair Anderson is the Vice President for Europe, the Middle East & Africa at Protegrity. Prior to joining Protegrity in 2020 Alasdair worked in Financial Services industry for over 20 years as a technology executive. Alasdair was an EVP at Nordea Bank in Copenhagen where he led the Data Technology division. Alasdair moved to Copenhagen after nearly a decade as a Director with HSBC in the Investment Banking technology area. Prior to HSBC, Alasdair worked in multiple data management roles for JP Morgan, BNP Paribas, RBS, Man Investments and other Financial Services companies.

Alasdair speaks frequently throughout Europe on the topics of Cyber Security, AI, Data & Analytics and Innovation. In 2017 Alasdair was appointed a Global Scot by the First Minister of Scotland for recognition of his effort to further Scottish Global Trade. A native of Glasgow, Scotland, Alasdair now resides in Amsterdam, The Netherlands. Alasdair can be reached online at ProtegrityTD@touchdownpr.com and at our company website https://www.protegrity.com/.

Who’s Minding the Store?

Why Operational Technology Security Has Become a Top Priority for Federal Security Leaders

By Heather Young, Regional Vice President US Federal, Claroty

The Federal OT footprint – from military base operations to their public utilities, from postal operations to NASA missions - is immense, which means the potential cyber attack surface is as well. As adversaries develop new tactics for potential OT-related disruption, Federal agencies and the Service Branches have been prioritizing OT now more than ever. (OT, sometimes referred to as cyber-physical systems, is defined as programmable systems or devices that interact with the physical environment or managed devices that interact with the physical environment.)

For Federal civilian and DoD agencies, defending against OT attacks presents unique challenges. A new study examining the state of OT security at Federal civilian and DoD agencies underscores the realities of the threat landscape they face and highlights how these Federal guardians have taken proactive measures to identify vulnerabilities and bolster their security posture.

In the study, Guardians of Government: The State of Federal OT Security, 90 percent of Federal OT administrators reported they have placed greater emphasis on OT security. And for good reason. Sixty-eight percent reported an OT cyber security incident in just the past year, and only 20 percent gave themselves an ‘A’ grade for OT security preparedness. When asked if they could mitigate and respond to an OT threat today, half of the respondents expressed a high degree of confidence.

The study provides a comprehensive assessment of the critical gaps they face and what best practices they’ve adopted to enhance operational security. The obstacles to achieving a desired state of resilience and readiness are multi-fold. They report gaps they seek to close in their OT security, including improved asset visibility, secure remote access and monitoring. Many Federal agencies face additional OT security challenges, such as managing broad geographic distribution of their connected endpoints and limited air-gapping. And 65 percent estimated that assets in their organization have reached end-of-life yet are still internet facing, thus adding to their cyber attack surface.

The good news is these leaders are taking proactive measures within their agencies to address their security needs, despite the complexity. First, they report significantly greater coordination between IT and OT organizations, and some agencies have even aligned these functions in their organizations. Second, more report that they have implemented continuous assessments and have begun standardizing risk models. And, they’ve focused on upskilling their teams to keep pace with both evolving technologies and persistent threats. These are all steps in the right direction and will ultimately result in greater resilience and higher levels of confidence in their ability to meet the threats of today and in the future.

As our Federal systems – and world – have become increasingly interconnected, and the extended Internet of Things has become a reality, it is vital that we safely protect the cyber and physical components of connected organizations. As these Guardians of Government have reported, the threats are real. However, the organizational processes and technologies exist today and, if implemented well - with up-to-date best practices and expediency - can meet these threats with confidence.

About the Author

Heather Young is regional vice president, US Federal, for Claroty. She is responsible for supporting and enabling clients across Federal, State and Local Government, and the Education sectors.

Heather can be reached at heather.y@claroty.com (@youngheather20 on X) and at https://claroty.com/.

Safeguarding The Backbone: The Critical Imperative to Protect Operational Technology (OT) Devices

By Joe Guerra, M.Ed, CASP+, Professor of Cybersecurity, Hallmark University

Introduction

Operational Technology (OT) devices, integral in controlling and monitoring industrial processes, have become prime targets for cyberattacks. Since late 2023, there has been a notable increase in attacks on internet-exposed OT devices, threatening to disrupt critical industrial processes and cause significant system outages. Many OT systems are inadequately secured, making them easy prey for attackers who exploit weak passwords and outdated software.

Understanding Operational Technology (OT)

What is OT?

Operational Technology (OT) refers to the hardware and software systems used to manage, monitor, and control industrial equipment, processes, and infrastructure. These systems are critical in various industries such as manufacturing, energy, utilities, transportation, and healthcare. OT systems include devices like Programmable Logic Controllers (PLCs), Distributed Control Systems (DCS), Supervisory Control and Data Acquisition (SCADA) systems, and other specialized control systems.

Why is OT Relevant?

OT systems are essential for the smooth operation of critical infrastructure and industrial processes. They ensure the efficient and safe functioning of physical systems by automating tasks, monitoring system performance, and providing real-time data for decision-making. The relevance of OT systems extends to several key areas:

- Industrial Automation: OT systems automate complex industrial processes, reducing the need for manual intervention and increasing efficiency.
- Critical Infrastructure: OT is crucial for managing utilities like electricity, water, and gas, ensuring these services are delivered reliably to the public.
- Safety and Reliability: OT systems help maintain safety standards by monitoring conditions and controlling operations to prevent accidents and failures.
- Operational Efficiency: By optimizing processes and providing detailed operational data, OT systems enhance the overall efficiency of industrial operations.

Given their importance, the security of OT systems is paramount. Any disruption or manipulation of these systems can have severe consequences, including physical damage, financial loss, and threats to public safety.

Timeline of Cyber Attacks on OT

Historical Context

The history of cyberattacks on OT devices reveals a concerning trend of increasing sophistication and impact. In 2000, a third-party insider incident in Maroochy Shire, Australia, caused a large spill of untreated sewer liquids by accessing OT systems without authorization. The 2010 Stuxnet worm marked a significant escalation, targeting Iranian nuclear facilities and physically damaging centrifuges. This was followed by Russian cyber actors de-energizing seven substations in Ukraine in 2015, affecting 225,000 customers, and a similar incident in 2016 causing a one-hour outage in northern Kyiv. The rise of double extortion tactics in 2020 further increased cyber activity against OT. By 2023, pro-Russia hacktivists were manipulating Human-Machine Interfaces (HMIs) in North America and Europe to cause equipment malfunctions.

Recent Attacks

Late 2023 saw a surge in cyberattacks on OT devices, especially those developed by Israeli companies, often linked to groups affiliated with Iran. In 2024, the Blackjack hacking group deployed destructive malware called Fuxnet against a Russian company, damaging filesystems and hardware components.

Where is This Happening?

Cyberattacks on OT devices are a global issue with significant incidents reported in:

- North America and Europe: Pro-Russia hacktivists have targeted Industrial Control Systems (ICS).
- Israel: There has been an increase in attacks on OT assets developed by Israeli companies.
- Russia: Industrial control systems have faced destructive malware attacks.

How is This Happening?

Several factors facilitate these cyberattacks on OT devices:

Weak Security Mechanisms: Many OT systems lack robust security measures, making them vulnerable to exploitation through internet scanning tools.

Outdated Software: OT devices often run on outdated software with known vulnerabilities, making them easy targets for cyberattacks.

Weak Passwords: Poor password management practices provide an easy entry point for attackers to gain unauthorized access.

Lack of Network Segmentation: Inadequate network segmentation allows attackers to move laterally within compromised networks, escalating the extent of damage.

How Was It Missed?

The vulnerabilities in OT systems have often been overlooked due to several reasons:

Legacy Components: Many OT systems use legacy components that are difficult to update and secure, leaving them vulnerable to modern threats.

Operational Priorities: OT environments traditionally prioritize safety, reliability, and process continuity over security, leading to delayed patching and updates.

Convergence with IT Systems: The increasing integration of IT and OT systems has expanded the attack surface, complicating the task of securing all components.

Why is This Happening?

The surge in cyberattacks on OT devices can be attributed to multiple factors:

Geopolitical Tensions: Conflicts, such as the Israel-Hamas war, have spurred targeted cyberattacks on critical infrastructure.

Economic Motives: Cybercriminals exploit OT systems for financial gain through ransomware and other extortion tactics.

State-Sponsored Attacks: Nation-state actors use cyberattacks to achieve strategic military and economic objectives.

Can It Be Fixed?

Addressing the risks posed by cyberattacks on OT devices requires a comprehensive approach:

Improving Security Hygiene: Regular vulnerability assessments, robust authentication methods, and effective monitoring are essential for enhancing security.

Reducing the Attack Surface: Implementing network segmentation and minimizing the internet exposure of OT devices can significantly reduce vulnerabilities.

Implementing Zero Trust Practices: Adopting a zero trust security model prevents lateral movement within networks, mitigating the impact of potential breaches.

Continuous Monitoring: Utilizing advanced monitoring tools to detect and respond to threats in real-time is crucial for maintaining security.

Mitigating Cyberattacks on OT Devices Using RMF and NIST SP 800-53

Operational Technology (OT) devices are increasingly becoming targets for cyberattacks, necessitating a robust and multi-faceted approach to security. The Risk Management Framework (RMF) and NIST Special Publication (SP) 800-53 provide comprehensive guidelines and controls to enhance the security posture of OT systems. Here’s how these frameworks can be leveraged to mitigate the risks:

Improving Security Hygiene

1. **Regular Vulnerability Assessments:**

- NIST SP 800-53 Controls: Implement controls such as RA-5 (Vulnerability Scanning) to conduct regular vulnerability assessments. This involves identifying, reporting, and mitigating vulnerabilities in OT systems.

- RMF Steps: The RMF process includes continuous monitoring and assessment of security controls. Regular vulnerability assessments are part of the “Assess” step, ensuring that vulnerabilities are identified and addressed promptly. [12][14].

2. **Robust Authentication Methods:**

- NIST SP 800-53 Controls: Utilize controls like IA-2 (Identification and Authentication) to enforce strong authentication mechanisms, including multi-factor authentication (MFA) for accessing OT systems.
- RMF Steps: During the “Implement” step, ensure that robust authentication methods are deployed and documented. Continuous monitoring of these controls is essential to maintain their effectiveness. [12][14].

3. **Effective Monitoring:**

- NIST SP 800-53 Controls: Implement controls such as SI-4 (System Monitoring) and CA-7 (Continuous Monitoring) to establish effective monitoring mechanisms. These controls help in detecting and responding to security incidents in real-time.
- RMF Steps: The “Monitor” step in RMF involves continuous monitoring of security controls to ensure they are functioning as intended and to detect any anomalies or breaches. [12][14].

Reducing the Attack Surface

1. **Network Segmentation:**

- NIST SP 800-53 Controls: Apply controls like SC-7 (Boundary Protection) to segment networks and restrict access to critical OT systems. This reduces the attack surface by limiting the pathways an attacker can use to reach sensitive systems.
- RMF Steps: During the “Select” and “Implement” steps, ensure that network segmentation strategies are chosen and deployed effectively. Continuous monitoring helps in maintaining the integrity of these segments. [12][14].

2. **Minimizing Internet Exposure:**

- NIST SP 800-53 Controls: Use controls such as AC-3 (Access Enforcement) and SC-5 (Denial of Service Protection) to minimize the exposure of OT devices to the internet. This includes disabling unnecessary services and ports.
- RMF Steps: The “Categorize” and “Select” steps involve identifying critical assets and selecting appropriate controls to protect them. Minimizing internet exposure is a key strategy in reducing vulnerabilities. [12][14].

Implementing Zero Trust Practices

1. **Zero Trust Architecture (ZTA):**

- NIST SP 800-53 Controls: Implement controls like AC-6 (Least Privilege) and IA-5 (Authenticator Management) to enforce zero trust principles. This includes ensuring that access is granted based on the principle of least privilege and is continuously verified.
- RMF Steps: The “Implement” and “Monitor” steps are crucial for deploying and maintaining a zero trust architecture. Continuous assessment ensures that access controls are effective and that any deviations are promptly addressed [12][14].

2. **Preventing Lateral Movement:**

- NIST SP 800-53 Controls: Use controls such as SC-28 (Protection of Information at Rest) and SC-29 (Heterogeneity) to prevent lateral movement within networks. These controls help in isolating compromised systems and protecting sensitive data.
- RMF Steps: The “Assess” and “Monitor” steps involve evaluating the effectiveness of these controls and ensuring that they are continuously enforced to prevent lateral movement [12][14].

Continuous Monitoring

1. **Advanced Monitoring Tools:**

- NIST SP 800-53 Controls: Implement controls like CA-7 (Continuous Monitoring) and SI-4 (System Monitoring) to deploy advanced monitoring tools that can detect and respond to threats in real-time.
- RMF Steps: The “Monitor” step is dedicated to continuous monitoring of security controls. This involves using automated tools to provide real-time insights into the security posture of OT systems and to detect any anomalies or breaches. [12][14].

2. **Real-Time Threat Detection:**

- NIST SP 800-53 Controls: Utilize controls such as IR-4 (Incident Handling) and SI-4 (System Monitoring) to establish real-time threat detection and incident response capabilities.
- RMF Steps: The “Monitor” and “Respond” steps ensure that any detected threats are promptly addressed and that incident response plans are effectively executed. [12][14].

By leveraging the RMF and NIST SP 800-53 controls, organizations can significantly enhance the security of their OT systems. This involves a comprehensive approach that includes improving security hygiene, reducing the attack surface, implementing zero trust practices, and continuous monitoring. These measures collectively help in mitigating the risks posed by cyberattacks and ensuring the resilience of critical infrastructure.

References

- NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations [12].
- NIST SP 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations [14].
- NIST SP 800-207: Zero Trust Architecture [9].
- NIST Risk Management Framework (RMF) [14].

Citations:
[1] https://csrc.nist.gov/news/2022/guide-to-operational-technology-ot-security
[2] https://www.agilicus.com/webinars/2023-04-11-protecting-critical-infrastructure-zero-trust-and-nist-800-53/
[3] https://insights.sei.cmu.edu/documents/73/2022_500_001_887544.pdf
[4] https://csrc.nist.gov/pubs/sp/800/207/a/ipd
[5] https://www.nccoe.nist.gov/sites/default/files/legacy-files/zta-project-description-final.pdf
[6] https://csrc.nist.gov/pubs/sp/1800/35/2prd
[7] https://www.energy.gov/femp/articles/cyber-securing-facility-related-control-systems
[8] https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf
[9] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
[10] https://www.nccoe.nist.gov/sites/default/files/legacy-files/ch-pe-project-description-final.pdf
[11] https://www.energy.gov/femp/operational-technology-cybersecurity-energy-systems
[12] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
[13] https://grcacademy.io/nist-800-53/controls/sa-15-5/
[14]
https://csrc.nist.gov/csrc/media/projects/forum/documents/2012/dec2012_cont_montor_risk_mgmt.pdf
[15] https://www.upguard.com/blog/third-party-risk-requirements-nist-800-53
[16] https://www.ivanti.com/blog/the-8-best-practices-for-reducing-your-organization-s-attack-surface
[17] https://www.titania.com/resources/guides/nist-sp-800-53-compliance-explained-how-to-be-compliant
[18] https://www.linkedin.com/pulse/assessing-improving-security-posture-critical-good-cyber-robert-bond
[19] https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf
[20] https://cvgstrategy.com/nist-special-publication-800-53/

About the Author

Joe Guerra, M.Ed., CASP+, Security+, Network+,Hallmark University. Meet Joe Guerra, a seasoned cybersecurity professor based in the vibrant city of San Antonio, Texas, at the prestigious *Hallmark University*. With a dynamic background as a cyber tool developer for the Department of Defense and the Air Force, Joe brings a wealth of practical knowledge and hands-on experience to the classroom. His journey in cybersecurity education is marked by a diverse teaching portfolio, having imparted wisdom at various esteemed universities across the nation, with a special focus on Texas.

Joe's expertise isn't confined to a single age group or skill level; he has an impressive track record of guiding students ranging from eager high schoolers to career-changing adults. His passion for education shines through in his ability to demystify complex cybersecurity topics, making them accessible and engaging. He thrives on the lightbulb moments of his students as they unravel intricate concepts once thought to be out of reach.

Beyond the realm of cyberspace, Joe is a dedicated father of three, finding joy and balance in family life. His creativity extends to his love for music, often strumming the strings of his guitar, perhaps reflecting on the symphony of cybersecurity's ever-evolving landscape. Joe Guerra stands as a testament to the power of passion, dedication, and the desire to empower through education. https://www.hallmarkuniversity.edu/

The Art of Possible: Redefining Cybersecurity in the Age of Data as the New Perimeter

By Nick Shevelyov, Founder and Managing Partner at vCSO.ai

I have now had the privilege of attending RSA for over 20 years, yet this conference never grows old! My RSA 2024 started on Sunday, speaking with a group of Cybersecurity executives on translating cybersecurity risks for a Board of Directors. The National Association of Corporate Directors (NACD) guidance on this topic came up a number of times, I find it useful, and you reference it as well.

The conference officially got started on Monday and was themed as "The Art of Possible". The conference served as a convergence point for over 40,000 cybersecurity professionals and business leaders in San Francisco’s Moscone Center and surrounding areas. This year's discussions delved into the forefront of cybersecurity innovations, addressing emerging threats, and the evolving landscape where data has become the new perimeter.

My key take-away, there are several important themes evolving in our industry and we have shifted from Identity as the new perimeter, to Data being the new perimeter of cybersecurity, and most companies are struggling to define that territory.

At times I have heard the analogy that cybersecurity is like a chess game. I would argue in chess you see the whole territory, or in this case the chess board. You know where all the pieces are, and you know how they are allowed to move. I think chess is too black and white, pardon the pun, related to the colors of the chess board. I think our craft is more like a series of poker hands, where we are making probabilistic bets based on incomplete data sets. Similar to only seeing your cards in poker and only the hands played by your opponents.

With that in mind, let's explore the pivotal insights from the conference, focusing on the implications of AI, data governance, geopolitical threats, quantum computing, and the importance of resilience in modern cybersecurity.

Artificial Intelligence in Cybersecurity

Artificial Intelligence (AI) emerged as a central theme, with over 100 sessions dedicated to exploring its impact on cybersecurity. The discussions highlighted both the opportunities and challenges presented by AI. Experts emphasized the necessity of distinguishing generative AI from other AI types and explored how large language models can enhance cybersecurity tools. AI's dual nature, acting as both a defender and a potential threat, was a recurring topic.

CrowdStrike CEO George Kurtz underscored the critical need for adopting AI-driven next-generation Security Information and Event Management (SIEM) solutions to stay ahead of cybercriminals. AI's ability to predict and prevent cyber threats before they manifest is seen as a game-changer. However, concerns about "shadow AI," akin to shadow IT, were raised, stressing the importance of monitoring and regulating unauthorized AI applications within organizations.

Data Governance: The New Cybersecurity Perimeter

Ten years ago, we started to analogize the data is the new oil. Given data may empower, but also imperil, I would suggest that day is the new uranium. Would you like to know where your uranium is?

As organizations increasingly digitize their operations, data has become the new perimeter in cybersecurity. I'm plagiarizing myself when I state "The World Bank defines governance as "the manner in which power is exercised in the management of a country's economic and social resources for development. Governance has been defined as the rules of the political system to solve conflicts between actors and adopt decision (legality)." Galileo Galilei, the Tuscan physicist, mathematician, astronomer, and philosopher who contributed to the Scientific Revolution, once said, "Wine is sunlight, held together by water." We can translate that into, "Resilience is execution, held together by governance." The RSA Conference 2024 brought data governance to the forefront, addressing the complexities of managing and securing data across different organizational levels. Effective data governance policies are crucial in ensuring compliance with evolving standards and protecting sensitive information.

Speaking of resilience…

Resilience Building: Beyond Technology

Resilience in cybersecurity goes beyond implementing advanced technologies. The RSA Conference emphasized the importance of fostering collaboration across different stakeholder groups to build a resilient cybersecurity posture. Mandiant CEO Kevin Mandia highlighted the evolving tactics of ransomware groups and the necessity of a holistic approach to resilience. Here is a simple question to ask yourself as a Chief Security Officer when things go sideways, “Who will suffer with me when we have a serious breach?” If you don’t have a list of stakeholders incentivized with skin in the game, you don’t have a collaborative and resilient team in place. Today is a good time to start building one.

Geopolitical Concerns and Cybersecurity

The intersection of cybersecurity and geopolitics was a significant focus at RSA 2024. With the rise of nation-state actors and their sophisticated cyber campaigns, the need for a robust and coordinated defense strategy has never been more critical. CISA Director Jen Easterly highlighted the increasing threats from countries like China and emphasized the importance of building a "secure by design" infrastructure.

The voluntary pledge signed by 68 leading software manufacturers to enhance product security from inception was a notable development. This pledge aims to address common vulnerabilities, promote multi-factor authentication, and improve transparency in vulnerability disclosures and can’t hurt in the age or Ransomware, also a hot topic at the conference. Such collaborative efforts are essential in fortifying national cybersecurity defenses.

Quantum Computing and Cryptography

Quantum computing, with its potential to revolutionize data processing and encryption, was another interesting theme. Renowned cryptographers, including Whitfield Diffie and Adi Shamir, discussed the implications of quantum computing on current cryptographic techniques. The panel addressed concerns about quantum computers breaking existing encryption standards and the need for developing quantum-resistant algorithms.

Recent advancements and scares in quantum computing have underscored the urgency of preparing for a post-quantum world. Organizations are advised to stay informed about developments in this field and begin planning for the transition to quantum-safe cryptographic methods.

The Future of Cybersecurity: Embracing the Art of Possible

As we look ahead, the insights from RSA Conference 2024 provide a roadmap for navigating the complex and ever-evolving cybersecurity landscape. The theme "The Art of Possible" reminds us that while challenges are inevitable, they can be overcome through innovation, collaboration, and a forward-thinking mindset.

1. Adopt AI-Driven Solutions: Leveraging AI to enhance threat detection and response capabilities is crucial. Organizations must stay vigilant about the ethical and secure use of AI to prevent it from becoming a double-edged sword.
2. Prioritize Data Governance: With data as the new perimeter, robust data governance policies are essential. Ensuring data integrity, compliance, and security across all levels of the organization can mitigate risks and enhance overall cybersecurity posture.
3. Strengthen Geopolitical Defense: In the face of rising nation-state threats, a coordinated and proactive defense strategy is vital. Collaborative initiatives like the "secure by design" pledge can significantly enhance national and organizational cybersecurity resilience.
4. Prepare for Quantum Computing: Staying ahead of quantum computing advancements and planning for quantum-resistant cryptography will be critical in maintaining secure communications and data protection in the future.
5. Build Resilience Through Collaboration: Technology alone cannot ensure cybersecurity. Building resilience requires a collective effort from all stakeholders, fostering a culture of security awareness, and promoting collaboration across different sectors.

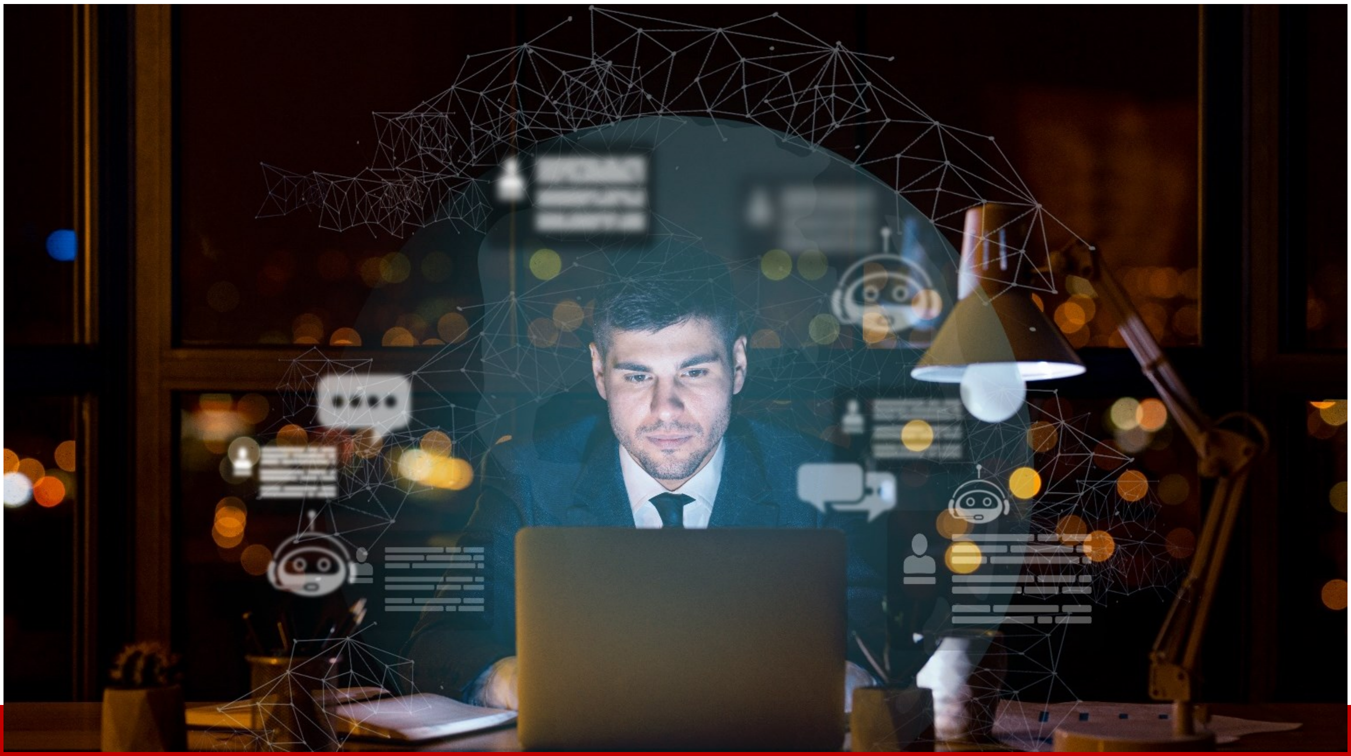
The RSA Conference 2024 has set the stage for a future where the possibilities in cybersecurity are boundless. By embracing innovation, prioritizing data governance, and fostering collaboration, we can navigate the challenges ahead and secure a safer digital world.

Conclusion

Key takeaways from the RSA Conference 2024 underscore the dynamic nature of cybersecurity as data has undeniably become the new perimeter. Effective governance, combined with cutting-edge technology and collaborative efforts, will be key to managing the risk probabilities we face. Embracing the "Art of Possible" is not just a theme but a call to action for the cybersecurity community to rise to the challenges and create a resilient, secure world. Thank you to Gary Miliefsky and the team at Cyber Defense Magazine. I will be speaking at their annual conference this October 31st – November 1st. Gary and team run a top notch event and I encourage you to attend!

About the Author

Nick Shevelyov is the Founder and Managing Partner at vCSO.ai, a cybersecurity and data privacy Advisory and Consulting firm helping companies enhance their risk strategies and product companies improve their go-to-market storytelling and channel development. He is the former Chief Security Officer (2007 - 2021) at Silicon Valley Bank, the bank of the innovation economy. He is the author of “Cyber War…and Peace”, has been published various periodicals, sits on the Board of Directors of the Bay Area CSO Council, and advises several Venture Capital and Private Equity firms.



RSA Conference 2024: Exploring our Current Cybersecurity Realities Amidst AI Myths

By Kylie Amison, Special to Cyber Defense Magazine

AI. Artificial Intelligence. One acronym, two words that seem to have reshaped the landscape of cybersecurity. At the 2024 RSA Conference, it was ubiquitous: stamped on almost every booth's showcase, invoked in nearly 150 speaker sessions, and echoed in my many interviews with C-level executives.

According to Vasu Jakkal, Corporate Vice President at Microsoft Security, it's estimated that 93% of organizations have some AI usage [1], reflecting the booming market projected to reach $407 billion by 2027 [2]. But what truly constitutes AI, and how does it differ from the already adopted machine learning technology? Are companies genuinely utilizing AI as professed? And if so, how do we, cybersecurity professionals, protect and govern something that is evolving so fast?

More concerningly, are attackers leveraging AI like we believe they might be? In both conversations with industry experts and attendance to keynote sessions highlighting current trends in security, I gained intriguing perspectives and observations, shedding light on our current cybersecurity realities amidst the pervasive use of AI.

Artificial intelligence represents the advanced technology that allows computers and machines to mimic human intelligence and solve intricate problems efficiently. This innovation, often integrated with tools like sensors and robotics, enables the performance of tasks traditionally requiring human thinking. From the widespread use of digital assistants to the precision of GPS navigation and the independence of self-driving cars, AI has manifested in numerous domains of our modern life. As AI continues to integrate into various industries, the conversation around ethical AI and responsible usage, and maintaining security becomes increasingly critical. [3].

Despite the widespread claims of AI adoption, many companies may not be utilizing true artificial intelligence but rather relying on machine learning techniques. While these terms are often used interchangeably, they represent different scopes and capabilities within the realm of advanced technology. As AI encompasses a broader scope of capabilities, machine learning operates as a subset within AI, focusing on the autonomous process of enabling machines to learn and improve from experience. Rather than relying on explicit and hardcoded programming, machine learning utilizes algorithms to analyze lengthy datasets, extract insights, and then make informed decisions.

As the machine learning model undergoes training with increasing volumes of data, its proficiency and effectiveness in decision-making progressively improve. While many companies harness the power of ML algorithms to optimize processes and drive insights, the utilization of true artificial intelligence is somewhat limited in adoption. Consequently, the threats and vulnerabilities associated with each differ significantly; machine learning systems are often susceptible to data poisoning and model inversion attacks, whereas AI systems face broader issues like hallucinations and adversarial attacks.

For instance, Jonathan Dambrot, CEO of Cranium, discussed how AI systems can "hallucinate," generating inaccurate outputs or falling prey to prompt-based threats. He stresses the importance of balancing the drive to adopt AI with a thorough understanding of its security implications. Organizations, fearing obsolescence, rush to implement AI without fully considering these risks, thereby exposing themselves to potential threats.

Brandon Torio, an AI expert and Senior Product Manager at Synack, identifies prompt injection as the most pressing threat to AI today. He distinguishes between security content management and traditional cybersecurity, emphasizing that to mitigate these risks, organizations must adopt a proactive approach. Torio advocates for "shifting left" in the development process, meaning thorough pre-deployment testing to catch vulnerabilities early. He acknowledges AI's benefits, such as making data more digestible and streamlining mundane tasks like simple script writing. However, he asserts the irreplaceable role of human oversight in contextualizing and interpreting AI-generated results.

In another conversation with John Fokker, Head of Threat Intelligence at Trellix, he noted that attackers are not leveraging AI as extensively as often portrayed or believed. He argues that while AI can assist attackers with tedious tasks like exploit development or creating deepfakes, it is not essential for most cybercriminal activities. "A human is more creative than a machine," Fokker states, underscoring the continuing superiority of human ingenuity over AI in crafting sophisticated attacks.

After attending and experiencing RSA 2024, and having had the opportunity to interview industry experts, my concluding thoughts are this: to harness AI's potential effectively, a balanced approach that includes proactive security measures and human oversight is crucial. While AI can, and does, offer unprecedented capabilities, it also introduces new vulnerabilities that require diligent attention.

The industry's leaders agree that a thorough understanding of AI's limitations, coupled with thorough testing and ethical considerations, is essential to protecting our digital landscape and future digital endeavors. As we continue to integrate AI into our cybersecurity frameworks, it is imperative to remain vigilant and adaptable, ensuring that technological advancement does not outpace our ability to secure it.

References:

[1] RSAC 2024 keynote speaker session “Securing AI: What We’ve Learned and What Comes Next”

[2] https://www.forbes.com/advisor/business/ai-statistics/

[3] https://www.ibm.com/topics/artificial-intelligence

About the Author

Kylie Amison is a proud alumnus of George Mason University where she obtained her Bachelor of Science degree in Cybersecurity Engineering with a minor in intelligence analysis.

She is working full time at a leading mobile security company as an Application Security Analyst where her main tasking involves pen-testing mobile applications, secure mobile application development, and contributing to exciting projects and important initiatives that are consistently highlighted throughout the security industry.

In addition, Kylie contributed to a startup company as a cybersecurity software developer where she was the lead developer on one of the company’s products; a geopolitical threat intelligence engine that combines a broad assortment of metrics and NLP sentiment analysis to calculate nuanced and real-time threat scores per nation state. Contributing to this initiative has been pivotal in her knowledge of creating secure software and has given her the opportunity to not only develop her first product, but to also start her own startup company, productizing the software and capabilities created in her threat intelligence engine. She is presently co-founder and CTO of Xenophon Analytics.

Throughout all of her experiences and coursework, she has gained essential skills in secure software development, penetration testing, mobile security and a plethora of coding languages. She has further aspirations of going back to school to get a graduate degree in the field of digital forensics and cybersecurity.

Beyond academics and professional life, Kylie enjoys watching anime, reading, and doing anything with nature involved. When asked her ultimate goal in life, she responded with “My goal in life is to learn every single day, and I am proud to be doing just that.”

Balancing the Scales: Addressing Privacy, Security, and Biases in AI based on the White House Blueprint for an AI Bill of Rights

By Céline Gravelines, Director of Cybersecurity Professional Services, Keyavi

Within the last few weeks, the major AI competitors OpenAI, Google, and Microsoft unveiled several new products and capabilities of their platforms. Perhaps, most notable was OpenAI's ability to now process speech and visual inputs in real-time. Social media was flooded with a mix of responses and many potential use cases. It's unavoidable at this point – AI is not only here to stay, but it is already transforming many industries and beginning to be commonplace in the consumer's everyday life.

Many CISOs are well aware that despite the gained efficiencies of AI, there are several major risks that need to be carefully examined. First, and most often cited, are the issues of privacy and security which enter a new level of importance now that these models are capturing voice and visual input and are even beginning to be worn on your person, as wearable AI seems to be next big thing. Second, and less often discussed, these algorithms can further exacerbate inequalities amongst already marginalized groups and technology illiterate. As the pace of innovation and rate of change increases, many will be left behind.

In this article I'll attempt to tease out some of the more granular issues that are being overlooked or under-examined. As a point of reference, I will use the current White House Office of Science and Technology Policy (OSTP) Blueprint for an AI Bill of Rights and will discuss other potential measures for regulation and best practices to improve trust, transparency, safety, and accountability, while minimizing harm of AI, particularly as it relates to marginalized communities.

The AI Dilemma

To put it simply, AI relies on massive amounts of data to create statistical correlations in order to accelerate decision-making. In the context of generative AI, models can create new text, image, sound, and more based on the training data sets. These operations have risks around privacy and security, and are already grappling with generating output that may be seen as bias or discriminatory.

Privacy and Security

AI algorithms are dependent on vast amounts of personal data being collected, stored, and analyzed. Like with any technology, the potential for data breaches and unauthorized access poses severe risks. Data leaks, tampering, and downtime of essential services can have significant effects on individuals and businesses depending on the AI systems. Effective cybersecurity controls must be implemented to minimize the likelihood of exposure, misuse, and other compromise. By its nature, the complexity of AI systems often makes it challenging for users to understand how their data is being used, raising concerns regarding transparency and true informed consent. Do you know what data is being collected and how it's being used and shared? Even if you know, can you do anything about it? Clear communication and implementing robust data privacy and security practices is critical to the effective protection of users.

Bias and Discrimination

AI algorithms depend heavily on the quality of the training data they receive and unfortunately, numerous headline-making stories have demonstrated the inherent risk of these platforms inadvertently amplifying existing biases which can lead to the unfair treatment of different groups, often those already marginalized. Gender biases in training sets can lead to unequal treatment, as shown in the well-documented case of Amazon's recruiting tool that was trained on previous resumes, which were predominantly men's, thus leading to the algorithm inadvertently favoring male applicants.

Leveraging biased data sets may also perpetuate systemic racism, leading to discretionary decision-making affecting equal employment opportunities, financial lending, or law enforcement. One example is demonstrated as an AI-based tool used to score the likelihood of criminal re-offense incorrectly labelled Black defendants as twice as likelihood to reoffend as white defendants. Having human intervention and fallback mechanisms are crucial in these situations before the biases are known. But that said – and knowing that nothing is ever easy – there are highly publicized instances of AI being over-corrected by manual intervention, such as with Google's Perspective API, an AI tool developed to curb hate speech online. It faced criticism that it was overcorrecting and censoring words used in benign contexts and sparking conversations about free speech and policing AI.

Blueprint for an AI Bill of Rights

To address the aforementioned risks, many have looked to government regulations. One example is provided by the White House Office of Science and Technology Policy (OSTP) which introduced a Blueprint for an AI Bill of Rights in 2022, designed to protect civil rights of the American public as the world adapts to AI seeping into nearly every aspect of society. This framework outlines five principles:

Safe and Effective Systems

AI systems must be thoroughly vetted with rigorous testing and ongoing monitoring to ensure they are safely and effectively operating. This is achieved with pre-deployment testing, risk identification and mitigation, and continuous monitoring. Implementing safety measures with regular audits to verify system performance and reliability is key to this success. The foundational goal of protecting users from harm, along with building public trust in AI technologies is dependent on prioritizing both safety and efficacy of these systems. Transparency is paramount in the development process, so that AI systems are both technically sound and in alignment with ethical standards and user expectations.

Algorithmic Discrimination Protections

AI systems must be prevented from perpetuating existing biases and discrimination, while designed in an equitable way. Designers, developers, and deployers of AI systems must include safeguards to actively identify, address, and mitigate biases in algorithms and data sets. Leveraging diverse and representative training data helps proactively minimize the risk of discriminatory outcomes. The use of regular audits and impact assessments can aid in detecting and correcting biases in the AI decision-making processes. By implementing these protections, AI systems are better positioned to treat individuals fairly, regardless of race, gender, religion, or other protected classifications, leading to more inclusivity and effectiveness.

Data Privacy

The rights associated with strong data privacy and security protections underscore the criticality of individual control and agency over personal data. Achieving this principle involves preventing compromises around unauthorized access, misuse, and exploitation requires robust security practices to be in place, along with providing transparency about data collection practices. Individuals must be clearly informed about how their data is being used and given the opportunity to make informed choices about that collection and usage. AI systems should leverage privacy by design model with default protections in place, such as only collecting data necessary for functionality in order to support the goal of trust and transparency with AI.

Notice and Explanation

By now, the ongoing theme of transparency is clear. Understanding the operations of AI is critical for ethical and true consent. AI should not be hidden, but rather, individuals should be clearly informed when and how AI is being used with accessible, understandable, and technically valid language. By ensuring that individuals grasp AI's involvement, logic, and decision-making processes, more trust can be established and potential issues like biases can be easier identified.

Human Alternatives, Consideration, and Fallback

While AI is advancing at an incredible rate, offering efficiencies and functionalities beyond human ability, it does not eliminate the need for maintaining human oversight. When possible, individuals should have the option for human intervention rather than depending solely on AI's automated processes. While AI has proven powerful and often effective, it's not at the point where it should have sole discretion over decisions that significantly impact lives, such as in healthcare, employment, or legal judgements. Fallback or escalation processes to human for consideration should be in place for system failures, errors, and for appeals of decisions made. These mechanisms are necessary for accessible, equitable, effective treatment. By preventing an over-reliance on AI and providing human touchpoints, risks can be more effectively mitigated, promoting accountability, trust, and transparency through these processes.

Regulatory Lag

While the framework above provides a solid foundation, it is simply a blueprint for the AI Bill of Rights – true regulations can take years longer. Regulatory lag is not a new concept and with the pace of AI advancements, the gap between AI, its concerns, and regulation will only grow. The EU has already published the EU Artificial Intelligence Act which, much like GDPR, is likely to set the groundwork for other regulations worldwide. With the power and trajectory of AI, perhaps it's time for an international governance body made up of diverse stakeholders (including governments, private businesses, academics) to oversee development and deployment of AI with proactive regulation and global standards. However, an attempt to push regulation may be viewed as stifling innovation, so there would be much debate to be had.

For now, the principles in the Blueprint for an AI Bill of Rights provide a valuable framework for AI designers and developers to safeguard the personal rights of users, while promoting fairness, safety, and effectiveness of the tools. While many are focused on bringing the public the latest innovative technologies, there must be a balance with accountability and liability to comply with the basic principles of privacy, security, and fairness.

What should a CISO do?

Virtually every conference, webinar, and local cybersecurity chapter meeting that I've personally attended this year has echoed the same themes. CISOs are struggling with enabling the business and end users to benefit from AI tools, while mitigating potential risks. Shadow IT is nothing new. However, preventing end users from accessing AI is particularly challenging due to the ubiquitous nature of the technology. It seems like every vendor is rushing to put AI into every software, platform, and hardware device. Other CISOs are examining the problem from a data classification point-of-view: where if they can only identify their most critical data and ensure it never gets processed into an AI model, then they can reduce most harm. I'm skeptical that this will be achievable.

So, what then should a CISO do? I return to the fundamentals. The back-to-basics approach is to begin with end user security awareness and training, specifically tailored to AI. Many end users do not truly know what AI is, how it actually works, yet they are still using it daily. Educating and empowering your front-line workers to exercise caution around AI will likely yield the best results. Creating a culture where security is enabling innovation, rather than outright blocking tools via policy mandate, is essential. I've seen great success with my partners who institute weekly lunch-and-learn sessions specifically for AI use cases. One CISO commented to me that their attendance as dramatically increased once AI became a regular topic. There is a real demand for learning about these tools, because as I mentioned earlier, no one wants to be left behind.

Below, I will revisit the core aspects of the AI dilemma previously discussed with recommendations and best practices to alleviate the potential harm.

Privacy and Security – Revisited

Incorporating privacy and security principles right from the design phase is imperative to minimize potential compromise of data and systems with the goal of increasing trust, transparency, and safety. Consider these practices:

1. Security controls: implement strong security principles (such as encryption, incident response, access control, network and endpoint security) to prevent unauthorized access, misuse of data, and tampering of data and systems.
2. Audits and transparency: regular audits of AI systems for bias, safety and effectiveness, and clear privacy controls must be publicly shared for true accountability and transparency.
3. Data minimization: only collect data that is necessary for functionality.
4. Purpose limitation: use data only for the specified purposes.
5. Data anonymization: remove identifiable information from data, however note that some Ais are able to re-anonymize de-identified data.
6. Informed consent: clearly explain how data is used, if it's being shared with third-parties, and provide updates when changes in data use and collection occur.
7. Individual rights: allow users the ability to select and modify their preferences, opt-out of certain processes, and delete their data.

8. Develop policies: as developers of AI, establish and enforce principles for effective security and privacy; as users of AI, establish and enforce requirements around usage of AI. Be sure to educate users on the why.

Bias and Discrimination – Revisited

Regarding bias and discrimination, the following is a non-exhaustive list of considerations to mitigate the risk of exacerbating unfair stereotypes and prejudices.

1. Diverse and representative datasets: AI training data should be diverse and representative of the population to mitigate bias and discrimination.
2. Inclusive design: design elements must be considered to ensure accessible and equal usability, regardless of background, identity, or physical ability.
3. Community engagement and feedback: diverse communities should be consulted for input of the design and implementation to ensure unique needs and perspectives are accounted for.
4. Socioeconomical impacts: consider the socioeconomic implications of AI-based automation for various tasks. While this may be an ethical question, take stock of how these systems can potentially lead to job displacement in low-income communities, widening the economic gap between groups.
5. Human intervention: ensure protocols are in place for fallback or escalations to people, particularly when AI is used for significant life-changing decisions.

Just like in aspects of cybersecurity where the advancement of technology leads to both more sophisticated tools and controls for defense, but also more savvy advisories and tactics on offense, AI poses a similar paradigm. As the algorithms get more advanced, the risks and potential for harm grows with it. It is crucial to keep the privacy, security, and biases top of mind when leveraging this technology and always calling for the highest standards of transparency, accountability, and protection.

About the Author

Céline Gravelines has 10 years of experience in the cybersecurity industry, specializing in data protection, security policies, incident response, risk & management, vulnerability management, privacy, and more. Named one of the Cyber Defense Global InfoSec Top Women in Security, she currently serves as the Director of Cybersecurity Professional Services at Keyavi where she works with self-protecting data technology to eliminate data loss. Céline holds a BSc in Computer Science and Physics, and a MSc in Computer Science, focusing on applying unsupervised machine learning to brain space.

Céline can be reached by email at celine.gravelines@keyavi.com and at our company website https://www.keyavi.com/

Transparency in Cybersecurity: The Importance of Accurate Vulnerability Disclosures

By Mike Walters, President and Co-Founder of Action1 Corporation

Recently, the cybersecurity world has been rattled by a series of critical vulnerabilities discovered in Ivanti Connect Secure VPN software. In the wake of these ongoing vulnerability issues, Ivanti has also faced criticism from members of the infosec community for its handling of vulnerability disclosures. Ivanti grouped multiple vulnerabilities under a single registered Common Vulnerabilities and Exposures (CVE) ID, rather than disclosing them as individual vulnerabilities. Juniper faced similar criticism for disclosing only two vulnerabilities instead of four.

These scenarios highlight the importance of accurate vulnerability disclosure. This article will examine how inconsistencies impact vulnerability remediation effectiveness and offer improvement suggestions.

Inaccuracies in Vulnerability Disclosures and Subsequent Risks

Vendors may choose to downplay the number of registered vulnerabilities for various reasons, such as simplifying their reporting process, minimizing public exposure of vulnerabilities, or reducing the perception of having a large number of individual vulnerabilities in their software.

However, grouping multiple vulnerabilities under a single registered CVE is a bad strategy as it makes it unclear for organizations which exact vulnerability needs to be addressed in the development cycle to resolve the CVE issue. This can result in communication problems within IT teams, leading to potential oversight of unpatched vulnerabilities. Ultimately, it complicates mitigation efforts for organizations, increases the risk of unnoticed vulnerabilities, and results in accusations against the vendor.

While Ivanti and Juniper faced public criticism, it's worth noting that the damage from mishandling vulnerability disclosure was not critical because they did disclose vulnerabilities. However, there is an older case involving Microsoft, where a certain vulnerability was concealed, allowing threat actors to exploit it for years.

In May 2017, Microsoft silently patched the vulnerability known as "EpMo" without publicly disclosing it in 2013 when it was initially discovered. This lack of disclosure allowed APT31 (attributed to China's Zirconium) to replicate the exploit in 2014 to form the "Jian" exploit and use it since at least 2015. The exploit was reported to Microsoft by Lockheed Martin's Computer Incident Response Team, indicating a potential attack against American targets. The delayed disclosure enabled APT31 to exploit the vulnerability for years. This example underscores the importance of timely and transparent disclosure of vulnerabilities by vendors, as it enables users and organizations to take necessary measures to protect themselves against potential threats.

Other Issues with Vulnerability Handling

Sometimes vendors, after detecting vulnerabilities in their software, issue the upgrade while retaining the previous version's public number. Consequently, it becomes unclear for a sysadmin whether the application in place is vulnerable or patched. Such cases often go unnoticed by the public, but they do happen. In June 2023, Dell Commander 4.9.0 was found to have CVE 2023-28071, with a NVD score of 7.1. The company released a new version internally marked as A02, but did not change the publicly available version number, which is visible in the Programs and Features view. A good practice would be to assign a new number to the updated version.

Best Practices to Disclose Vulnerabilities

When software vendors disclose vulnerabilities and assign CVEs, they should adhere to certain rules. First, they need to coordinate with CVE Numbering Authorities (CNAs), which are responsible for assigning CVE IDs and maintaining the CVE database. This ensures that the vulnerability meets the criteria for CVE assignment.

Entities discovering vulnerabilities should disclose them to relevant parties, including vendors, CERTs, and vulnerability databases, allowing vendors time to develop patches before public disclosure.

Following the designated process for requesting CVE IDs is crucial, as it requires providing accurate and detailed information about the vulnerability. When disclosing the vulnerability, vendors should provide a clear description, including its impact, affected versions, potential attack vectors, and any known mitigations. Assigning a Common Vulnerability Scoring System (CVSS) score helps quantify the severity of the vulnerability.

Errors in assigning CVE IDs are inevitable, with a resolution process involving rejection, merging, or splitting of entries. Organizations must adhere strictly to update rules, rejecting CVEs if research disproves a vulnerability, fixing typos causing misuse, or merging multiple IDs for one vulnerability. Selected CVE IDs incorporate information from others, while unselected ones are updated with rejected descriptions. Split CVE when assigning a single CVE ID when more than one is required, splitting the entry into multiple CVE entries. This is done to ensure accurate and granular identification of different vulnerabilities.

Vendors should also provide clear information about any subsequent updates if that's applicable, such as new patches, versions or mitigations, or changes to the CVSS score.

It's essential to conduct responsible disclosure, minimizing the risk of exploitation and prioritizing the security of affected users. Finally, vendors must ensure compliance with laws governing vulnerability disclosure practice.

Conclusion

In my opinion, vendors should not hesitate to disclose vulnerabilities with all pertinent information. They owe it to their customers to be transparent. This approach will result in more secure applications and clearer patch management processes.

About the Author

Mike Walters, President and co-founder of Action1 Corporation - managing product strategy for the company. Previously Co-CEO & Co-Founder of Netwrix Corporation, Michael was responsible for go-to-market strategy, sales and evangelism. At Netwrix Mike and Alex built a very successful cybersecurity business, and then they both left Netwrix after transition to a new CEO. Well known for its visibility and user behavior analytics platform, Netwrix became a leader with more than 10,000 customers worldwide. Mike lives in Laguna Beach, CA, and he has three kids. He is an avid surfer and philanthropist who cares about environmental protection.

Mike can be reached online at our company website https://www.action1.com/team/

The Undeniable but Often Overlooked Human Element Of Cybersecurity

By Sam Rehman, SVP, Chief Information Security Officer at EPAM Systems, Inc.

It is firmly established that there is no such thing as 100% security – in fact, a security breach is not a matter of 'if' but 'when.' In other words, risk will always exist, and businesses need to shift their thinking from completely neutralizing it (which is impossible) to managing it accordingly.

Despite this reality, many business leaders unfortunately expect and demand 100% security from their teams. Because such a posture is impossible, companies will settle for a false sense of security to allow their people to function. This mindset is not only incorrect but irresponsible.

Business leaders must abandon this outdated notion of 100% security and adopt a mindset of risk management. This strategy asks questions about the size of the blast radius and how long it takes teams to detect and remediate. Such an approach also recognizes that humans play a fundamental role in cybersecurity – namely, managing risk – and adjusts strategies and processes appropriately.

Train General Employees Similarly to Cyber Teams

Despite the need for cybersecurity talent, the global shortage of nearly four million cyber professionals makes hiring difficult. This shortage places pressure on understaffed teams, forcing them to do more with less and consequently increasing burnout. Short of getting lucky and landing a skilled worker, businesses cannot magically solve the talent shortage through hiring alone. However, companies can bolster the security competency of their general employees to take a load off the shoulders of overworked cybersecurity teams.

General employees don't receive sufficient training. The typical security awareness training is little more than watching videos and completing simple comprehension quizzes. It should come as no surprise that human error accounts for 95% of cybersecurity issues. Alternatively, businesses should provide the same training methods cybersecurity teams use to everyone else – namely, interactive simulations and life-like rehearsals.

Spontaneous security simulations, such as mock phishing emails, will allow companies to understand their workforce's security fitness and offer tailored training to those departments that performed poorly. Plus, by using role-relevant training mockups, organizations can arm their people with the proper protocol for real incidents, reducing anxiety and instilling confidence.

Avoid Complexity, Design with People in Mind

Training is invaluable to strengthening a company's security posture. But if security processes are too complex or cumbersome and not simple to use, no amount of training will encourage people to spend precious minutes trying to resolve an issue. For example, while employees may know not to click on a suspicious link, they don't want to spend time confirming that the link is unsafe. Most likely, they might not know how to verify that a link is dangerous beyond their gut instinct.

Organizations must design security processes to incorporate principles of secure-by-design and human-centered design. The former approach places security as a core business goal rather than as some technical feature. The latter approach places people at the heart of the solution – more specifically, the designers are empathic toward the people they are trying to help. When dealing with shady links, for example, the security team and designers must create a user-friendly link verification solution that is not complicated but quick and easy to use, ensuring employees will perceive its value and be encouraged to use it to benefit the entire organization.

Interestingly, this trend toward human-focused security solutions continues to gain traction. Gartner predicts that by 2027, 30% of cybersecurity functions will redesign application security to be consumed directly by on-cyber experts and owned by application owners.

Implement a Zero-Trust Model

When businesses think about cybersecurity, they might imagine a castle with high walls and a deep moat. They build their fortress to repel outsider attackers, often forgetting the threats lurking inside the walls.

These risks, known as insider threats, account for 60% of data breaches and can be malicious or accidental.

Zero trust is about managing the blast radius – meaning, if and when something bad happens, what is the size and amount of the damage; likewise, how long does it take teams to detect the breach and perform remediation? This model maintains strict access controls, verifies everything and monitors continuously. Zero-trust architecture also divides the network through microsegments to isolate and block attacks, restricting the lateral movement of bad actors should they gain access.

A zero-trust model transforms a simple castle into a labyrinth of passageways, gates, and checkpoints, minimizing the damage from intentional and unintentional threats. While this approach may seem overly distrustful of employees, it is more than appropriate in today's unpredictable threat environment.

Every Individual Has a Role to Play in Security

Cybersecurity is constantly evolving with the introduction of new technologies. Generative AI, for instance, benefits businesses and bad actors alike, forever changing the landscape. Although technology continuously evolves, causing techniques and best practices to become irrelevant overnight, humans will always be a core element of any risk management strategy. As such, businesses must remember the influence each member of the organization has on the organization's security wellness or lack thereof.

About the Author

Sam Rehman is Chief Information Security Officer (CISO) and Head of Cybersecurity at EPAM Systems, where he is responsible for many aspects of information security. Mr. Rehman has more than 30 years of experience in software product engineering and security. Prior to becoming EPAM's CISO, Mr. Rehman held a number of leadership roles in the industry, including Cognizant's Head of Digital Engineering Business, CTO of Arxan, and several engineering executive roles at Oracle's Server Technology Group. His first tenure at EPAM was as Chief Technology Officer and Co-Head of Global Delivery.

Mr. Rehman is a serial entrepreneur, technology expert and evangelist with patented inventions in software security, cloud computing, storage systems and distributed computing. He has served as a strategic advisor to multiple security and cloud companies and is a regular contributor in a number of security industry publications.

LinkedIn

Website: https://www.epam.com/

Maximizing Cybersecurity Impact Within Budget Constraints

Bridging Cybersecurity Gaps with Layered Integrations

By Joe Tibbetts, Senior Director, Technology Alliances & API, Mimecast

Cybersecurity is the cornerstone of organizational stability and resilience today. Despite its critical importance, budgetary allocations often fall short due to competing priorities.

Mimecast recently surveyed 1,100 CISOs and information technology professionals for their 2024 State of Email and Collaboration Security report. Report findings highlight the stark reality facing IT teams: while cybersecurity remains a top concern, investment in cybersecurity fails to meet the mark. On average, organizations dedicate a mere 9% of their IT budget to cybersecurity, a figure significantly lower than the perceived ideal of 12%. This gap has major consequences, with 37% of IT professionals acknowledging their inability to detect and respond to threats with the speed and efficiency demanded by today's threat landscape.

Underfunded cybersecurity initiatives yield significant consequences for IT teams and businesses. Mimecast found that 40% of respondents compromise on cybersecurity tools, while 36% acknowledge significant gaps in their organization's defenses due to underspending. Considering these findings, the urgency for effective cyber defense strategies becomes undeniable. IT teams must learn to maximize the impact of limited resources while strengthening defenses against an ever-evolving range of cyber threats.

Layering Cyber Solutions Can Help Enhance Protections While Keeping Costs Down

To address these challenges, IT teams must adopt a strategic approach to cybersecurity investments. A layered defense strategy, integrating multiple interoperable services, offers a manageable solution to enhance security posture while remaining budget conscious. By implementing a layered defense strategy, organizations can effectively address the shortcomings highlighted by budgeting gaps while maximizing the efficiency of their investment.

As cyber leaders begin to create a layered defense strategy for their organizations, they must prioritize these key considerations:

- **Enabling Depth and Breadth of Protection:** Layered cybersecurity offers both defense in depth and comprehensive protection. By deploying multiple security layers, organizations create overlapping defenses against various threats, ensuring a robust security posture. This approach minimizes the likelihood of successful cyber-attacks by covering multiple attack vectors and provides a stronger overall defense strategy.
- **Improved Detection, Response, and Resilience:** Layered integrations enhance threat detection capabilities, facilitate rapid incident response, and bolster resilience against sophisticated attacks by diversifying defense measures. Furthermore, embedding different layers of solutions can provide insight into potential threats at various stages of an attack lifecycle. When this insight is shared across vendors in the cyber stack, organizations can improve their detection capabilities and mitigate threats before they fully infiltrate a system.
- **Scalability and Adaptability:** As new threats emerge, cyber leaders must adapt and implement new layers or make adjustments to existing layers. Flexible solutions help IT teams keep up with evolving organizational needs and shifting threat vectors, to ensure that defenses are always effective against whatever threats come their way.
- **Strategic Prioritization:** In a layered cybersecurity defense strategy, it's critical to use resources strategically by aligning defense strategy with organizational goals, and deploying the right resources to ensure the company’s most vulnerable areas are prioritized. This involves identifying which specific areas could pose the biggest threat and focusing on protecting those areas. For example, organizations can provide targeted training for employees based on individual risk profiles. This proactive approach helps lower the likelihood of cyberattacks and limits damage to the organization's assets and reputation.

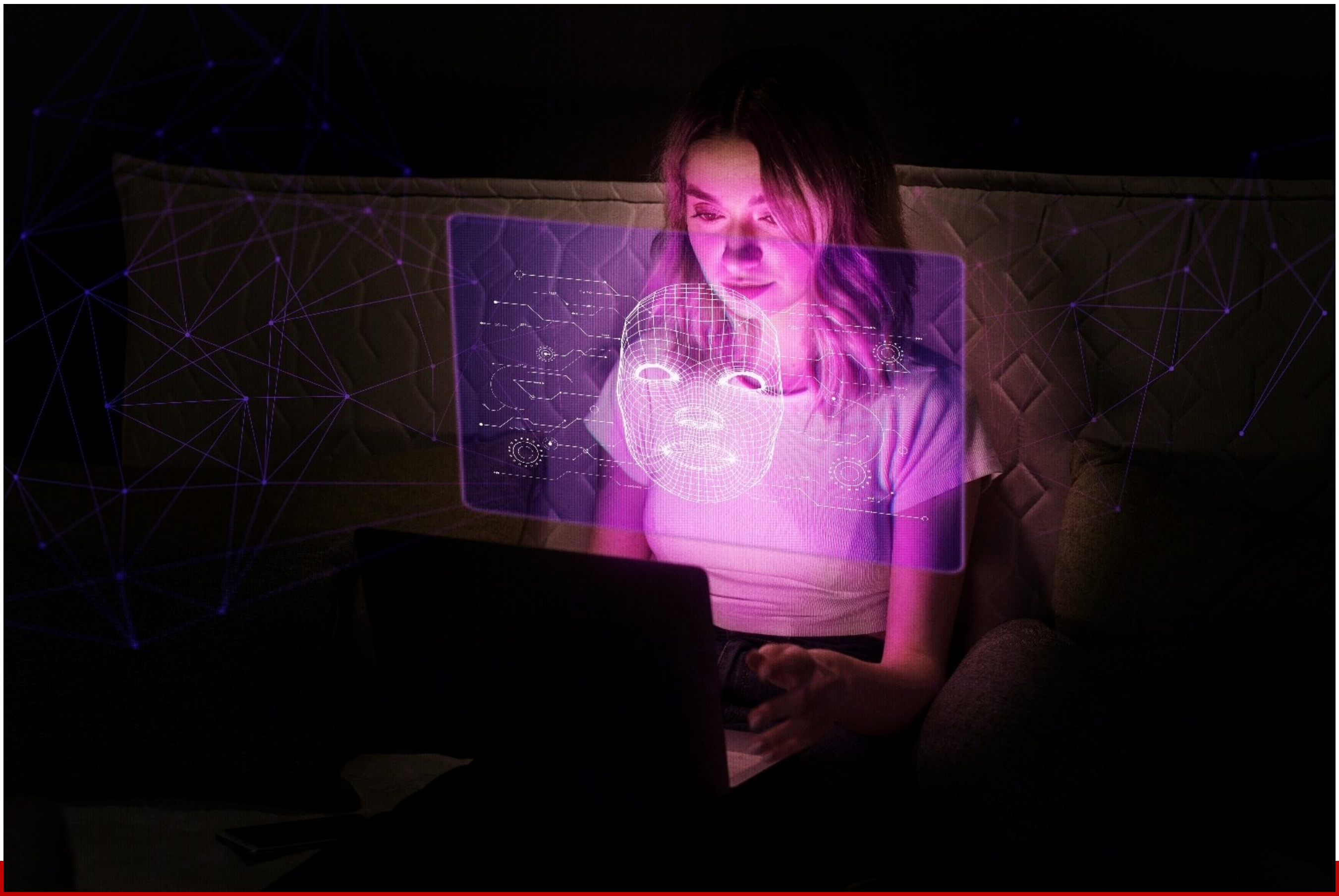
Building a Resilient Future with Integrated Solutions

In a threat landscape where digital attacks are constantly changing, the strategic planning and integration of cybersecurity solutions is paramount. When selecting cyber solutions, cyber leaders must prioritize scalability, interoperability, and futureproofing.

By investing in flexible and adaptive technologies, organizations can maintain a competitive edge, anticipate emerging threats, and ultimately save money in the long run. While investing in cybersecurity requires upfront costs, the long-term financial benefits of preventing data breaches, protecting intellectual property, minimizing downtime, preserving reputation, and reducing incident response costs far outweigh the initial investment. Through strategic investment and layered defense strategies, businesses can navigate the complexities of cybersecurity while optimizing resource utilization and maximizing impact.

About the Author

Joe Tibbetts is the Senior Director of Tech Alliances & API at Mimecast. Building upon Mimecast's successful API program launch in 2018, Joseph Tibbetts is focused on integrating world class third-party platforms to improve customer and partner efficacy by connecting the dots in the enterprise security ecosystem. Since inception, Mimecast is integrated into over 100 security products and offers 65 formal Technology Alliance Partners with the most robust email security API in the market.First Name can be reached on LinkedIn and at our company website.



Shedding Light on The Dark Web: Enhancing Cybersecurity Through Proactive Monitoring

By Josh Smith, Principal Threat Analyst, Nuspire

In the digital age, the dark web has emerged as a clandestine marketplace for illicit activities, including the sale of stolen data, illegal software and various forms of malware. The proliferation of these marketplaces poses significant threats to personal, corporate and national security. As a Principal Threat Analyst, I have observed firsthand the evolution of cyber threats and the increasing sophistication of cybercriminals who exploit the anonymity of the dark web. This article not only highlights the concerning trends I've seen in dark web activities and the surge in infostealer malware, but also empowers you with the knowledge of how dark web monitoring can be a crucial tool in combating this growing threat.

The expanding threat landscape on the dark web

The dark web is a part of the internet that is not indexed by traditional search engines and can only be accessed through special software like the Tor browser, which anonymizes user activity. It is part of the larger deep web, which includes all parts of the internet that are not indexed by search engines. However, unlike the deeper parts of the web, which can consist of anything from academic databases to confidential corporate web pages, the dark web is known for its anonymity and is often associated with illegal activities.

The anonymity provided by the dark web supports a variety of illicit activities, including the sale of illegal drugs, weapons, and stolen data. Transactions on the dark web often use cryptocurrencies, which further anonymize the buyer and seller, making it difficult for authorities to trace the parties involved. This has led to the dark web becoming a favored venue for cybercriminals looking to buy, sell, or trade illegal goods and services.

Recent data from Nuspire's Q1 2024 Cyber Threat Report reveals a substantial 58.16% increase in dark web marketplace listings, with a total of 3,938,507 listings identified in the first quarter of 2024 alone. Among these, there are 437,657 listings for credit cards, 122,839 for email account access and 92,718 for social security numbers. Additionally, listings for shell and Remote Desktop Protocol (RDP) access are notably high, with 40,144 and 37,169 listings, respectively. This significant uptick in dark web listings highlights not only the vast amount of stolen data available, but also the ease with which cybercriminals can access and exploit personal and corporate information.

The rise of infostealer malware

Infostealers, as the name suggests, are a type of malware specifically designed to steal sensitive information from an infected computer. This category of malware is particularly insidious because it targets personal and financial information that can be used for identity theft, financial fraud and other cybercrimes. The information targeted by infostealers can include, but is not limited to, credentials used in online banking services, social media sites, emails or FTP accounts.

A key player in the realm of infostealers is the Lumma Stealer malware, which has seen more than a doubling in activity since Q4 2023, according to Nuspire’s data. Lumma Stealer first emerged in 2023 and has quickly become a leading tool for cybercriminals, thanks to its developers' aggressive marketing on dark web forums and private access chats. This malware is typically spread through phishing emails, cracked software and social engineering tactics on platforms like Discord and Telegram. Once installed, Lumma Stealer employs anti-sandbox techniques to evade detection and begins exfiltrating sensitive data, including cryptocurrency wallet information, browser profiles and persistent cookies.

The imperative for dark web monitoring

The escalating activities on the dark web and the proliferation of infostealers underscore the critical need for robust dark web monitoring. Dark web monitoring employs specialized tools and techniques to scan hidden parts of the internet. These tools act like search engines tailored for the dark web, sifting through forums, marketplaces and private sites where data is often traded. When a company’s data is found — be it employees' personal information, leaked internal documents or compromised customer data — the monitoring service alerts the organization. This enables them to act quickly to mitigate potential damages.

By keeping a vigilant eye on dark web marketplaces, ransomware extortion sites and private access forums, cybersecurity professionals can gain valuable insights into the latest cyber threats and cybercriminals' methods. This intelligence is crucial for proactive threat hunting and the development of effective defense strategies.

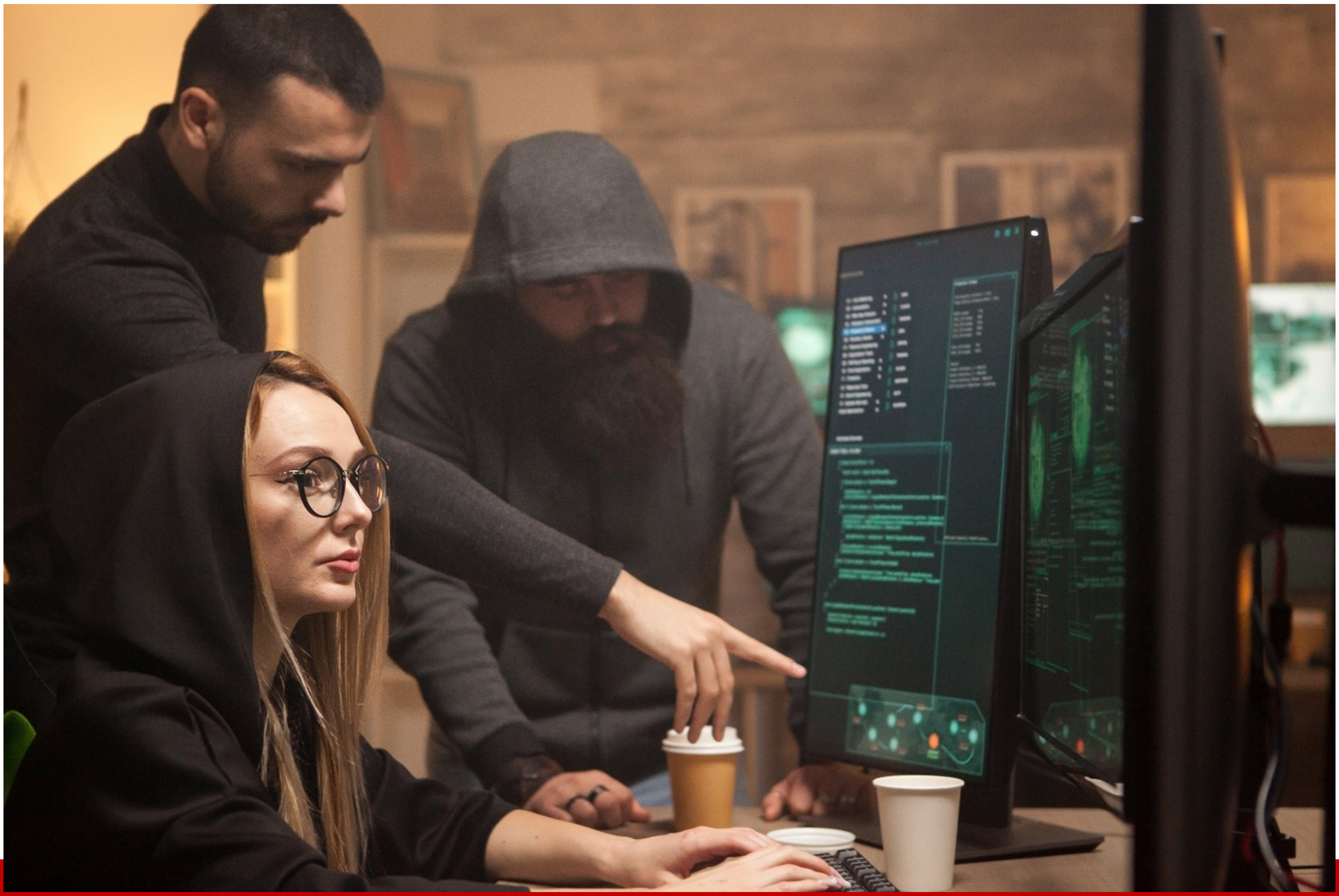
For instance, if an organization’s stolen credentials are detected on the dark web, it can quickly reset passwords and tighten access controls before these credentials can be used in a breach. Additionally, by analyzing the tactics and tools sold and discussed on the dark web, organizations can better prepare their defenses against potential attacks. This might include implementing stronger security protocols like multi-factor authentication (MFA) and conducting targeted cybersecurity awareness training that addresses specific threats like phishing schemes.

The importance of a proactive defense

The dark web represents a formidable challenge in cybersecurity, with its anonymous nature serving as a breeding ground for cybercriminal activities. The alarming increase in marketplace listings and the rise of infostealer malware like Lumma Stealer highlight the evolving threats that organizations and individuals face. In this context, dark web monitoring emerges as an indispensable tool in the cybersecurity arsenal, providing the intelligence needed to anticipate and mitigate cyber threats effectively. As we navigate the complexities of the digital landscape, we must remain vigilant and proactive in our efforts to safeguard our digital assets and protect against the ever-present threats emanating from the dark web.

About the Author

Josh Smith is Nuspire’s Principal Threat Analyst, working closely in organizational threat landscapes, curating threat intelligence, and authoring Nuspire’s Quarterly Threat Landscape Report. Josh is currently pursuing his master’s degree in Cybersecurity Technology. Previously, he served with the U.S. Navy as an Operations Specialist with 14 years of service. Josh has been quoted in Forbes, CSO Online, Channel Futures, Dark Reading and others. Josh can be reached online via LinkedIn at our company website https://www.nuspire.com/



Defense in Diversity: A Strategy for Robust Cybersecurity

By Craig Burland, CISO, Inversion6

The concept of “defense in depth” dates back to ancient times, epitomized by the ramparts, draw-bridge, towers, and battlements surrounding a medieval castle. Cybersecurity’s adaptation of the idea -- multiple layers of security controls to protect data and systems forces intruders to “get it right” over and over before reaching their goal -- has long been a cornerstone of strategic planning and is considered a best practice.

However, as major cybersecurity vendors like Microsoft, Palo Alto, Okta, and CrowdStrike fill gaps in their portfolio to provide “complete and comprehensive” security coverage, it’s time to consider a complementary strategy: "defense in diversity". Defense in Diversity emphasizes the importance of using different vendors at different layers of defense to mitigate the risk of a compromise due to insular thinking or a singular, fatal flaw. Diversity in the context of this article means being composed of differing vendor sources, operating characteristics, defensive philosophies, and fundamental principles, rather than a political concept.

The Risks of Vendor Homogeneity

The recent successful attack on Microsoft has starkly illuminated the risks associated with relying on a single vendor for all layers of security. When Microsoft's Azure cloud services were compromised, the breach extended beyond the immediate impact, affecting multiple security layers that depended on Azure. This incident underscores a critical flaw in security strategies that depend heavily on one provider: the interconnected nature of services offered by a single vendor means that vulnerabilities in one area can expose weaknesses across the entire system, leading to potentially catastrophic breaches.

Imagine, for a moment, the expression on the king's face when his prized keep, surrounded by nothing but an elaborate series of moats, is besieged by invaders equipped with boats, pontoons, and portable bridges.

Diversifying security vendors when deploying a multi-layered defense strategy can mitigate this risk by ensuring that a breach in one layer does not automatically compromise others. This approach not only enhances resilience but also reduces the likelihood of widespread disruption in the event of a targeted attack on a primary security vendor.

The Positive Impact of Diversity: An Analogy

The importance of defense in diversity can be likened to the positive impact of diversity in decision-making and organizational makeup. Diverse teams are proven to be more innovative and better at problem-solving. They bring together different experiences, viewpoints, and ideas, which can lead to more creative solutions and better decision outcomes. Organizations that embrace diversity in their workforce tend to be more adaptable and resilient. Diverse organizations are better equipped to handle challenges because they can draw on a wider range of experiences and perspectives.

Just as diverse teams bring varied perspectives and strengths to the table, creating a more innovative and resilient organization, a diverse set of security vendors creates a more robust defense against cyber threats. Each vendor brings unique strengths and capabilities that can cover the gaps and weaknesses of others, resulting in a more comprehensive security posture.

Embracing Defense in Diversity

The counterpoint to defense in diversity is largely an economic one. With enterprise suites including a full complement of security platforms, it's important to weigh the financial benefits of a single vendor bundle versus the benefits of a diverse approach. Selling senior leaders who are more comfortable talking about the bottom line than reviewing the risk register will likely need additional convincing as to why the additional investment makes sense. Following are the benefits of a diverse approach to assembling your cybersecurity stack.

Reduced Risk of Systemic Failures

Using different vendors for different security layers ensures that a vulnerability in one system does not necessarily compromise others. For instance, if your identity management is handled by Okta and your cloud security by another provider, a breach in Okta would not directly affect your cloud security, and vice versa. This segmentation reduces the risk of a single point of failure causing widespread damage.

Leveraging Best-of-Breed Solutions

Different vendors excel in different areas. By diversifying your security providers, you can take advantage of best-of-breed solutions for each specific layer of defense. For example, you might use a specialized vendor for endpoint security, another for network security, and yet another for identity and access management. This approach allows you to tailor your security architecture to your specific needs and threat landscape.

Enhanced Detection and Response Capabilities

Different vendors often have unique detection and response capabilities. By leveraging multiple vendors, you can benefit from a wider range of threat intelligence and incident response mechanisms. This diversity can help in identifying and mitigating threats more effectively, as different tools may detect different aspects of an attack.

Avoiding Vendor Lock In

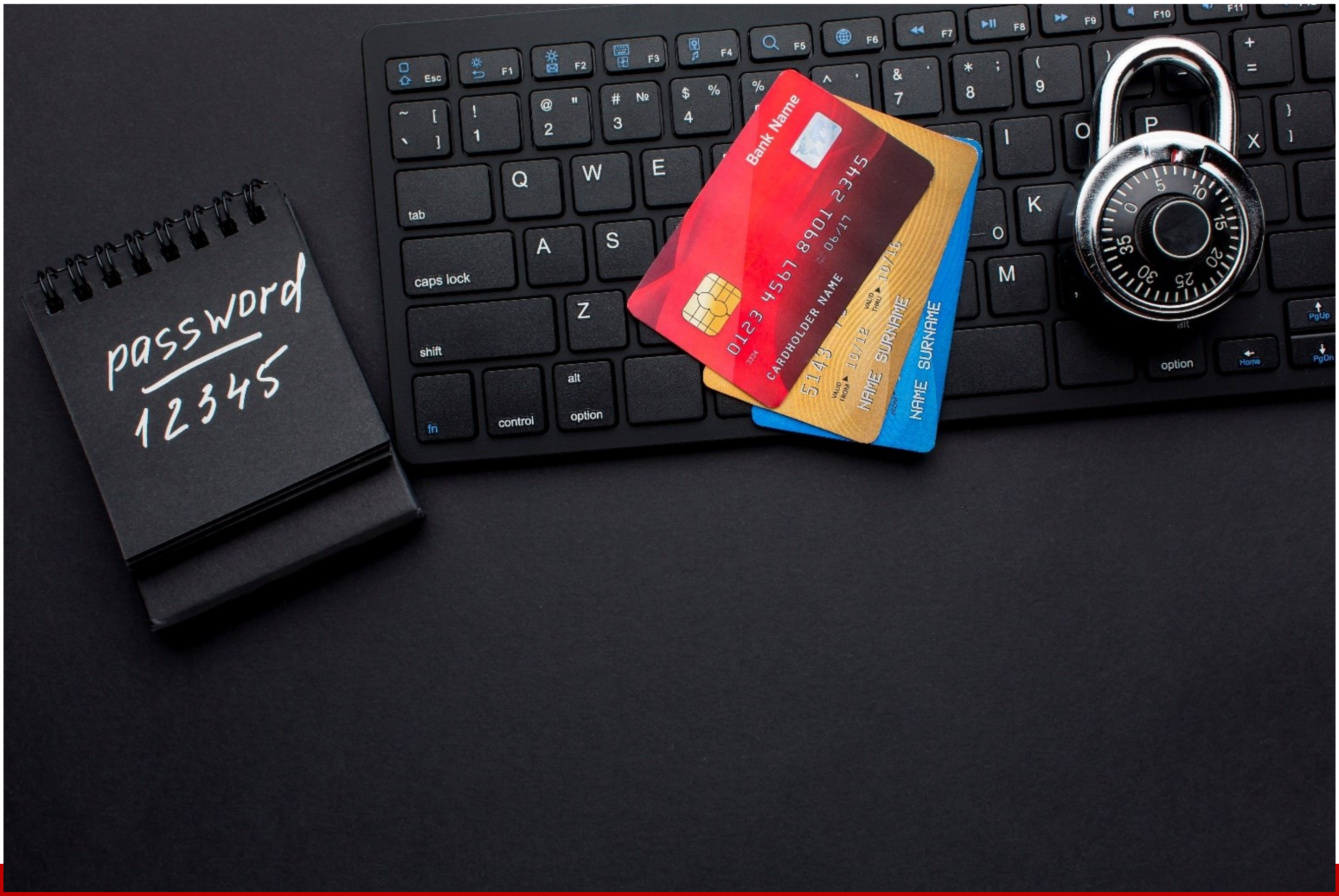
The obvious danger of vendor lock in rests with the loss of leverage an organization's experiences when tightly coupled to a single provider. The less obvious impact is the organizational brain drain as resources get trained on a single suite, participate in road mapping from a single source, are hired or promoted for their specific platform experience, etc. Over time, the vendor's technology strategy becomes the organization's technology strategy and other perspectives are no longer considered.

Conclusion

In today's threat landscape, a diverse and multi-layered defense strategy is not just a good practice—it's essential. The recent attacks on Microsoft and Okta have shown that relying on a single vendor for multiple layers of security can leave organizations vulnerable to systemic failures. By embracing a defense in diversity approach, you can build a more resilient and robust security posture that is better equipped to withstand the complexities of modern cyber threats. Just as diversity in decision-making and organizational makeup leads to stronger and more innovative outcomes, a diverse set of security vendors creates a more resilient and effective defense. Remember, in cybersecurity, diversity is strength.

About the Author

Craig Burland is CISO of Inversion6. Craig brings decades of pertinent industry experience to Inversion6, including his most recent role leading information security operations for a Fortune 200 Company. He is also a former Technical Co-Chair of the Northeast Ohio Cyber Consortium and a former Customer Advisory Board Member for Solutionary MSSP, NTT Global Security, and Oracle Web Center. Craig can be reached online at LinkedIn and at our company website https://www.inversion6.com/.



Choosing Security: Why Companies Should Reject Ransom Payments

By Bogdan Glushko, Chief Information Officer, Proven Data

With ransomware attacks reaching unprecedented levels, businesses face tough decisions when their data is held hostage. While the temptation to pay the ransom to recover data quickly is strong, this approach poses significant risks and ethical dilemmas.

One of these dilemmas is that victims may fuel cybercriminal activities by paying ransoms, empowering criminal networks, and perpetuating attacks globally. Also, legal risks loom large, as payments may violate regulations and support criminal enterprises, potentially leading to sanctions.

Experts encourage robust preventive measures, such as comprehensive backup systems, enhanced cybersecurity solutions, and professional incident response plans, to mitigate ransomware risks effectively.

Dangers of paying ransoms

Paying ransoms can have severe consequences that jeopardize businesses financially, reputationally, and legally. The following are the main negative consequences of paying the ransom demand and why any payment or communication with the threat actors should be avoided.

1. Encourages cyber criminals in their activities

When victims pay the ransom demand, they financially support cyber criminals, inadvertently enabling them to launch more attacks and perpetuating a cycle of cyber extortion globally. The financial support provided by ransom payments can also fuel other forms of illegal activity, including terrorism and organized crime, exacerbating global security challenges.

2. No guarantee of data recovery

Often, cybercriminals disappear after receiving the ransom payment and do not deliver the decryption key as promised. In this case, the organization will suffer additional financial losses, as they must hire a data recovery company to retrieve or decrypt the files.

3. Incomplete data decryption and corruption

Even if a decryptor is provided, the process may result in incomplete data recovery or corruption, complicating an attack's aftermath.

Legal and ethical considerations

Under the International Emergency Economic Powers Act (IEEPA), ransom payments may be considered a sanctionable offense. This legislation and other regulatory frameworks aim to prevent the flow of funds to criminal enterprises, including those involved in cyber extortion. **Compliance with these laws is crucial, as violating them can lead to severe penalties, including hefty fines and legal action against the offending organization**. Programs like the Office of Foreign Assets Control (OFAC) are essential to mitigate legal risks associated with ransom payments and help ransomware victims recover data while adhering to regulatory requirements.

The ethical implications of paying a ransom are profound since, as mentioned, when organizations succumb to ransom demands, they directly fund criminal enterprises and perpetuate the ransomware economy. This funding enables cybercriminals to enhance their capabilities, launch more sophisticated attacks, and expand their operations, leading to a broader impact on other organizations and individuals. This cycle of crime not only emboldens existing attackers but also attracts new perpetrators into the lucrative field of cyber extortion.

Beyond immediate financial and operational impacts, **ransom payments can have long-term consequences for an organization**. When companies comply with ransom demands, they contribute to normalizing extortion as an acceptable business practice. This normalization can erode trust and credibility among stakeholders, including customers, partners, and investors, who may view the decision as failing to uphold ethical standards and a sign of vulnerability. Over time, this can damage the organization's reputation and undermine its competitive position in the market.

Proactive cybersecurity measures

Implementing strategies such as regular security audits, employee training, and robust backup, among other strategies, are crucial steps in defending against these relentless threats. By taking these measures, businesses can protect their assets and maintain their stakeholders' trust and confidence in an ever-evolving cyber landscape.

Regular security audits and assessments

Regular security audits involve systematically reviewing and evaluating an organization's IT infrastructure to identify vulnerabilities and weaknesses that could be exploited by cybercriminals.

Organizations can detect potential threats early by conducting regular security assessments, implementing necessary patches, and updating security protocols to mitigate risks.

Employee training and awareness

Since human error is often a significant factor in successful cyberattacks, educating employees about security best practices can significantly reduce this risk.

Comprehensive training programs should cover topics such as recognizing phishing attempts, safe internet usage, password management, and the importance of reporting suspicious activities.

Creating a culture of cybersecurity awareness encourages vigilance and proactive behavior, making employees the first line of defense against potential breaches.

Backup strategy

Organizations should implement a comprehensive backup strategy that includes regular, automated backups of all critical data and systems. These backups should be stored in secure, off-site locations to protect them from being compromised during attacks. To enhance data security, adopt the 3-2-1 backup strategy—three copies in two devices with one stored offsite.

Effective backup and recovery plans ensure business continuity by enabling organizations to resume operations with minimal downtime and data loss.

Incident response plan

An incident response plan outlines the steps an organization should take in the event of a security breach, from initial detection and containment to eradication, recovery, and post-incident analysis.

A well-defined incident response plan includes roles and responsibilities, communication protocols, and procedures for documenting and analyzing incidents.

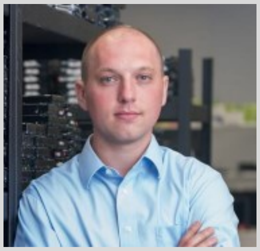
Regularly updating and testing the plan through simulations and drills ensures the response team is prepared to act swiftly and effectively in a real incident.

Engage with cybersecurity experts

Cybersecurity experts can conduct thorough assessments, identify vulnerabilities, and recommend tailored security solutions. They offer insights into the latest threat intelligence and emerging attack vectors, helping organizations stay ahead of cybercriminals.

Collaborating with external experts ensures that organizations benefit from a broader perspective and expertise that may not be available in-house. Additionally, experts can assist in developing and implementing comprehensive cybersecurity strategies, conducting employee training, and responding to incidents.

About the Author



Bogdan Glushko is the Chief Information Officer of Proven Data. Glushko actively leverages his years of experience restoring thousands of critical systems after incidents. Glushko is a trusted voice guiding organizations on resilient data strategies, ransomware response protocols, and mitigating evolving cyber threats. Through proven leadership, he continues delivering cutting-edge data preservation and recovery solutions that fortify business resilience against breaches, outages, and data loss from modern cyber attacks.

Bogdan Glushko can be reached online at https://www.linkedin.com/in/donglushko/ or via info@provendata.com, and at our company website https://www.provendata.com/.

Addressing Cybersecurity Challenges in Healthcare: A Strategic Approach

By David Lee, Chief Evangelist and Visionary for Tech Diversity, The Identity Jedi

As the healthcare sector becomes increasingly digital, it faces a growing threat from cybersecurity attacks. Recent years have seen a disturbing rise in data breaches, ransomware attacks, and other cyber threats targeting healthcare organizations. The consequences of these attacks are not just financial but can also compromise patient safety and trust. This article delves into the specific challenges posed by outdated software and limited integration with external partners and explores effective strategies that cybersecurity professionals can employ to enhance resilience across the healthcare ecosystem.

The Impact of Outdated Software and Limited Integration

Outdated software and limited integration with external partners are two significant factors that exacerbate the cybersecurity risks in healthcare. Many healthcare institutions still rely on legacy systems that are no longer supported by vendors, leaving them vulnerable to exploits that newer software would prevent. Additionally, the lack of integration with external partners means that data flow is often insecure and fragmented, creating multiple points of vulnerability.

Healthcare organizations hold vast amounts of sensitive data, including personal and medical information. Outdated software often lacks the necessary security patches, making it easy for cybercriminals to breach systems and steal data. Limited integration further complicates matters, as disparate systems make it challenging to implement a comprehensive cybersecurity strategy, increasing the risk of data breaches.

To effectively combat these risks, healthcare organizations must adopt tailored cybersecurity strategies that address their unique challenges. A one-size-fits-all approach is inadequate given the complexities of healthcare data and operations. Below are some key components of a tailored strategy:

Proactive Measures Over Reactive Responses

Historically, many healthcare organizations have adopted a reactive approach to cybersecurity, addressing threats only after they occur. However, this is no longer sufficient. Proactive measures, such as regular security audits, continuous monitoring, and threat intelligence, can help identify vulnerabilities before they are exploited. Implementing advanced threat detection systems and conducting regular penetration testing are also crucial steps in a proactive approach.

Comprehensive Risk Assessments

Conducting comprehensive risk assessments is essential for understanding the specific vulnerabilities within an organization. These assessments should consider both internal and external threats and account for the unique operational environment of healthcare institutions. By identifying the areas of highest risk, organizations can prioritize their cybersecurity investments more effectively.

The Role of Collaborative Efforts

Collaboration between hospitals, medical practices, and technology vendors is vital for enhancing cybersecurity resilience across the entire healthcare ecosystem. Such collaborative efforts can provide several benefits, although they also come with challenges that must be managed.

Benefits of Collaboration

- Shared Knowledge and Expertise: Collaborative efforts enable the sharing of knowledge and expertise, helping all involved parties to stay abreast of the latest threats and best practices.

- Resource Optimization: Pooling resources can lead to more effective and efficient cybersecurity measures, particularly for smaller organizations that may lack the means to invest in advanced solutions independently.
- Standardization: Working together allows for the development of standardized protocols and procedures, which can simplify the integration of new technologies and improve overall security coherence.

Challenges of Collaboration

- Data Privacy Concerns: Collaboration often involves sharing sensitive data, raising concerns about data privacy and compliance with regulations such as HIPAA.
- Coordination Issues: Achieving seamless coordination between different entities can be challenging, particularly when there are varying levels of cybersecurity maturity and differing priorities.

Fostering a Culture of Security Awareness

While technological solutions are critical, they must be complemented by a culture of security awareness and continuous improvement within healthcare organizations. Employees at all levels must understand the importance of cybersecurity and be trained to recognize and respond to potential threats.

Regular training sessions should be mandatory for all staff members, covering topics such as recognizing phishing attempts, proper password management, and the importance of data encryption. Continuous education ensures that employees stay updated on the latest cyber threats and how to mitigate them.

Leadership Support

Leadership plays a crucial role in fostering a culture of security. Executives must prioritize cybersecurity and allocate the necessary resources to support robust security measures. By leading by example, they can instill a sense of responsibility and urgency throughout the organization.

The rise in cybersecurity attacks within the healthcare sector is a pressing concern that requires immediate and sustained attention. By understanding the impact of outdated software and limited integration, adopting tailored and proactive cybersecurity strategies, fostering collaboration, and cultivating a culture of security awareness, healthcare organizations can significantly enhance their resilience against cyber threats.

In this rapidly evolving landscape, continuous improvement and vigilance are paramount. As healthcare executives, cybersecurity professionals, and technology vendors work together, they can create a more secure and robust healthcare ecosystem, ultimately safeguarding both patient data and the future of healthcare delivery.

About the Author

David Lee transitioned from a software engineering background to become a harbinger of change and inclusivity in the tech world. With over two decades of experience, he has left his mark on government agencies, Fortune 500 companies, and numerous fields, specializing in identity and access management. Recognizing that for technology to truly transform the world, it must embrace diversity, David serves as an agent of transformation, inspiring individuals to unlock their full potential. His influential voice and actionable insights have solidified his reputation as a respected figure in the ever-evolving tech landscape. When he speaks people listen. He is The Identity Jedi. David can be reached online at https://www.linkedin.com/in/identityjedi/ and at our company website https://www.theidentityjedi.com/.

How To Respond to The Rise of Banking Trojans

By Zac Amos, Features Editor, ReHack

The resurgence of banking trojans has become a major cybersecurity concern for financial institutions and their customers. These malicious backdoor programs continue to evolve and succeed due to their ability to evade detection and bypass traditional device security. As these attacks become more sophisticated, the need for robust protection mechanisms and agile response systems is more paramount than ever.

What Are Banking Trojans?

Banking trojans are a type of malware disguised as legitimate software and used by cybercriminals to attack online banking systems. They get their name from the infamous wooden horse used by the Greeks to infiltrate Troy and sack the city during the Trojan War.

These programs are particularly insidious due to their ability to initiate malicious activities undetected, having tricked the user into downloading them and granting the necessary operational permissions. By the time the victim discovers the attack, they've already lost huge sums of money.

Banking Trojans on the Rise

Banking trojans have existed since the dawn of online banking, steadily evolving over the years and increasing in functionality. In 2020, the FBI warned about the potential rise of app-based trojan intrusions following a 50% surge in mobile banking amid the COVID-19 pandemic.

It turns out the alert was warranted, as the number and complexity of banking trojan attacks have soared since then. According to Kaspersky's 2022 Mobile Threats report, nearly 200,000 mobile banking Trojan installers were detected — two times more than in 2021.

Despite stronger bank security features and newer system designs, malware continues to persist, adapting in scope and technical ability. What first started as a program primarily targeting bank customers has become a menace across various financial institutions, including FinTech and blockchain companies.

Even more concerning is that these attacks have become an international affair affecting organizations and their customers across continents. A recent example is Grandoreiro — a devious banking trojan operated as a malware-as-a-service to impersonate government entities in Africa, Europe, South America and the Indo-Pacific regions. This malware has targeted 1,500 banking applications in over 60 countries through sophisticated email phishing attacks.

How Do They Work?

Banking trojans are designed for different functions, including:

- **Overlay attacks:** The malware overlays a fake log-in page onto legitimate applications. When users enter their credentials, the trojan captures and sends them to the hacker. One example is the SharkBot banking malware, which primarily targets Android users.
- **Device control:** Some trojans can remotely control devices, including the lock and unlock features, camera, text messaging, and even screen content capture. The malware uses these to bypass security before perpetrating theft.
- **Keylogging:** These banking trojans record a user's keystrokes when logging into their bank accounts, allowing hackers access.
- **Data exfiltration:** This malware can exfiltrate SMS messages, intercepting sensitive information necessary for financial transactions, such as 2FA and OTP codes.

How Can Users Protect Against Banking Trojans?

Addressing malware's increasing pervasiveness requires a comprehensive framework involving a mix of top-notch security measures and the most recent cybersecurity best practices.

1. Install Anti-Virus and Malware Detection Software

Just as locking doors and windows prevents physical infiltrations, installing the latest antimalware and antivirus programs protects banking information from malicious threats. Financial institutions can employ advanced analysis tools with hybrid functionality to scan for threats and open detected trojans in a Sandbox for safe assessments.

2. Avoid Using Public WiFi for Banking Transactions

Wireless networks freely provided in public spaces like hotels and coffee shops may present an entry point for malware intrusion. Hackers piggybacking the connection can execute man-in-the-middle attacks to intercept online financial transactions.

Unfortunately, up to 20% of Americans continue to use public WiFi for their banking-related activities, exposing themselves to higher risks of attacks. A workaround is to use a VPN when connecting to these networks, as these systems encrypt data and protect sensitive information.

3. Employ Strong, Unique Passwords

Passwords are like the final piece to the cyberthreat puzzle. Once breached, hackers can initiate various forms of malware attacks on a user's online account. Best practices recommend changing passwords every three months, ensuring they are complex enough to limit the efforts of threat actors. The rule of thumb is to create passwords containing over 16 characters with a combination of letters and numbers.

4. Use Multifactor (MFA) Authentication

MFA provides an extra security layer against malware threats by requiring additional forms of verification. This can prevent unauthorized access even if login credentials are compromised. However, this measure may soon become ineffective, as more sophisticated threats like the Chameleon banking trojan can disrupt biometric authentication operations, highlighting the need for a multifaceted approach to cybersecurity.

5. Download Only Trusted Apps

Kaspersky's 2023 Financial Threats Report shows mobile banking malware has increased by 32% compared to 2022. This underscores the need for users to install apps from trusted sources only — the Apple App Store, Google Play or Amazon Appstore. Even so, many apps from these stores are not 100% failsafe, but at least they undergo some form of security screening before being listed.

6. Be Cautious with Email Links

Avoid clicking links or downloading attachments from unknown emails to prevent phishing attacks. For example, the Emotet trojan typically spreads through malicious email attachments disguised as invoices or shipping notifications.

Don't Fall Like the Trojans

Banking trojan intrusions have become more frequent and complex in recent years. The best way to protect against this evolving threat is to maintain a robust security posture against all potential attack surfaces. This means employing a mix of cybersecurity measures and best practices. Financial institutions must step up their efforts to safeguard their systems by utilizing the latest advanced threat monitoring and analysis tools.

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.

Getting Wins for Security Leaders: Strategies and Considerations for Success

Navigating the Cybersecurity Landscape: Achieving Impactful Wins Through Data, Collaboration, and Continuous Improvement

By Chris Schueler, CEO, Simeio

Do not think of advocating for critical security investments as a single battle, but a drawn-out campaign requiring extended support. Like any long war, the only way to secure backing is to convince your commanders that these efforts are worth the trouble. By identifying and pursuing objectives which are most likely to yield impressive wins, security leaders set themselves up for long-term success. fighting chance to secure their enterprises.

This article explores practical strategies and considerations to help security leaders achieve impactful wins in today's ever-evolving cyber threat landscape. As such, it considers four overarching focus areas which are critical in communicating successful results.

Empowerment Through Data-Driven Insights:

Data-driven insights provide hard-hitting numbers which are easily understood by those without expert-level cybersecurity knowledge. For example, a 25% increase in productivity, a $250,000 value from a security initiative, and clear evidence of breach attempts are all easy to digest. Use this information to communicate impact.

● Metrics that Matter: Move beyond vanity metrics. Focus on key performance indicators (KPIs) that demonstrate the effectiveness of security controls in mitigating real threats.

● Security ROI (Return on Investment): Quantify the value proposition of security investments. Translate the impact of security measures into financial terms to gain buy-in from leadership.

● Actionable Threat Intelligence: Utilize threat intelligence to prioritize vulnerabilities and focus resources on the most critical risks.

Building Strong Alliances for Collaboration:

Communicating value is more than just listing out numbers. Security leaders must build a rapport with their tech-focused peers as well as fellow employees in business-oriented departments. Ensure that the full tapestry of an enterprise knows what the security team is doing. As a result, they will become much less defensive when changes are needed.

● Breaking Down Silos: Foster collaboration between security teams and other departments like IT, HR, and legal. Align security initiatives with broader business goals.

● Executive Advocacy: Secure executive sponsorship for security initiatives. Educate leadership on the potential cost of cyberattacks and the value of proactive security measures.

● Industry Collaboration: Share best practices and learn from others. Participate in industry associations and leverage threat intelligence communities to stay informed about emerging threats.

Prioritizing User-Centric Security Solutions:

Customers and employees are the lifeblood of any enterprise yet can be a serious vector for data breaches. Cultivate awareness of cybersecurity best practices and leverage security- focused applications. Doing so shrinks potential attack surfaces and removes friction from the user-experience.

● Usability Matters: Implement security solutions that are user-friendly and minimize disruption to workflows. A balance between security and user experience is crucial for successful adoption.

● Security Awareness Training: Invest in ongoing security awareness training programs to educate employees on cyber threats and best practices for secure behavior.

● Empowering Users: Provide employees with the tools and resources they need to identify and report suspicious activity.

Demonstrating Continuous Improvement:

Filing and presenting regular reports on the upward trajectory of a digital transformation is critical to advocating for its continuation. Therefore, make use of compiled metrics by linking them to your audits and assessments. Communicate the necessity of ongoing improvements by highlighting emerging cybersecurity threats and thus the business value of emergent technologies.

- Regular Security Assessments: Conduct periodic vulnerability assessments and penetration testing to identify and address security gaps proactively.

- Metrics-Driven Reporting: Regularly communicate security posture improvements to leadership using data-driven reports. Showcase the effectiveness of implemented controls.

- Adaptability and Continuous Learning: Stay current with evolving threats and adapt security strategies accordingly. Embrace continuous learning to ensure your security posture remains effective.

By focusing on these strategies, security leaders can achieve and communicate the impact of their hard-fought wins. Thus, they demonstrably improve an organization's overall cybersecurity posture while making key stakeholders aware of this. Communication, collaboration, and data-driven decision making are key to securing lasting success.

Therefore, the most impactful security leaders are those who embrace the link between the success of their work and the success of their fellow employees.

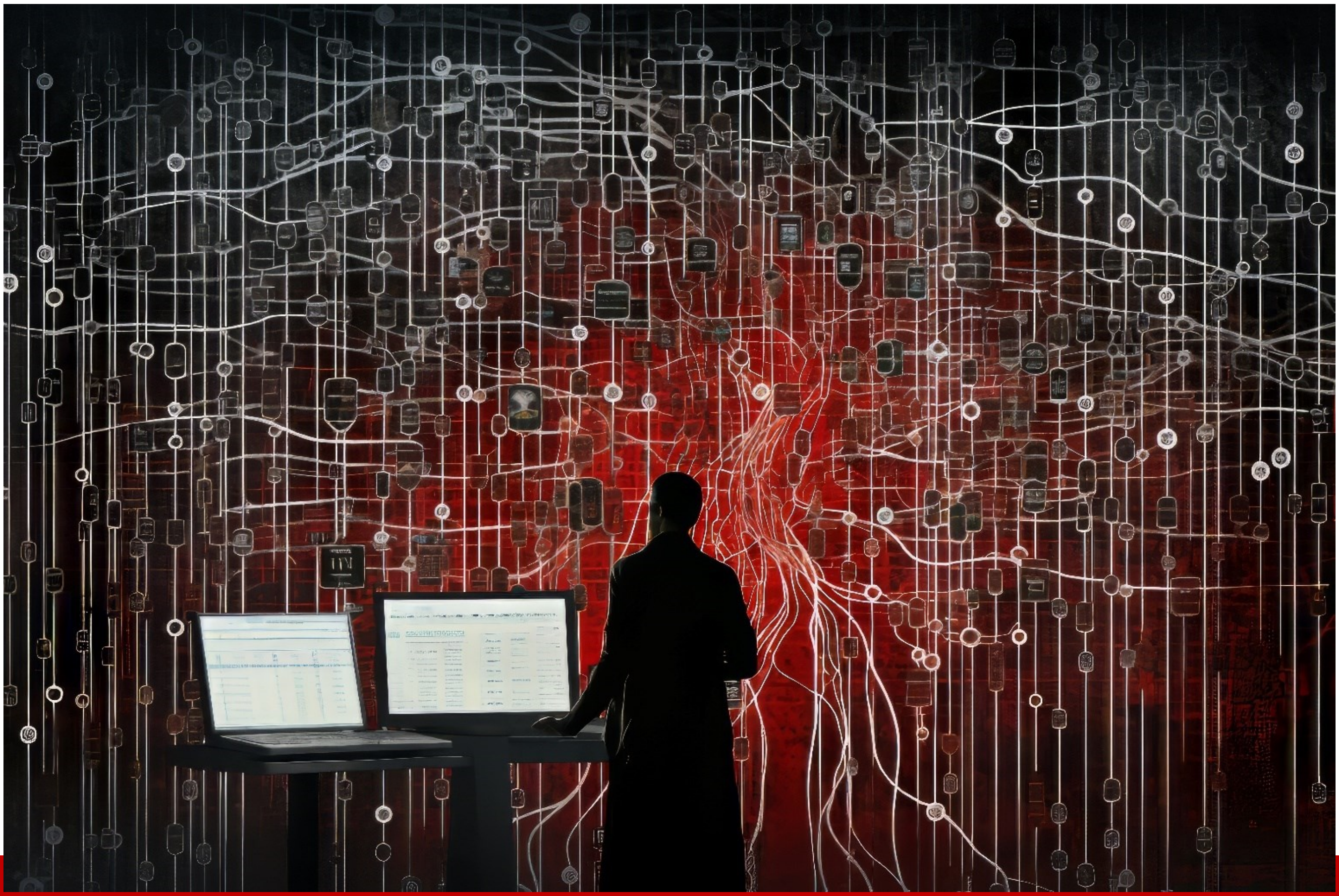
About the Author

Chris Schueler, as Chief Executive Officer, drives the overall vision and strategy for Simeio. He is a proven leader with extensive experience in Go To Market, Operations, and Product Development in the managed security services space.

He joined Simeio from Trustwave; leading all aspects of their security services and go-to-market. Under his leadership and strategy, created a significant growth engine in revenue and profit, ultimately moving Trustwave's services into global leadership positions in all markets and analyst communities. Prior to that, Chris spent 11 years with IBM building, growing, and expanding their cloud and security managed services businesses achieving significant growth in revenue, margin, and NPS in both large public and small emerging environments. Chris is a veteran of the US Army and spent 12 years in Information Operations Commands.

Chris received a Bachelor's degree in OMIS from Northern Illinois University and his Master's of Business Administration degree from Auburn University. He is a husband and father to 3 daughters, a health and fitness enthusiast, and an outdoorsman.

Chris can be reached online https://www.linkedin.com/in/cschueler/ or by contacting us on our website: https://simeio.com/contact/



Internal And External Threat Intelligence

How To Balance the Two Sources

By Vlad Ananin, Technical Writer, ANY.RUN

In cybersecurity, threat intelligence covers a broad range of activities concerning collection, analysis, and dissemination of information on the current threat landscape. In terms of sourcing, the two primary types of threat intelligence are internal and external, and finding the right balance between these two can be key to not only robust but also efficient cybersecurity strategy.

Understanding Internal and External Threat Intelligence

Internal threat intelligence is the data collected from within an organization's own networks and systems. This can include data on attempted or successful cyber attacks, system vulnerabilities, and anomalous network activity. Specifically, such data can be pulled from organization’s logs and traffic data for network-connected devices, security systems like SIEMs, IDS, and antivirus software.

External threat intelligence refers to the data collected from outside sources about past and current threats. This can include information about threat actors, their tactics, techniques, and procedures (TTPs), indicators of compromise (IOCs), and more. This type of intelligence is provided by different products, including feeds, as well as specialized platforms and portals that accumulate large databases and allow users to search them.

Advantages of Internal Threat Intelligence

Detailed and Specific Understanding

Internal threat intelligence, being sourced from the organization's infrastructure, provides a detailed and specific understanding of an organization's unique threat landscape.

Real-Time and Relevant Data

Internal threat intelligence offers real-time and highly relevant data. It allows organizations to quickly identify and respond to threats that are directly impacting their systems and networks.

Historical Records

Historical records in internal threat intelligence, encompassing past alerts and network activity, offer valuable insights into potential incidents. These records also aid analysts in quickly deciding if an alert is a false positive, enhancing threat response speed and accuracy.

Advantages of External Threat Intelligence

Broader Understanding of Current Threats

Internal security systems can only identify threats that are already known. External threat intelligence offers fresh information from various sources. In the event of a possible security incident, such intelligence can provide valuable context and insights.

For instance, it can help you determine if the incident is part of a larger campaign targeting multiple organizations, or if it's an isolated incident. It can also supply information about the threat actor's typical behavior and tactics, which can guide your incident response strategy.

Proactive Threat Anticipation

External threat intelligence enables organizations to anticipate potential threats and vulnerabilities. By understanding the TTPs of threat actors and the latest trends in cyber attacks, security teams can proactively strengthen their defenses and be better prepared to respond to incidents.

Bringing Internal and External Threat Intelligence Together

Use Internal Data for Baseline Security

Internal threat intelligence should be the foundation of your organization's security strategy. This means that the data from your own networks and systems must always be analyzed and processed to continuously improve your security measures.

Leverage External Data for Threat Anticipation

External threat intelligence can be used to anticipate and prepare for threats that have not yet directly impacted your organization. Regularly review external intelligence for information about new and emerging threats and use this information to update your security measures and train your employees.

Combine Both for Incident Response

In the event of a security incident, both internal and external threat intelligence can be valuable. Internal data can help you understand the nature and scope of the incident, while external data can provide context and insights about the threat actor and their tactics.

Threat Intelligence Portal from ANY.RUN

One example of external threat intelligence is ANY.RUN's suite of TI products that includes Feeds and Lookup.

The services provide users with access to refined data extracted from ANY.RUN sandbox's public database of threat samples uploaded by its global community of over 400,000 cybersecurity experts. The result is an extensive repository of up-to-date information related to the latest attacks around the world.

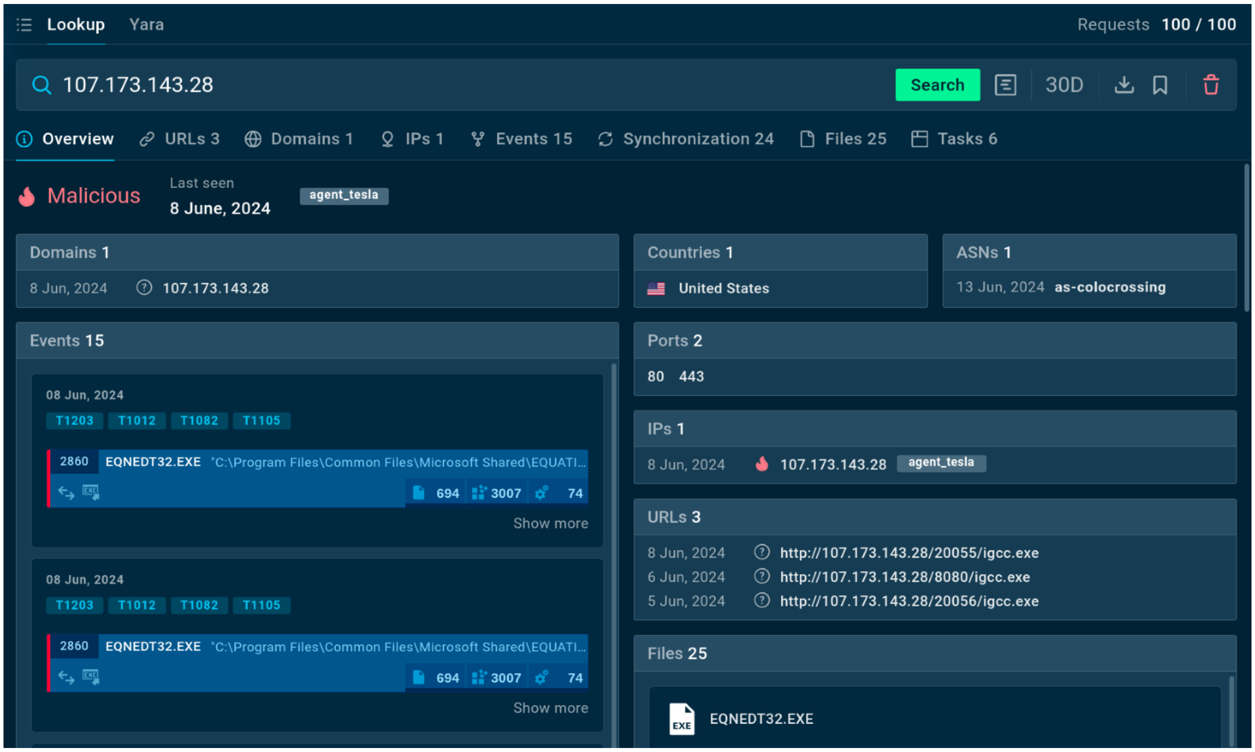
Threat Intelligence Feeds supply a continuously updated stream of fresh indicators of compromise directly into SIEM and TIP systems in STIX format. The feeds can be integrated and used completely free of charge in the form of a demo sample.

Threat Intelligence Lookup provides users with a platform for threat investigations with a built-in search engine. Analysts can use it to search ANY.RUN's extensive database of threat data and enrich their indicators and understanding of threats they encounter.

By submitting artifacts, such as file hashes, domains, IP addresses, TTPs, ports, registry keys, etc. (a total of over 30 ones), users can identify their context in the form of corresponding IOCs, as well as ANY.RUN sandbox sessions, where these artifacts were detected.

The service also supports combined searches, making it possible to submit a query featuring several artifacts at the same time for more refined results.

Consider the example below, where we submit a search query for a certain IP.



107.173.143.28

Malicious — Last seen 8 June, 2024 — agent_tesla

Domains 1
8 Jun, 2024 107.173.143.28

Countries 1
United States

ASNs 1
13 Jun, 2024 as-colocrossing

Events 15

08 Jun, 2024
T1203 T1012 T1082 T1105
2860 EQNEDT32.EXE "C:\Program Files\Common Files\Microsoft Shared\EQUATI...
694 3007 74

08 Jun, 2024
T1203 T1012 T1082 T1105
2860 EQNEDT32.EXE "C:\Program Files\Common Files\Microsoft Shared\EQUATI...
694 3007 74

Ports 2
80 443

IPs 1
8 Jun, 2024 107.173.143.28 agent_tesla

URLs 3
8 Jun, 2024 http://107.173.143.28/20055/igcc.exe
6 Jun, 2024 http://107.173.143.28/8080/igcc.exe
5 Jun, 2024 http://107.173.143.28/20056/igcc.exe

Files 25
EQNEDT32.EXE

The service identifies it as “malicious” and as belonging to Agent Tesla. It provides a wealth of context, including ports, ASN, country of origin, files, and a list of interactive sandbox sessions that we can explore in-depth to see how this particular threat operates. Organizations can request a free trial of the service.

Conclusion

Balancing internal and external threat intelligence is crucial for a robust and efficient cybersecurity strategy. Internal threat intelligence offers detailed, specific, and real-time insights into an organization's unique threat landscape. In contrast, external threat intelligence provides a broader understanding of current threats and enables proactive threat anticipation. By leveraging both sources, organizations can enhance their security posture and effectively respond to incidents.

About the Author

Vlad Ananin is a technical writer at ANY.RUN. With 5 years of experience in covering cybersecurity and technology, he has a passion for making complex concepts accessible to a wider audience and enjoys exploring the latest trends and developments. Vlad can be reached online at the company website https://any.run/

From Crisis to Catalyst: A CEO's Lessons Learned from A Cybersecurity Incident

By Ariel Katz, CEO, Sisense

There are events in business and life that put everything else into perspective. Sometimes, these are moments of crisis, yet also moments of clarity; moments of shock, and moments of growth.

In April, Sisense, the company I lead, suffered a cybersecurity incident. As a tech company serving some of the biggest names in the industry, it wasn't a huge shock. We were hardly the first—and certainly won't be the last—company to suffer a security incident, and the question wasn't really "if", but "when" it would happen.

Adversity comes with the unique opportunity to surpass yourself and I believe that is exactly what we at Sisense have done – rise above. The wisdom and lessons we've gained from this incident are precious and hard-earned, and I thought I'd take some time to share what I learned from one of the most challenging months of my career.

Leading with transparency through crisis

A security incident is a harsh reality, and this one hit us hard. While the details were initially confusing, I knew staying silent wasn't an option and recognized that we needed to be completely transparent with our customers from the get-go. Sharing this experience on my LinkedIn account wasn't just about Sisense—security threats are an industry-wide challenge. By being open, I hoped to learn from others and offer solidarity to CEOs facing similar situations. In the face of crisis, transparency can foster trust and pave the way for a more secure future for everyone.

Crisis reveals your team's untapped potential

A crisis can act as a crucible, forging unexpected strengths within your team. You discover colleagues you can trust implicitly to deliver, even when the task is far removed from their usual duties. Some individuals step up and become true leaders during stressful times, demonstrating that leadership is not earned with a title but through action. Crisis can be a transformative learning experience, showcasing the hidden depths of talent and dedication within your team. When facing such challenges, collaboration is key. Working together, a team can unlock hidden reserves of creativity and problem-solving skills, allowing them to overcome even the most daunting obstacles.

Human touch in crisis: prioritizing customer care

A security incident can feel impersonal, but I realized the impact on our customers was anything but. I knew I had to put myself in their shoes, understand their worries, and address them directly. They were accountable to their stakeholders, and I felt a deep responsibility to provide clear facts and a commitment to a swift resolution. Recognizing that both us and our customers were affected, I promptly picked up the phone and personally called dozens of our top customers.

These weren't scripted conversations: I wanted genuine human interaction. In addition to these calls, we held daily video briefings. It took time, but I believe those efforts went a very long way in building trust. Every communication that followed, from daily FAQs to ongoing support, was tailored to our customers' needs. We listened closely to their concerns and actively addressed them. In a crisis, a human touch can make all the difference: it shows we care about our customers as people, not just numbers. And being customer-centric has always been, and always will be one of our core values as a company. Faced with the dilemma of oversharing in response to customers' requests versus sticking to facts and risking complaints about a lack of information, I chose to stick to facts for the benefit of the customers.

Learning from crisis: a CEO's responsibility

My leadership journey has taken me from corporate executive to CEO. At Microsoft, I was part of a team, tackling problems collaboratively and having a manager to share responsibility with. Now, at Sisense, I have the privilege of shaping the company's vision and turning ideas into action. But with that responsibility comes accountability. There's no one to pass the buck to: the onus rests on my shoulders during good times and bad times. This incident was a stark reminder of that responsibility but also a chance to learn. By taking full ownership, I could lead by example, navigate the crisis, and emerge stronger alongside the Sisense team. A CEO must learn from challenges and turn them into opportunities for growth.

Lessons Learned: Building a stronger security culture

The recent security incident served as a reminder. We were lucky to maintain business continuity, but it exposed vulnerabilities. Now, our focus is on continuous enhancements.

We're working to identify and address weaknesses. A systematic review of security protocols and communication is crucial to eliminate those chinks in the armor. This isn't just a job for the CEO or CISO: cybersecurity is a company-wide responsibility. Everyone plays a part.

Moving forward, we'll leverage this experience and will come out stronger. While the team responded admirably under pressure, we could also have been more prepared. For instance, companies of our size don't always have a crisis response plan, but having one would have saved us valuable time. Most importantly, we'll be continuing to cultivate a culture of security awareness. Every employee needs to understand their role in safeguarding our company. By proactively creating a comprehensive communication incident response plan, we'll be better equipped to navigate future challenges. The time to invest in preparedness is now. This way, we can focus our energy where it truly matters: delivering exceptional value and service to our customers.

About the Author

Ariel Katz, CEO, Sisense. Ariel brings over 25 years of experience to the world of technology and the development of large enterprise cloud products. He played a leading role at Microsoft in establishing and building Power BI, one of the world's leading cloud BI services. Later, he led the development of Dynamics 365 for Sales, and helped turn it into a smart and modern cloud service. Ariel was part of the senior management team at Microsoft's development center in Israel and was previously the site's Chief Technology Officer.

Ariel can be reached on his LinkedIn page at Ariel Katz

Cyber-Informed Engineering – A New Perspective on OT Security

By Andrew Ginter, VP Industrial Security, Waterfall Security Solutions

Cyber-Informed Engineering (CIE) is a new perspective on OT cyber risk – one that is being embraced by OT/engineering teams and IT/enterprise cybersecurity teams alike. This kind of consensus among IT and OT teams is unprecedented in the twenty-year history of the OT security field.

Threats

The OT threat environment continues to worsen, which means we have an increasingly pressing need to engage IT and OT teams in addressing material cyber risks to physical operations. In particular, in 2023, 68 cyber-attacks shut down, damaged, or otherwise physically impacted over 500 operational technology (OT) sites, according to the latest Waterfall / ICSStrive 2024 Threat Report. The rate of this class of attack was mostly "flat" between 2010 and 2019, with zero to five attacks in the public record every year for manufacturing and heavy industry. Since the turn of the decade, the number of these attacks has roughly doubled annually, compounded. The problem of OT security has changed, from a "theoretical" problem, to one that is real and growing exponentially.

Most attacks causing these shutdowns are ransomware, though hacktivist, supply chain and nation-state attacks are increasing as well. Worse, the most sophisticated ransomware groups are buying and selling attack tools from and to nation states – the tools and techniques used by the two kinds of threat actors are becoming indistinguishable.

OT Is Different

A perennial problem with cybersecurity in OT is that OT is different. In most IT networks, information is the asset, and our imperative is to protect the information. OT networks automate physical processes – often very expensive, dangerous physical processes. The cybersecurity imperative on OT networks is to protect safe, reliable and efficient physical operations, and only secondarily to protect sensitive trade secrets and other information, if there is any information such in the OT network at all.

A second issue with OT networks is change control. When enterprise security teams ask engineering teams to bring the entire OT network up to date with security updates, the engineering teams most often refuse. Why? The clarifying question most engineering teams really should ask but rarely do, is “How likely is that change to kill anyone?” Engineers need that question answered before they make any change, and the likelihood of a safety incident is never zero. There is no way to make physical processes perfectly safe.

A second question that helps clarify the problem is “How likely is that change to trip the plant and trigger an un-planned shutdown of our billion-dollar asset?” All change represents a physical risk. Engineering teams are required, by their businesses, by their professional associations and often by law, to address material risks to physical operations. Engineering Change Control (ECC) is the discipline by which the risks of proposed changes are evaluated, tested and managed. The problem is that ECC is very expensive. Change on OT networks is not impossible, but someone is going to have to allocate budget to charge engineering services against, especially in organizations with small or no in-house engineering teams.

Cyber-Informed Engineering

These threats and the “difficult” nature of OT / industrial automation networks are why Idaho National Laboratory is working on the new Cyber-Informed Engineering (CIE) initiative. CIE is positioned as “a coin with two sides.”

- One side is cybersecurity – from teaching engineering teams about cyber threats to physical operations and engineers' obligations to the business and to society to address those threats.
- The other side is engineering – use the powerful tools that engineers have for managing physical risk – use these tools to address cyber threats as well.

For example, imagine you work in a large refinery. The refinery uses catalytic crackers – six story tall pressure vessels filled with hot hydrocarbons. Imagine you work 8 hours a day inside the kill radius of a worst-case cracker explosion. How would you prefer to be protected from a cyber-attack that over-heats the furnace under one of your crackers? Would you prefer a mechanical, spring-loaded over-pressure relief valve that, if the cracker over-pressurizes, is forced open mechanically to route hot hydrocarbons to a flare stack? Or would you prefer a longer password on the computer controlling the furnace?

Most people answer that they would prefer a mechanical valve – these valves have no CPUs after all, and thus are in a real sense "unhackable." True experts respond that they want three or four of these valves, thank you, because there are risks of corrosion and metal fatigue that might impair the operation of a single valve. And they want a longer password on the computer controlling the furnace. And they want an absolute "boatload" of cybersecurity in addition to these two measures – this is their life on the line after all. This latter answer is the correct one – when we "spend the CIE coin," we do not spend one side of the coin or the other. We spend the whole coin.

But think about it – where is the over-pressure relief valve in the ISO 27001 standard? In the NIST Cybersecurity Framework? Or even in the industrial IEC 62443 standard? There is no hint of over-pressure relief valves or other engineering tools in those standards – these are cybersecurity standards, not engineering standards. Safety engineering, protection engineering, automation engineering and related disciplines all have powerful tools at their disposal to address all threats that can bring about physical operations. These tools have not been applied universally nor systematically to address cyber threats but should be.

The Most Significant Change In a Decade

CIE is arguably the most significant change in OT security in over a decade. When engineering teams and even many enterprise security teams learn about CIE, they often react with something like, "This makes so much sense. Why is this new? This shouldn't be new. Why have we not been looking at the problem this way since the beginning?"

Engineers understand consequences, physical process design, and a wide variety of "unhackable" electro-mechanical and other protections and need to come up to speed on cyber threats and the applicability of their tools to cyber threats. Enterprise security understands threats and the "boatload" of cybersecurity mitigations that can be deployed as needed for those systems that do not yet have electro-mechanical or analog mitigations. With each team contributing their unique knowledge and perspectives, the OT security problem suddenly becomes tractable and affordable.

About the Author

Andrew Ginter is the VP of Industrial Security at Waterfall Security Solutions. He leads a team of subject matter experts who work with the world's most secure industrial sites. Andrew also writes about what he learns from these sites, having written three books on OT security and contributed regularly to industrial security standards and guidance.

For a high-level introduction to CIE, the engineering perspective on cybersecurity and due care obligations, you can request a free copy of Andrew’s latest book Engineering-Grade OT Security. Andrew can be reached at andrew.ginter@waterfall-security.com and at our company website https://waterfall-security.com/

Strategizing Compliance and Security In AI: A Hands-On Guide for IT Leaders

By Neil Serebryany, Founder and CEO of CalypsoAI

Navigating the complex web of compliance in the AI era is a formidable challenge, and aligning your organization with existing and emerging legal, ethical, and regulatory standards has never been more important. Using AI-driven tools proactively, businesses can achieve higher levels of data governance and threat detection than they would by using traditional methods. The key to proactive compliance is having a deep understanding of both the opportunities and vulnerabilities AI tools introduce. This requires a dual focus on the compliance landscape and the ever-present threat of cyberattacks, which means incorporating rigorous oversight and meticulous implementation of security measures. Employing sophisticated AI algorithms allows companies to monitor vast networks for abnormal activity and react in real time, which can significantly reduce the potential for major breaches.

It's imperative that compliance be considered at every stage of the AI system development lifecycle, from the initial design to deployment. Embedding compliance-centric considerations into project planning can ensure every phase achieves the required standards of data privacy and ethical use. The importance of this goes beyond merely legal requirements; systems designed to be technically proficient, culturally sensitive, and ethically sound will bolster public trust and brand integrity.

Before this can happen, however, the DevOps teams must be equipped with the necessary knowledge about AI compliance and the latest cybersecurity practices, and downstream user teams, from tech specialists to management, must also understand compliance issues that might arise. To future-proof your organization against problematic, but avoidable, compliance issues, consider these elements of an AI security culture, which are both strategic and practical:

Risk Assessment

Conducting thorough risk assessments can identify potential compliance risks your organization faces. In addition to being regular, these assessments should be exhaustive, and involve scrutiny of every internal decision related to AI, from reviewing data handling procedures to comprehensively analyzing how AI impacts privacy, fairness, and transparency within your organization to reviewing and auditing security protocols. Such assessments should be the foundation of your cybersecurity strategy, ensuring that every aspect of AI deployment is scrutinized for potential risks.

Policy Management

Developing clear and robust policies is essential for guiding all aspects of organizational behavior in your organization, and AI-related activities must be included. AI governance policies should outline the expectations for employee conduct, the controls in place to support those expectations, and the consequences of non-compliance.

Technical Controls

Implementing technical controls, such as policy-based access and traceability mechanisms, to monitor and manage how AI tools are used within your company can go a very long way toward ensuring your digital infrastructure remains secure against both internal and external threats.

Transparency and Accountability

Discussing accountability with a group of decision-makers usually guarantees applause; transparency not so much. But early GenAI deployments have shown that it’s tough to have one without the other. Maintaining transparency with employees about how AI technologies are used by, for, and within your company helps build trust *and* accountability, and lessen resistance to compliance mandates. It’s also important that external stakeholders, customers, and the public understand what AI-dependent measures are in place to safeguard their data and privacy.

Continuous Education and Training

Developing an on-going AI compliance training curriculum and ensuring that every person in the company participates will equip your teams with the necessary knowledge and tools to handle AI responsibly. A regular cadence of refreshers and updates help cultivate a compliance-first mindset across the organization.

Navigating the complex world of AI compliance and security is challenging, but doing so successfully is essential to maximizing the technology's benefits and utility. Integrating compliance into every aspect of your AI initiatives and utilizing AI-driven security solutions can protect your organization's digital assets and help to maintain a consistent regulatory posture.

About the Author

Neil Serebryany, founder and CEO of CalypsoAI, holds multiple patents in machine learning security and is widely regarded as a leading voice in the field. Being one of the youngest venture capital investors and working on the front lines of national security innovation at the Department of Defense spurred him to create AI Security, an industry that didn't exist four years ago. CalypsoAI's mission is to become the trusted partner and global leader in AI Security. Neil can be reached online at X (formerly Twitter), LinkedIn, email via neil@calypsoai.com and at our company website https://calypsoai.com/.

Sheltering From the Cyberattack Storm – Part Two

By Nick Lines, Security Product Expert, Panaseer

In the first part of this series, I discussed sophisticated cyberattacks, analyzed an example, and offered advice on how to remediate against such an attack. But the cybersecurity storm doesn't stop there.

While sophisticated attacks may be the hardest to defend against, they're also the rarest, requiring a level of skill and knowledge usually limited to state-backed adversaries or well-established cybercrime groups. Because they have a lower bar for entry, the majority of attacks we see fall into the categories of human-operated industrialized and opportunistic attacks – which are often automated. But that doesn't make them any less dangerous, and they often have long, destructive tailwinds. However, research shows that 98% of attacks could be prevented with basic cyber hygiene, and in this second installment I'll show how this applies to both industrial and opportunistic attacks.

Industrial attack inundation

Industrial attacks are operated by humans and require some level of technical skill. But either the initial exploit or the lasting impact is exacerbated by poor cyber hygiene. There are multiple examples of such attacks from the last few months, but the biggest was the MOVEit attack in June 2023. At the latest count, the attack has impacted close to 2,800 organizations and almost 95 million individuals. Sadly, education and healthcare institutions were most affected.

The main perpetrator was the infamous Cl0p cybercrime gang, which industrialized an SQL injection vulnerability within MOVEit to distribute ransomware widely. The attack was so damaging that the SEC is currently investigating Progress Software – the maker of MOVEit. But whilst the initial breach of MOVEit was down to a tenacious human effort from the attackers, organizations are still falling victim to it almost a year later. This could be avoided by patching MOVEit.

Another recent industrialized attack is the Okta support system breach in October 2023. This was caused by stolen credentials rather than a highly skilled exploit. While the initial attack on a support system may seem innocuous, it prevented Okta from releasing updates to customers for 90 days. The lesson here is that every system – no matter how insignificant – must be considered as an entry point, and that the right controls have to be in place to prevent infiltration.

Opportunistic overflow

The last attack type is opportunistic. These attacks target low-hanging fruit and are the easiest to execute, often relying on vulnerabilities that have existed for years being exploited by automated adversaries. Log4J is a prime example of an opportunistic attack. Disclosed in late 2021, the vulnerability was so damaging because Log4J – an open-source logging library – was widely used in organizations of all kinds. It’s estimated that 93% of enterprise cloud environments were impacted.

Checking for known vulnerabilities, knowing where they are in your code base, and addressing them would confine the Log4J vulnerability to the annals of history. However, as recently as December 2023, two years after the exploit was discovered, a third of applications were still using an unpatched and thus vulnerable version of Log4J.

Similarly, Microsoft Exchange continues to be a rich source for automated attacks, as the UK’s Electoral Commission found to its cost in August 2023. Data from the ShadowServer dashboard shows there are more than 88,000 publicly accessible Exchange servers that possibly have critical vulnerabilities. Some may have been mitigated, but when you consider that keeping up to date with patches could remediate these vulnerabilities, it’s a frightening figure.

Turning a downpour into a drop

With attackers tending to pick off the easiest targets, focusing on security fundamentals, better cyber hygiene, and ensuring the right controls and policies are in place will help head off almost all industrialized and opportunistic attacks.

Yet, having policies and controls is only half the battle. The shifting, evolving IT landscape makes security a moving target. Organizations need total and continuous visibility over where and how controls have been implemented, to identify whether they are working as they should be, and close potential coverage gaps.

Too often organizations are relying on incomplete, siloed and even contradictory information. Security tools can be unreliable witnesses; they only report on what they alone can see, not the whole picture. This leads to conflicting reports, allowing undiscovered vulnerabilities and threats to hide in the fog. Overworked and stressed security teams are drowning in data but lacking insights that can drive change.

Overcoming these problems is a big data challenge. CISOs need a validated system of record they can trust that gives total visibility over coverage gaps and their true control status. Trusted data allows businesses to assess risk in the context of their business. This enables security teams to identify and take action on high risk issues to mitigate them instead of focusing on the wrong things, such as reporting, fixing yesterday's problems, or just dealing with indicators of compromise instead of solving the root causes.

As it's the root cause of so many attacks, let's take patching as an example. Ensuring every single asset on your network is updated is a daunting task. But with the right contextual data to show which machines represent the greatest risk, security teams can focus on the highest priority assets first. This targeted approach will drastically reduce risk exposure and improve the efficiency of overstretched security practitioners.

Brighter skies ahead

Sophisticated, industrialized, and opportunistic attacks all differ, and remediation tactics vary from ensuring zero trust to patching. But there is one key thread woven throughout the approach to defense against each – data. Without it, security leaders and their teams are left in the dark, unsure which assets are critical and require immediate attention, and which can be prioritized for now.

Those organizations that can harness the power of the data at their fingertips will be well equipped to ride out the cyberattack storm. Whilst those that continue to ignore this invaluable resource will remain caught up in the never-ending downpour of attacks.

About the Author

Nick Lines, Security Product Expert, champions Panaseer's unique value and ensures they're helping solve the biggest challenges in cybersecurity. He's worked for multinational systems integrators and consultancies in roles including developer, technical sales, and offering management, and previously spent a decade at Microsoft. Nick can be reached online at LinkedIn and at our company website https://panaseer.com/.

Striking a Balance Between the Risks and Rewards of AI Tools

By Michael Gray, Chief Technology Officer, Thrive

With all the recent hype, many may not realize artificial intelligence is nothing new. The idea of thinking machines was first introduced by Alan Turing in the 1950s, and the term “artificial intelligence” was coined nearly 80 years ago. However, the technology has gained new notoriety thanks to the introduction of generative AI. Yet, the buzz has come with hesitations around things like implementation, training, and ultimately, security.

Many business leaders are still questioning whether they should implement generative AI within their organizations. Each company has different goals and capabilities and therefore needs to look at the benefits and challenges associated with the technology within the context of their business. As such, anyone exploring AI adoption must understand the promised rewards and the potential risks of doing so, asking the right questions along the way to determine the right approach for their company.

Promised Rewards of AI

Large language models (LLMs) like ChatGPT have introduced AI to the masses and have been rapidly adopted by employees, students, and consumers alike to ease everyday tasks. ChatGPT and other generative AI-powered chatbots allow people to ask questions in plain language, meaning using it is simple and doesn't require much technical skill.

Beyond ease of use, the technology promises:

- **Increased productivity:** With LLMs helping workers do everything from coding faster to digesting large quantities of research in minutes, workers are now free to focus on more strategic tasks, instead of time-intensive ones.
- **Operational efficiencies:** By embedding generative AI tools like chatbots into software or processes, organizations can get the information they need to execute on tasks quickly or automate processes altogether – significantly streamlining workflows.
- **Cost savings:** When time is saved and employees are more productive, organizations can reduce spend while also increasing profit.

Potential Risks of AI

While glamorous at first look, AI does not come without pitfalls. Understanding these pitfalls – and the risks they pose to businesses – can help prevent misuse, bias, security breaches, and more. A few risks organizations should be aware of:

- **Data sharing**: To get the answers relevant to a specific business or function, that organization needs to first give an LLM data. For example, if you want ChatGPT to write a summary of a meeting, you will have to share the meeting transcript. This means that if proprietary information gets shared with an LLM, it remains in the LLM's knowledge system and can be accessed by other users. This is typically outlined in an End User License Agreement – which many users typically sign without much thought.
- **Bias or inaccurate answers**: Answers provided by LLMs have been known to be biased, inaccurate, or made up. Understanding where the model is getting the information from and reviewing the information with an air of caution before using it can help identify any of these risk factors before they cause harm.
- **Copyright infringement**: It is also important to remember that anything produced by generative AI is considered part of the public domain – so, putting your name on something produced by ChatGPT could lead to copyright troubles down the line.

Deciding the Right Approach

Deciding whether to use this technology will not be black and white. Luckily, there are steps organizations can take as they consider next steps that can help guide them:

- **Define the use case:** Organizations should take a step back and ask themselves why they want to adopt the technology – is it to improve specific processes? If so, which ones?
- **Determine desired outcomes:** Once the use case is defined, a business should put specific metrics around it to understand how they will define success.
- **Select a tool and start small:** There are a lot of generative AI tools available, and organizations must decide which ones to adopt that will best serve the use case and deliver the desired results. From there, the tool should be given to a small group of people as proof of concept before scaling.
- **Measure, iterate, and improve:** Like any new process, things may not go smoothly the first go around. But measuring against success, understanding employee (or customer) feedback, and making adjustments along the way may help ultimately decide if this is a tool worth expanding within an organization, or scrapping altogether.

If an organization is leaning toward adopting generative AI tools, implementing employee education, and establishing company policies are crucial steps to mitigating the risks of doing so. In terms of education, businesses should consider providing company-wide training, informational sessions like webinars, office hours for questions, and consistent communications around the tool's use. Likewise, company-wide policies should be rolled out, clearly defining acceptable tools, acceptable use, data that can and cannot be used with the tool, and how violations will be handled.

The adoption of AI is dependent on a business's needs and will look different for each company. Determining what level of risk and reward is appropriate may not be a simple task, but if done correctly, it will open up the right conversations that increase security and innovation across the organization.

About the Author

Michael Gray is the Chief Technology Officer at Thrive, a leading managed security services provider. Michael has served as a strong technology leader at Thrive over the past decade, contributing to the consulting, network engineering, managed services and product development groups while continually being promoted up the ladder. Michael's technology career began at Dove Consulting and later at Praecis, a biotechnology startup that was acquired by a top-five pharmaceutical firm in 2007. Serving in his current role, he is now responsible for Thrive's R&D and technology road-mapping vision, while also heading the security and application development practices. He is a member of several partner advisory councils and participates in many local and national technology events. Michael has a degree in Business Administration from Northeastern University and he also maintains multiple technical certifications including Fortinet, Sonicwall, Microsoft, ITIL, Kaseya and maintains his Certified Information Systems Security Professional (CISSP).

Michael can be reached online at thrive@v2comms.com and at our company website https://thrivenextgen.com/

Encryption of Data at Rest: The Cybersecurity Last Line of Defense

Defending business against cyberattack

By Abimbola Ogunjinmi

Encryption of Data at Rest: The Cybersecurity Last Line of Defense

In the ever-evolving landscape of cybersecurity, where threats are becoming increasingly sophisticated and pervasive, traditional defenses alone are no longer sufficient to protect sensitive data. Despite the implementation of comprehensive security measures such as Zero Trust architectures and Defense in Depth strategies, organizations continue to experience significant security breaches. A critical vulnerability that remains is the exfiltration of data by cybercriminals. Unlike the ransomware attacks of the past that focused primarily on data encryption to demand ransom, modern adversaries now exfiltrate data, posing severe privacy and regulatory risks. In this context, encryption of data at rest emerges as the last and indispensable line of defense, rendering stolen data useless to attackers.

The Modern Threat Landscape

The shift from simply locking data to exfiltrating it marks a dangerous evolution in cyber threats. Cybercriminals today are not just interested in disrupting business operations but also in stealing valuable information. This stolen data can be used for identity theft, corporate espionage, or sold on the dark web, causing immense financial and reputational damage to organizations. In most instances, the exfiltrated data is used to compel organization to pay for ransom especially organizations operation in the industries (Health, Education) where privacy is a major requirement. Data exfiltration breaches are particularly concerning because they involve the unauthorized transfer of sensitive data from within the organization's secure environment to an external location. For example, change healthcare cyber attack of 2024 which according to United Healthcare first quarter financial statement has cost the company about USD820m(https://www.cbsnews.com/news/unitedhealth-cyberattack-change-healthcare-hack-ransomware) happened in spite of the layers of defense that exist within the organization. etc.

The Inadequacy of Traditional Defenses

Despite advancements in cybersecurity practices, breaches still occur due to various factors, including sophisticated social engineering attacks, zero-day vulnerabilities, supply chain attack, poor implementation of sophisticated defense technology and insider threats. Zero Trust, which operates on the principle of "never trust, always verify," and Defense in Depth, which layers multiple security controls, are robust frameworks. However, even these can be circumvented by determined attackers, leaving data exposed and organizations vulnerable to significant fallout.

Understanding Different States of Data:

Data can exist in three distinct states:

1. Data in Transit: This is data actively moving from one location to another, such as over a network.
2. Data at Rest: This is data stored on a physical medium, like a database server, hard drive or cloud storage, and not actively being used.
3. Data in Use: This is data currently being processed or accessed by a system.

For example, when you send an email, the message is considered data in transit. Once it reaches the recipient’s inbox, it becomes data at rest. If the recipient opens and reads the email, it turns into data in use. Eventually, all data typically returns to a resting state for storage and future access.

While there are various encryption schemes for data in transit, less has been done to encrypt data at rest. Consequently, once security defenses are breached by malicious actors, the data becomes vulnerable. Encrypting data at rest complements the cybersecurity defense system and ensures that even if bad actors manage to defeat the security mechanisms, their efforts have little effect.

The Role of Encryption in Data Protection

Encryption of data at rest involves converting sensitive data stored on physical media into an unreadable format using cryptographic algorithms. This process ensures that, even if cybercriminals manage to breach the perimeter defenses and access the storage devices, the data remains unintelligible without the decryption key. Here’s why encryption of data at rest is crucial in the current cybersecurity climate:

1. **Nullifying Data Exfiltration Risks**
   - When data is encrypted at rest, any exfiltrated data becomes useless to the attackers. Without the decryption keys, the data cannot be read or exploited, thereby mitigating the impact of the breach. This is particularly vital in preventing the misuse of sensitive information such as personal identifiable information (PII), financial records, and intellectual property.
2. **Compliance with Privacy Regulations**
   - Regulatory frameworks such as GDPR, HIPAA, and CCPA mandate strict measures for protecting sensitive data. Encryption helps organizations comply with these regulations by ensuring that stolen data remains protected, thereby avoiding hefty fines and legal consequences associated with data breaches.
3. **Maintaining Customer Trust**
   - Data breaches can severely damage an organization's reputation and erode customer trust. By implementing encryption of data at rest, companies can reassure their clients and stakeholders that they are taking all necessary steps to protect their data, even in the event of a security breach.

Implementing Effective Encryption Strategies

To maximize the effectiveness of encryption as the last line of defense, organizations must adopt a comprehensive approach:

1. **Identify and Classify Sensitive Data**
   - Conduct thorough assessments to identify which data needs to be encrypted. This typically includes PII, financial information, intellectual property, and any other sensitive business data.
2. **Select Robust Encryption Algorithms**
   - Choose industry-standard encryption algorithms such as Advanced Encryption Standard (AES) with 256-bit keys, which provide a high level of security and are widely recognized for their effectiveness. There are some encryption methods that have been deprecated and should not be used.

Below are some of the deprecated encryption algorithms that must be avoided:

DES (Data Encryption Standard):

- **Reason for Deprecation**: DES uses a 56-bit key, which is too short to provide adequate security against brute-force attacks. Modern computing power can crack DES encryption relatively quickly.

3DES (Triple DES):

- **Reason for Deprecation**: While 3DES was designed to improve the security of DES by applying the DES algorithm three times with different keys, it still has vulnerabilities and is relatively slow compared to newer algorithms. It also has a shorter effective key length and is susceptible to certain attacks.

MD5 (Message-Digest Algorithm 5):

- **Reason for Deprecation**: MD5 is a hash function rather than an encryption method, but it is included here because it is often used in contexts requiring secure hashing. MD5 is vulnerable to collision attacks, where two different inputs produce the same hash output, making it unsuitable for cryptographic security.

SHA-1 (Secure Hash Algorithm 1):

- **Reason for Deprecation**: Similar to MD5, SHA-1 is a hashing algorithm and has been found vulnerable to collision attacks. The computational feasibility of these attacks has rendered SHA-1 insecure for most cryptographic purposes.

RC4 (Rivest Cipher 4):

- **Reason for Deprecation**: RC4 has several vulnerabilities, including biases in its output that can be exploited in certain attacks. It is considered weak and is no longer recommended for use in secure communications.

3. **Employ Strong Key Management Practices**
   - Implement centralized key management systems to securely generate, store, and manage encryption keys. Ensure that access to encryption keys is tightly controlled and monitored to prevent unauthorized access.

4. **Encrypt All Storage Solutions**
   - Apply encryption across all storage mediums, including databases, file systems, and backup storage. For cloud environments, use encryption services offered by the cloud provider or deploy your own encryption solutions.

5. **Regularly Update and Audit Systems**
   - Keep encryption software, operating systems, and hardware security modules updated with the latest patches. Conduct regular audits to ensure compliance with security policies and identify potential vulnerabilities.

Overcoming Challenges

While encryption is a powerful tool, it is not without challenges. Organizations must balance the need for security with performance, as encryption can introduce processing overhead. Effective key management is also critical to avoid the risk of key loss, which could render data permanently inaccessible. However, with careful planning and implementation, these challenges can be managed effectively.

Conclusion

In the face of evolving cyber threats, encryption of data at rest stands as the last and most resilient defense against data breaches. By transforming sensitive data into an unreadable format, encryption ensures that even if cybercriminals penetrate other security layers and exfiltrate data, it remains unusable without the decryption keys. This not only protects organizations from severe privacy and regulatory repercussions but also helps maintain customer trust in a time where data security is paramount. In the cybersecurity defense lineup, encryption of data at rest is not just an option—it is an essential safeguard in safeguarding the digital fortress.

About the Author

Abimbola Ogunjinmi (MCMC, MNSE, MIEEE, mISC2, mISACA), is a distinguished leader in secure Technology infrastructure deployment. With a scholarly bias for cybersecurity and over two decades of hands-on experience in Information Technology and Telecommunication Infrastructure deployment, he has established himself as a formidable figure in the field. Beginning his career as an engineer, Abimbola has ascended to prominence through his expertise in technology infrastructure deployment. He holds a myriad of industry certifications from ISC2, PMI, Scrum, Cisco, Nokia, Alcatel-Lucent and EXIN. He earned certification such as project management professional (PMP) and Scrum product owner, Scrum Master, CCNP, CCDP, NRS, and ITIL certifications. Abimbola is a prolific contributor to both emerging and legacy technologies, including but not limited to 5G, cyber defense technologies, AI, wireless transmission, satellite communication, and Optical network systems.

Abimbola can be reached online at https://www.linkedin.com/in/abimbolaogunjinmi/

The End of the Tunnel Vision: Why Companies Are Ditching VPNs for Zero Trust

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

Virtual private networks (VPNs) have been the workhorse of secure remote access for decades. They offer a seemingly simple solution: they create a secure tunnel between a user's device and the corporate network, granting them access to internal resources.

However, as our workforces become increasingly mobile and cloud-based, companies are recognizing VPNs' limitations in this new hybrid world and seeking a more secure, user-friendly, and scalable solution.

Enter Zero Trust Network Access (ZTNA), a security model rapidly gaining traction.

According to the 2024 VPN Risk report by Cybersecurity Insiders, 98% of businesses currently use a VPN service, and 92% of users use a VPN at least once a week. However, 56% of companies are considering alternatives to traditional VPNs. Security concerns are a significant driver of this shift, along with poor user experience, with 81% of users being dissatisfied with their VPN and complex management due to 65% of organizations having three or more VPN gateways to support.

The report highlights a growing number of organizations (92%) are concerned that VPNs will jeopardize their ability to secure their environments, reflecting a clear industry-wide trend toward a more robust security posture.

Let's delve deeper into the factors driving this shift away from VPNs and towards ZTNA:

The Security Minefield of VPNs:

While VPNs offer a basic level of security, their inherent design creates vulnerabilities.

- **Wide-Open Gates:** VPNs establish a broad access tunnel into the corporate network. This unrestricted access makes it easier for unauthorized users to exploit compromised credentials or gain access by piggybacking on legitimate connections. Once they gain a valid login, hackers can infiltrate the network, potentially wreaking havoc.
- **Target-Rich Environment:** VPNs themselves can become targets for cyberattacks. Phishing campaigns aimed at stealing VPN credentials are on the rise. Additionally, vulnerabilities in VPN software can be exploited to gain unauthorized access to the network.

The Management Maze of VPNs:

As companies embrace cloud-based applications and services, managing secure access through a single VPN becomes cumbersome and complex.

- **Point-to-Point Purgatory:** Traditional VPNs require point-to-point connections between user devices and the corporate network. This becomes a logistical nightmare when managing access to a growing number of cloud applications and resources.
- **Security Stack Sprawl:** Adding additional security solutions like multi-factor authentication (MFA) to VPNs creates a complex security stack. This patchwork approach increases the risk of misconfigurations and vulnerabilities, weakening the overall security posture.
- **Administrative Overload:** Managing and maintaining multiple VPN configurations for a distributed workforce can significantly burden IT, teams. This complexity slows down onboarding times and hinders overall network agility.

The User Friction of VPNs:

The user experience with VPNs can be frustrating and hinder productivity.

- **Slow Connections and Lag:** VPN connections can introduce latency and slow down application performance, impacting user experience and productivity.
- **Compatibility Chaos:** VPNs can be incompatible with specific devices and applications, requiring troubleshooting and workarounds.
- **Constant Login Hurdles:** Users often repeatedly log in to the VPN client and corporate resources, creating unnecessary friction and disrupting workflows.

The Rise of Zero Trust: A More Secure and Streamlined Approach

Zero Trust Network Access (ZTNA) offers a compelling alternative to VPNs by adopting a "never trust, always verify" approach. Here's how ZTNA addresses the shortcomings of VPNs:

- **Granular Access Control:** ZTNA grants access based on a user's unique identity, device, location, and the specific application or resource they need. This minimizes the attack surface and reduces the potential for lateral movement within the network if a breach occurs. Even if a hacker gains access to a user's credentials, they would be limited to the specific resource they were authorized for.
- **Seamless Cloud Integration:** ZTNA integrates seamlessly with cloud-based applications, eliminating the need for complex network configurations and point-to-point connections. This simplifies IT management and reduces the overall attack surface. Users can access authorized cloud resources directly without needing to access the corporate network first.
- **Simplified User Experience:** ZTNA eliminates the need for cumbersome VPN connections. Users can access authorized resources directly with minimal friction, improving productivity and overall user experience.

The Road to Zero Trust: Challenges and Considerations

While ZTNA offers significant benefits, implementing a zero-trust architecture requires careful planning and integration with existing security tools. Here are some key considerations:

- **Planning and Integration:** A successful ZTNA deployment requires careful planning and integration with existing identity management and access control systems. This ensures a smooth user experience and minimizes disruption during the transition.
- **User Training:** Educating users on ZTNA and proper security practices is crucial for its success. Users need to understand the importance of strong passwords.

About the Author

Jaye Tillson is Field CTO & Distinguished Technologist, at HPE Aruba Networking, boasting over 25 years of invaluable expertise in successfully implementing strategic global technology programs. With a strong focus on digital transformation, Jaye has been instrumental in guiding numerous organizations through their zero-trust journey, enabling them to thrive in the ever-evolving digital landscape.

Jaye's passion lies in collaborating with enterprises, assisting them in their strategic pursuit of zero trust. He takes pride in leveraging his real-world experience to address critical issues and challenges faced by these businesses.

Beyond his professional pursuits, Jaye co-founded the SSE Forum and co-hosts its popular podcast called 'The Edge.' This platform allows him to engage with a broader audience, fostering meaningful discussions on industry trends and innovations.

Strengthening Your Cybersecurity Insurance Posture with Privileged Access Management (PAM) Solutions

By Martin Cannard, VP of Product Strategy, Netwrix

In an era where cyber threats loom larger than ever, businesses are increasingly relying on cyber insurance as a critical component of their risk management strategy. Indeed, the Netwrix 2024 Hybrid Security Trends Report found that 62% of organizations either have such a policy or plan to purchase one within the next 12 months.

However, to obtain and maintain a comprehensive cyber insurance policy, organizations must demonstrate adherence to stringent cybersecurity protocols. In the Netwrix survey, 18% of respondents said they had to make changes to their security strategy to reduce their premium — and 30% had to make improvements to their security posture to even be eligible for cybersecurity insurance at all.

Privileged Access Management (PAM) solutions are a pivotal technology in this context. In fact, 42% of organizations reported that they had to have PAM in place in order to obtain their cyber insurance policy, up from 36% in 2023.

Mitigating Insider Threats

Insider threats pose a significant risk to data security. The frequency and financial impact of insider-related incidents keep increasing, averaging an annual cost of $15.38 million, according to the 2022 Cost of Insider Threats Report by Ponemon Institute.

Accordingly, insider threat protection is a key element in cyber insurance risk assessments. PAM directly reduces this aspect of an organization's risk profile by enforcing strict access controls and providing close surveillance of privileged accounts, thereby making it more favorable in the eyes of insurers.

Facilitating Regulatory Compliance and Alignment with Cybersecurity Frameworks

Cyber insurance providers frequently mandate proof of adherence to regulatory standards like GDPR, HIPAA, and PCI DSS. These regulations demand rigorous management of access to sensitive information — an area where PAM solutions excel.

Moreover, integrating PAM into security protocols helps organizations align with cybersecurity frameworks like NIST CSF and COBIT. Insurers often view such alignment as a testament to an organization's commitment to cybersecurity because these frameworks provide best practices and key benchmarks for mitigating risk.

PAM solutions are crucial in aligning with the NIST cybersecurity framework. In this case, such solutions help organizations:

- **Identify and protect critical assets**: PAM solutions identify privileged accounts and provide robust protections to secure them.
- **Detect anomalous activity**: Through continuous monitoring and logging of privileged account activity, PAM aids in the early detection of potential security breaches.
- **Respond promptly to incidents**: PAM enables organizations to quickly restrict access to compromised accounts.

Transport and logistics service provider H. Essers provides a real-life example of how PAM assists in aligning with NIST. The company had achieved ISO 27001 certification, but they also needed to comply with the NIST framework to meet cyber insurance requirements. Netwrix Privilege Secure, a comprehensive PAM solution, enabled them to gain the strong control and monitoring they needed over vendor and contractor access to company systems through capabilities like multifactor authentication (MFA) for admin sessions and improved password management — which enabled them to secure the renewal of their cyber insurance. Plus, the solution also fulfilled their requirements for ease of use, scalability, and agility to adapt to changing cyber insurance demands. Indeed, the solution enabled the company to "avoid large-scale consultancy costs and shorten the setup process to a single day, compared to the several weeks required by other products," according to Ivar Indekeu, Senior Manager of IT Operations for H. Essers.

Demonstrating Proactive Security Measures

Cyber insurers today require organizations to proactively safeguard their IT ecosystems. Forrester Research estimates that 80% of security breaches involve privileged credentials, including certificates, keys, passwords and tokens. Dedicated PAM tools can dramatically reduce the chance of security breaches related to privileged access. The resulting overall breach reduction likelihood translates into lower risk profiles for insurance purposes. This potentially leads to more favorable insurance premiums and terms.

Conclusion

As cyber threats evolve, so does the importance of cyber insurance in an organization's risk management strategy. However, securing advantageous cyber insurance terms requires more than just basic security measures. Implementing a robust PAM solution plays a strategic role in enhancing an organization's security posture, ensuring regulatory and NIST framework compliance, and ultimately fulfilling cyber insurance requirements. All in all, PAM is not just a fundamental security tool but a strategic asset in navigating the complexities of cyber insurance procurement and maintenance.

About the Author

An accomplished VP of Product Strategy at Netwrix with a 30-year track record of success from startups to enterprise software organizations, Martin Cannard is specifically experienced in the privileged access management and identity and access management areas. Leveraging his years in the privilege space, Martin has taken a visionary approach to attack surface reduction to redefine an established PAM market with Netwrix's next-generation zero standing privilege solution. Martin is a seasoned speaker who regularly participates in global technological events and webinars.

Martin Cannard can be reached at his LinkedIn: https://www.linkedin.com/in/martincannard/ and at https://www.netwrix.com/

Making Progress and Losing Ground

By Jeff Reich, Executive Director of the Identity Defined Security Alliance (IDSA)

As an industry and a society, we are finally making progress in protecting both our digital and physical identities. The good news is that many people are now aware of Multi-Factor Authentication (MFA), understand the need for strong passwords, and have access to numerous tools that support identity security.

Think of this discussion like a well-known sandwich. We started with some positive news and, I promise, we'll end with some good news too. But let's delve into the middle part—the challenges we still face.

Ransomware continues to grow at a remarkable rate. Although we may not see as much publicity of these attacks as we once did, the scale of instances is growing. And one of the key factors is that the bad guys no longer have to write ransomware code, it's readily available as a service. The ease-of-use and availability of ransomware today is extremely concerning.

Cryptocurrency payments are estimated to have grown, with over $1 billion equivalent paid in 2023. Expand this to supply-chain attacks and that footprint becomes unmanageable. Every year, the Identity Defined Security Alliance conducts a research survey on trends in identity security.

While MFA, one-time verification codes, and hardware tokens are effective, people often suffer from authentication fatigue. Companies may be hesitant to turn on MFA to avoid increasing friction for employees and consumers. We need to focus on improving the interoperability and portability of identities, which can reduce the scope of the problem to a manageable size.

One major challenge in identity management is identity sprawl. Of the organizations we surveyed, 93% are actively taking steps to manage identity sprawl. The proliferation of cloud SaaS services has increased productivity, and it also creates a new identity or account with each service. This forces a choice between managing each of them uniquely or lowering your security profile and managing all of them in the same way. The explosion of identities costs more than we realize. Only 15% of organizations track specific metrics of cost per identity by customer or employee type and need. Unchecked identity sprawl leads to higher costs and greater security exposure.

This year an astonishing 84% of identity stakeholders said identity-related incidents directly impacted their business. The primary cost was a distraction from their core business to address the incidents. Nearly the same percentage indicated that costs to recover from an incident had a significant impact.

While we’re in the middle of the sandwich, let’s focus on the main ingredient: phishing-related attacks. These attacks account for nearly double the impact of any other incident type. We all have moments of distraction when we click on a link without thinking, and that’s when these attacks happen.

Let’s add some dressing to this sandwich and top it with the other slice of goodness. In the recent survey, 73% of respondents indicated that effectively managing and securing digital identities is among their top three priorities. This shows we’re moving in the right direction.

An impressive 97% of respondents have an incident response plan and most have had to use it more than once in the past year. While 3% is small, it’s still too many. Having a plan is crucial because although you can’t stop every attack, you can be prepared to respond effectively.

I'll leave you with two key facts. First, 93% of identity stakeholders said that security outcomes could have reduced the business impact of incidents. Even more encouraging, 99% of businesses reported they are planning to further invest in security outcomes over the next 12 months.

We are making good progress in protecting our identities. Despite challenges like identity sprawl and increasing attacks, it may feel like we are losing ground, we just need to run a little faster to stay ahead of the curve.

About Jeff Reich

Jeff Reich has been the Executive Director of the Identity Defined Security Alliance since 2023 and has been actively involved in the security and identity community for five decades. He is a well-known advocate for cybersecurity awareness and education. He joined IDSA from the Cloud Security Alliance. Before CSA, he created and built the security and risk functions at ARCO, CheckFree, Dell, and Rackspace. Jeff did the same at multiple financial services companies and five startups. He has received numerous accolades and certifications as a cybersecurity expert and industry leader, including CISSP certification from ISC2 in 1993, and the ISSA Distinguished Fellow designation in 2011. In 2015, Jeff was inducted into the ISSA Hall of Fame. Jeff can be reached online at https://www.linkedin.com/in/jreich/ and https://www.idsalliance.org/.

Black Basta Cybersecurity Advisory: Endpoint Protection for Healthcare

By Jason Mafera, Field CTO, IGEL

Recent studies have estimated that as many as 90% of successful cyberattacks and 70% of data breaches originate at the endpoint. This growing issue is especially impactful within healthcare systems nationwide. In 2023, HHS OCR disclosed a record high, 725 data breaches, exposing 133 million hospital and patient records. This incredibly alarming report was not alone in its findings, after digging deeper, the 2024 Horizon Report found that 80% of healthcare breaches came from hacking, such as malware attacks, phishing, spyware, or ransomware. Of the various forms of hacking the HIMSS Healthcare Cybersecurity Survey found that 57% of respondents reported phishing as their most significant security incident. Despite hacking ranking as the most common reason for breaches, most hospitals do not use basic credential protection and endpoint security measures to protect themselves and their patients; Black Basta picked up on this as well.

About Black Basta

Black Basta is delivered as a ransomware-as-a-service (RaaS) offering, making the barrier to entry for a potential attacker very low. RaaS vendors generally provide their customers with full technical support and make it a turn-key operation for criminal enterprises. Black Basta was first seen in the wild in April 2022 and has targeted over 500 private industry and critical infrastructure organizations, including healthcare companies, in North America, Europe and Australia. In their first few months of operation, they attacked 19 prominent enterprises and were responsible for more than 100 confirmed victims. The group uses a double extortion tactic, encrypting the victim's data and servers, as well as ransoming their sensitive data on their public leak site. While most recent hacks and attempts have targeted healthcare systems, such as Ascension Healthcare, Black Basta is also responsible for several significant hacks such as the attack on Dish Network, the American Dental Association, The Toronto Public Library system, Capita, ABB and many more.

Today, Black Basta remains at large. The group's structure has shifted, splitting off into smaller groups that can be linked through their similar attack practices and vulnerabilities. That said, there are ways to protect yourself and your organization from these threat actors.

Prevention and Protection

In response to the increasing cyber threats identified as the Black Basta group by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI) and the Department of Health and Human Services (HHS), healthcare facilities are actively searching for stronger system security. In their advisory they offered preventive options and response mitigation suggestions every organization should look into. These included:

- Backing up data regularly
- Storing data offline or off-network
- Continuously updating software and hardware as the latest security patches are released
- Using strong passwords and multi-factor authentication for all accounts and systems
- Requiring all employees to receive training on recognizing and avoiding phishing attempts
- Implementing network segmentation and access control policies to limit the exposure of sensitive data and systems
- Using antivirus software and firewalls to detect and block malicious traffic and activity
- Reporting any ransomware incidents to your local FBI field office or CISA

While all organizations are advised to utilize antivirus software, use caution with suspicious emails, educate staff about phishing and back up their data, organizations are now also advised to bulk up their protection through more proactive approaches, such as is provided by the IGEL Preventative Security Model.

This model prioritizes proactive prevention over merely reactive measures, ensuring that healthcare organizations are responsive and fortified ahead of sophisticated malware and ransomware attacks that exploit endpoint vulnerabilities. As threats like Black Basta continue to evolve, employing advanced tactics such as spear phishing and exploiting critical vulnerabilities within commonly used software, the emphasis on robust endpoint security and comprehensive threat prevention strategies has never been more important.

Security Begins at the System Level

To use preventative endpoint security, healthcare organizations require a proactive and secure operating system (OS) on all employee endpoints. A secure OS will significantly reduce the risk of an attack vector infiltrating through human error or stolen credentials.

When looking for a secure OS, ensure it will effectively minimize the attackable surface by removing the vulnerabilities at the endpoint targeted by cyber-criminals. To deliver the greatest protection, a secure OS should…

- Ensure that no local data is stored at the endpoint, which prevents the download of potentially malicious attachments or code to the endpoint.
- A read-only OS ensures malicious changes cannot be made to the OS itself.
- Deliver a secure boot process, cryptographically checking each operating system module and resetting the OS to a known secure state should tampering be detected.
- Integrate with MFA and SSO, including Microsoft EntraID, Imprivata, Okta, Ping and AuthX, to reduce the potential of stolen credential attacks while keeping clinical workflows optimal.
- Support a modular design to reduce the endpoint attack surface by only deploying the necessary software components and applications.

Utilizing a secure OS will remove a critical part of the attack chain by eliminating the endpoint as an attack vector and integrating it with MFA solutions to reduce the chances of stolen credential attacks. That said, user education will always be a critical aspect of any security planning and should not be ignored.

To truly protect our healthcare systems from threat actors like Black Basta, organizations must take a multifaceted approach, heeding the advice from CISA and investing in proactive approaches such as the IGEL Preventative Security Model.

About the Author

Jason Mafera is field CTO, North America for IGEL. He comes to IGEL with more than 20 years of experience in the delivery of cybersecurity-focused enterprise and SaaS solution offerings and has worked for a broad range of companies from start-ups and pre-IPO organizations to public and privately backed firms. Prior to joining IGEL in October 2022, Mafera served as Head of Product and then Vice President of Sales Engineering and Customer Success for Tausight, an early-stage startup and provider of healthcare software focused on delivering real-time intelligence for securing and reducing compromise of electronic Personal Health Information (ePHI) at the edge. Before that, he held a succession of leadership roles with digital identity provider Imprivata. Mafera spent 12 years at Imprivata, first defining and driving to market the OneSign Authentication Management and VDA solutions, then leading the Office of the CTO. Early on in his career, he was systems engineer and later product manager at RSA, The Security Division of EMC.

Jason Mafera can be reach through LinkedIn: https://www.linkedin.com/in/mafera/ and at https://www.igel.com/

The Evolution of Device Recognition to Attack Fraud at-Scale

By André Ferraz, Co-Founder and CEO of Incognia

Fraud prevention today is like a game of whack-a-mole. When one fraudster or attack method is stamped out, another arises to take its place. Similarly, when a fraud prevention solution makes life difficult for bad actors, they work to crack it.

In the years since device fingerprinting was established as a fraud-fighting best practice, several things have deprecated its effectiveness. To evolve, it's important to understand what has changed, why it matters, and what companies should look for to ensure they are deploying future-proof fraud prevention solutions.

Traditional device fingerprinting doesn't work well anymore

First, it is worth noting that not all device fingerprinting technologies were built for fraud prevention. A solution developed to manage users or personalize marketing for them will not withstand even the simplest tampering methods. Many companies misunderstand this and end up with a solution that gives them a false sense of security.

But even device fingerprinting solutions that are purpose-built for fraud prevention have become less effective over the last few years. The big operating systems have limited the way third-party solution providers can use device data, making it even more difficult for traditional device fingerprinting solutions to identify new and returning devices.

Fraudsters have also become increasingly sophisticated. They leverage advanced tools and tactics, like emulators, a device that enables them to tamper with apps in a synthetic environment, app cloners, and reset schemes to manipulate or disguise device attributes. For example, fraudsters will perform factory resets or reinstall apps, effectively creating a "new" device in the eyes of basic fingerprinting solutions. These “new” devices create “new” accounts that bad actors use to carry out scams at scale without detection.

At this point, fraud teams are effectively flying blind. They might see 30 new accounts when, in fact, they have all been created by the same user from the same device. Without reliable device identification capabilities, apps are significantly disadvantaged in their fight against fraud.

The advantages of a modern approach

Modern device fingerprinting solutions are purpose-built for fraud and risk management. Many of these approaches are intentionally cookieless, making them much more stable and immune to manipulation techniques like cookie theft. By focusing on high-quality data signals, not personal information, these solutions provide a much higher device recognition rate and remain privacy-centric.

Next-generation device fingerprinting solutions, like the one developed by Incognia, take a new approach to device identification. By adding new layers, like advanced tamper detection and location intelligence, modern device recognition solutions are more reliable and provide greater accuracy.

Here’s what you should look out for when evaluating device fingerprinting solutions:

1. Tamper detection: Advanced tamper detection mechanisms identify and thwart attempts to mask device identity, ensuring that even sophisticated fraud attempts are detected.

2. High device recognition rate: Modern device fingerprinting technologies are designed to persist against common fraud tactics such as factory resets, app reinstalls, and emulators or app cloners. Location intelligence adds an additional layer of security. By analyzing location patterns, unexpected relationships between devices and accounts often emerge, revealing risky behavior.

3. Built-in risk analysis: Recognizing a device as new or returning is only half the battle. How do you know if it is risky or not? Look for solutions that provide you with risk analysis so that you can take action. A solution that combines hard-coded rules and machine learning models that adapt to new fraud gives you the most comprehensive and actionable solution.

As fraud continues to evolve, so should your fraud prevention vendors. If you are using a legacy device fingerprinting vendor, there is a chance that some risky behavior is slipping through the cracks. Modern device recognition signals will help protect your bottom line and users from fraud.

About the Author

André Ferraz is the Co-Founder and CEO of Incognia, the innovator of next-generation identity solutions that enable secure and seamless digital experiences, with teams in the U.S. and Brazil. André is an expert on location technology and a strong advocate for user privacy. Originally from Brazil. André founded his first company while a university student in computer science and has Endeavor Entrepreneur and Forbes Under 30 Brazil badges. Today the location technology developed by André and his co-founders has been deployed on over 200M smartphones in over 25 countries. André can be reached online at André Ferraz on LinkedIn and at our company website https://www.incognia.com/

The Internet of Things Technological Perspective

By Milica D. Djekic

The Internet of Things (IoT) is a boom which has come with the ongoing industrial progress and revolution offering something inexpensive and suitable to everyone, but yet quite unreliable and unsecure which has triggered a novel group of the concerns in accordance with a wellbeing of those using such a gird and letting themselves be exposed to a serious threat.

Developing an IoT project is, from an engineering point of view, pretty obtainable and even communities across the globe which deal with an assembly industry might make such a technical system remaining competitive at a national, regional or even international stage. In other words, today it is possible mastering such a technology and many being in business can expect a good return of investments (ROI) if they give some money for an IoT project.

Even if some theory of the fear regarding an IoT solution is present in the world the companies' race for a profit will not be shaken as those being on the marketplace will always do anything to stay positioned in an overall competition not paying a lot of the attention to creeps coming from those who advocate safety and security, so far. The fact with the IoT technologies is they rely on a web connectivity in order to govern interconnected devices communicating with each other and as it is well-known, the internet is a critical infrastructure which provides an access to many literally getting them exposed to any kind of the high-tech operations that can affect the entire objects and their networks.

Indeed, if it is coped with a security challenge, a logical thought could be how such a risk could be avoided or mitigated giving new sorts of the requirements to engineering teams worldwide in regard to better assurance of those being the consumers of such products and services which have opened a new question and that is a transition from an unsafe to safe exploitation of the emerging technological ideas and their brainstorming pillars.

At the beginning of any project, it is important to define some initial requirements which might contribute to better quality, reliability and security of the final technological solution that should capture all inner, outer and combined challenges being part of any technical system, so far. The IoT is a paradigm that still needs to be smartly used as those inventing such a technology have been in a search for an answer to the previous engineering challenge and that has been some resources shortage across the world. In other words, at that time the humankind has looked for a response to that challenge equally trying hard to provide something economically suitable which will from a business perspective have a marketplace as cost-effectiveness with the functionality are the main demands of an optimal approach.

About a couple of decades ago, when the IoT has started it was quite obvious that for such a time a well-developed and implied Wi-Fi communication could make a great job which was the fact then, but only after a few years many have become aware that such a digital transformation has a plenty of weaknesses that could affect lives and businesses of a lot of people over the globe.

The current tendency suggests that the IoT is a well-accepted concept nowadays even if there are yet a heap of vulnerabilities with such an opportunity and apart from so with new innovations those barriers could be removed as if it is imagined that an information exchange between devices is sensitive to the hacker’s attacks certainly some of the high-tech defense techniques and tactics could be applied in order to mitigate any threat which is not anyhow annoying as a wheel of the history goes forward and even the modern technologies are just a phase of the development in an overall progress and evolution of the human beings across the planet.

Apparently, one engineering challenge is well-tackled and truly the IoT might offer a plenty of options and from such a reason it should not be excluded like that as it can additionally bring a lot of false positives as its false negatives should be assumed as some concerns being such an expected in a world of math and science and undoubtedly the clever minds which has resolved one engineering challenge will be capable to proceed with the next maybe not in an ongoing generation of the technological development, but more likely with the future collection of talents in an area of science and technology.

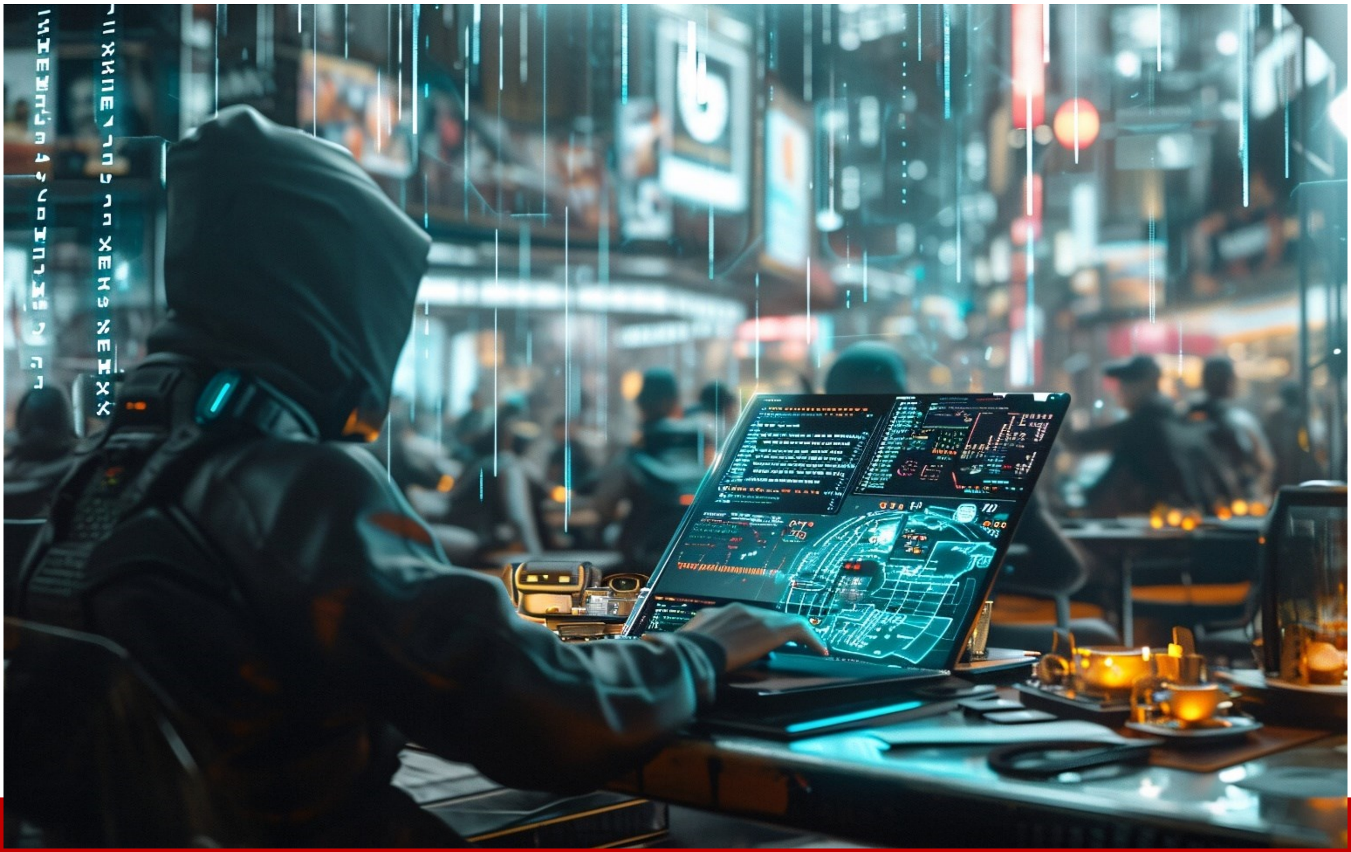
The mindful individuals throughout history have always dealt with the rational decisions providing to their environments a true knowledge and in a case of the engineering stuffs which will literally work and be based on the rigid scientific findings and evidence. Further, a real scientific thought will not hesitate to give an accuracy and those who have left a track in an arena of the math and science have always avoided all those oversufficient speculations which might destroy the beauties the human mind has created during the time as only if it is coped with the pragmatic facts some dangerous mistakes could be prevented and the world might remain in safe hands as it should be an imperative of some prospective actions.

Indeed, a typical scientist will spend a lot of time thinking hard and once all angles are observed some pieces of knowledge could be taken into consideration and despite to those who must ruin the science will always put some blocks into their right places building the world being known today and if led by ethical principles those community members will always attempt to neutralize any sort of the destruction simply thinking in a fully positive and constructive manner.

Finally, in a sense of the IoT products and services there are yet a lot of open questions which course the world will take in the future and even if there are some engineering challenges at the present those concerns will confidently be overcome tomorrow supporting the entire societies to deal with a less irrationality and put onto a fire the real ratio which will help to those making decisions and keeping directions instead of many to be wise leaders who will cope with the facts, not beliefs.

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.



Unlocking The Context Behind Bot Attacks: Protecting Your Go-To-Market Strategy

By Asaf Botovsky, CTO at CHEQ

Safeguarding your enterprise's data operations is more critical than ever. The rise of malicious bot attacks poses a particular threat, making it imperative that businesses develop a cybersecurity strategy that identifies these attacks and understands their intent. This knowledge is key to fortifying your enterprise against potential exploitation and revenue loss while protecting consumer data.

Developing a cybersecurity strategy that monitors the intent of bot attacks is the key to bolstering your enterprise's go-to-market strategy. It allows companies to evaluate changes they must make on their websites and within their data structures to better protect consumer data while avoiding exploitation and revenue loss.

The Growing Threat of Malicious Bots

As consumers become increasingly committed to digital services, the risk of hacking continues to rise. Shockingly, many studies suggest that about half of internet traffic is composed of malicious bots. Understanding the specific context behind these attacks is crucial for enterprises to take informed steps toward securing their operations.

To mitigate risk, companies must implement sign-up and lead protections that shield against form, sign-up, and application abuse. Recognizing the weaknesses within a business's strategy is essential to protect against these attacks and prevent exploitation and lost revenue.

Pinpointing the Riskiest Attacks

Understanding the context behind bot attacks involves using tools to pinpoint the riskiest attacks, allowing enterprises to prioritize their investigations. In a world with limited time and resources, cybersecurity software becomes necessary for businesses to identify the most critical context-based attacks that require further examination.

For instance, distinguishing between a credential stuffing or account takeover attack informs businesses about the risk against Personally Identifiable Information (PII). Simultaneously, identifying invalid bot activity, such as scrapers, provides a different output for protection. By leveraging these tools, enterprises can efficiently allocate resources and focus on investigating the attacks that pose the most significant risk.

The Holy Grail of Understanding Bot Intent

Understanding the intent of bots is the 'Holy Grail' for enterprises aiming to protect their data infrastructure. In a privacy-first world, implementing technology that adheres to best practices enables businesses to identify weaknesses in their go-to-market strategy. Armed with this knowledge, they can proactively fortify their defenses, ensuring robust protection against future cyberattacks.

AI algorithms, trained on historical data, can discern the subtleties in attack vectors, distinguishing between benign anomalies and malicious activities. Additionally, advanced intrusion detection systems (IDS) integrated with threat intelligence platforms provide real-time insights into the nature and motive of the attacks, whether they are financially motivated, aimed at data theft, or part of a larger, coordinated cyber espionage campaign. This context-specific understanding enables companies to fortify their defenses against current threats and anticipate and prepare for future attacks, ensuring a more resilient and proactive cybersecurity posture.

As technology advances, businesses must stay vigilant against the evolving threat landscape. Developing a comprehensive cybersecurity strategy that goes beyond mere identification to understanding the intent of bot attacks is paramount. By doing so, enterprises can safeguard their go-to-market strategy, uphold consumer trust, protect sensitive data, and mitigate the potential financial impact of cyber threats. The proactive approach of unlocking the context behind bot attacks is the key to a resilient and secure digital future for businesses.

About the Author

Asaf Botovsky is Co-Founder and CTO at CHEQ. Asaf can be reached online at (asaf.b@cheq.ai) and at our company website https://www.cheq.ai/

When CIOs and CFOs Align, Businesses Thrive

By Martin Greenfield, CEO of Quod Orbis

The C-suite drives business strategy and shapes a company's future. Communication and alignment between key players are paramount, yet silos still persist particularly between two crucial roles: the Chief Financial Officer (CFO) and the Chief Information Officer (CIO).

As the guardians of financial performance, CFOs prioritise the company's bottom line above all else. Meanwhile, CIOs are entrusted with the responsibility of achieving technological objectives to enhance operational efficiency and conveying the intricacies of digital security to the board. Historically, these two executive positions have worked side by side with minimal interaction.

However, the current business landscape necessitates a shift towards collaboration. As threats to corporate assets escalate and attack methods grow increasingly sophisticated, CIOs require advanced tools and technologies to keep pace. Yet, this demands support from the entire organisation. The challenge arises when the CFO and other board members lack awareness of the magnitude of risk, potentially leading to discord.

Shifting perceptions of cybersecurity from cost burden to strategic enabler

Traditionally, the CFO has perceived the CIO as a cost centre rather than a revenue generator. CIOs often have substantial technology budgets that can be seen as a drain on resources that could be allocated elsewhere. Consequently, CFOs have often been sceptical when CIOs request additional technology investments, especially when previous investments might not have fully resolved the problems they were meant to address.

The crux of the issue lies in the lack of effective communication between the two roles. CIOs have struggled to articulate the business case for investing in IT security infrastructure in terms that resonate with their financial counterparts. In the face of declining or stagnant budgets, it is more critical than ever for CIOs to clearly communicate the value and necessity of their technology investments to secure support of the CFO and the board.

Conversely, CFOs have historically viewed cybersecurity as an operational concern rather than a strategic imperative. They may not fully comprehend how vulnerabilities in the company's digital assets could lead to financial losses, intellectual property theft, or erosion of customer trust. There is often an underlying assumption that "it won't happen to us" until a breach occurs.

However, this perception is evolving. There is a growing recognition that digital security is an enabler and an investment that delivers genuine business value, even if its benefits are not immediately apparent on a daily basis.

In the wake of a cyberattack, not only is there a significant cost associated with investing in recovery technology, but there is also the potential impact on the brand to consider, which ultimately affects the overall financial control of the organisation.

To mitigate these risks, the CIO should be responsible for developing and executing a comprehensive IT strategy that encompasses both defensive measures, such as cybersecurity, and revenue-generating areas, including the company's website and e-commerce platforms. Although the CISO may have a direct line to the board, they will typically report to the CIO on a daily basis to ensure seamless coordination and implementation of the organisation's technology initiatives.

The more a company invests in the CIO upfront, the less the financial impact will be in the long run. Automation is a significant driver of improved efficiencies; removing manual processes helps increase engagement across teams using shared digital platforms rather than manual spreadsheets and data. The more automation the CIO can apply, the more effective they will be, and from the CFO's perspective, the more the business can get out of every single individual.

Investing in the CIO saves money in the long term – while there may be an upfront cost, this is greatly outweighed by the savings over time.

Harnessing the power of real-time analytics

To secure complete business buy-in, CIOs must be able to effectively communicate the company's digital health to the board in a manner that is easily comprehensible. However, before they can achieve this, CIOs require comprehensive visibility of the entire digital infrastructure.

The challenge lies in the fact that businesses often have a complex web of disparate tools, legacy systems, and a combination of cloud and on-premises solutions that have long hindered the ability to obtain a clear view of an organisation's operational resilience.

The traditional approach to managing business tech stacks is outdated. Companies may invest in numerous products, but they often operate in isolation, failing to communicate with each other in a meaningful way. It is crucial to understand how firewalls relate to network systems, as this level of intelligence, gained through continuous monitoring, is essential to a comprehensive security strategy.

Many regulatory compliance frameworks are incorporating the need for continuous monitoring to provide businesses with real-time data on their security posture. However, companies must elevate their security strategy beyond mere regulatory compliance; if they are investing in technology, it is essential to maximise its potential.

Continuous Controls Monitoring (CCM) emerges as a powerful solution to address this need. By seamlessly integrating with various systems and tools across the IT ecosystem, CCM offers a unified view of an organisation's digital health. It breaks down silos and enables real-time analytics that empower both the CIO and CFO to make informed decisions.

Real-time analytics provided by these tools ensures that the information is always up-to-date and never obsolete. With real-time analytics, powered by automation, the interests of the CFO and CIO align, fostering a collaborative approach to cybersecurity.

Fostering collaboration

To optimise a company's overall strategic objectives, it is crucial for CIOs and CFOs to break down the silos that have traditionally separated them. By developing a deep understanding of each other's distinct goals and priorities, they can work together to maximise the achievement of the organisation's strategic aims.

There is a significant opportunity for CIOs and CFOs to forge a close partnership, aligning technology investments with financial objectives, mitigating risks, enhancing decision-making processes and boosting overall operational efficiency. Although they play different roles within the organisation, CIOs and CFOs are ultimately part of the same team, working towards a common purpose.

About the Author

Martin Greenfield is the CEO of Continuous Controls Monitoring (CCM) provider, Quod Orbis. Martin has over two decades of experience in the cyber security space. With his team, Martin helps deliver complete cyber controls visibility for clients via a single pane of glass through Quod Orbis' CCM platform. This helps companies see and understand their security and risk posture in real time, which in turn drives their risk investment decisions at the enterprise level. Martin can be reached online via LinkedIn and at our company website https://www.quodorbis.com/

Artificial Intelligence and Cybersecurity: A New Era of Defense

Is AI a pain and hassle for Cyber professionals or can it be leveraged for better Cyber defense?

By Daniel Wilfred Chandolu aka Danny Wilfred, Principal Cybersecurity Architect, Providence St. Joseph Health

Artificial Intelligence has been a game-changer today in various fields, and cybersecurity is no exception. As cyber threats become more advanced and sophisticated, traditional methods of defense are proving to be inadequate. This is where AI can be leveraged in building innovative solutions to protect our digital assets.

The Role of AI in Cybersecurity

AI tools focussed on cybersecurity can analyse vast amounts of event data at an incredible speed, identifying patterns and anomalies that could indicate a potential cyber threat. This ability to process and analyse data is particularly useful in detecting zero-day vulnerabilities, which are unknown flaws in software that threat actors can exploit.

AI can also automate routine tasks, freeing up cybersecurity professionals to focus on more complex issues where human intervention is needed. For instance, AI can automate the process of patching vulnerabilities, reducing the window of opportunity for hackers.

AI-Powered Threat Detection

One of the most significant contributions of AI to cybersecurity is its ability to detect threats in real time. Traditional security systems often rely on signature-based detection, which can only identify known threats. In contrast, AI-powered systems use machine learning algorithms to learn from past incidents and predict future attacks, even those that have never been encountered before.

The Double-Edged Sword

While AI offers numerous benefits in cybersecurity, it's important to note that, on the flip side, the same capabilities of this technology can be exploited by cybercriminals in no time. Hackers can use AI to automate their attacks, making them more efficient and harder than ever to detect. They can also use AI to analyse cyber defense mechanisms and find new ways to bypass them.

The Future of AI in Cybersecurity

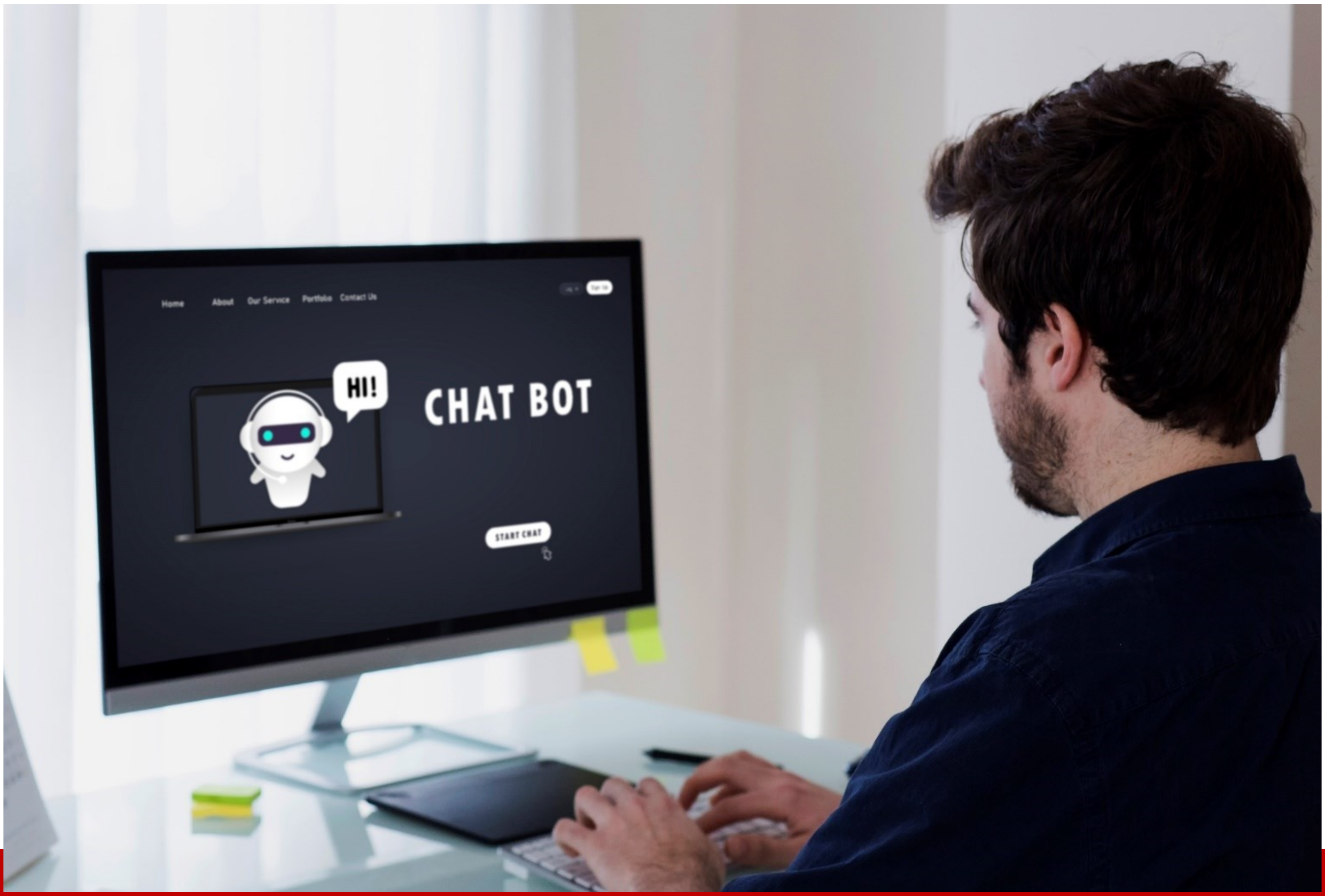
Despite the potential risks, the benefits of using AI in cybersecurity far outweigh the drawbacks. As AI technology continues to evolve, we can expect to see even more sophisticated and more robust AI-powered cybersecurity solutions. These could include autonomous systems capable of responding to threats in real time, or predictive models that can forecast cyber-attacks before they happen.

Cybersecurity is an ever-evolving landscape and AI has emerged as a powerful ally. By automating routine tasks, detecting threats in real time, and predicting future attacks, AI is and will be revolutionizing the field of cybersecurity. However, as with any technology, it's crucial to consider the potential risks and ensure that AI is used responsibly and ethically in the fight against cyber threats.

In conclusion, the integration of AI in cybersecurity signifies a new era of defense, promising a safer digital future for all. But beware, malicious actors are always a step ahead!

About the Author

Daniel Wilfred Chandolu (goes by the name Danny Wilfred mostly) is a Highly experienced IT professional with a unique blend of experience in Cybersecurity, Artificial Intelligence and multiple IT Infrastructure Technologies having served in the Defence, Healthcare & Finance domains. Currently working as a Principal Cybersecurity Architect responsible for the Information Security Strategy and Policy in Providence St. Joseph Health, USA. Main qualifications include a Masters Degree in Computer Applications, industry certifications like CISSP, CC and ISO27001 LI and an accomplished history both as a leader as well as an individual contributor in the field of IT.



Headline-Stealing Hacks Involving AI-Based Voice Chatbots & Automated MSPs

By Marc Laliberte, Director of Security Operations at at WatchGuard Technologies

Every new technology trend opens up new attack vectors for cybercriminals. With an ongoing cybersecurity skills shortage, the need for Managed Service Providers (MSPs), unified security and automated platforms to bolster cybersecurity and protect organizations from the ever-evolving threat landscape has never been more important. As we dive into 2024, the emerging threats targeting companies and individuals will be even more intense, complicated, and difficult to manage. Today, I'm sharing three 2024 cybersecurity predictions from WatchGuard's Threat Lab research team and explaining the reasoning behind them.

AI Spear Phishing Tool Sales Boom on the Dark Web

While AI/ML may still only account for a fraction of attacks, during 2024 we expect to see threat actors really begin experimenting with AI attack tools and start to sell them on the underground. We foresee a boom in the emerging market for automated spear phishing tools, or a combination of tools, on the dark web. Spear phishing is one of the most effective tactics attackers have to breach networks. However, traditionally it has also required a massive amount of manual work to research and target victims. There are already publicly available tools for sale on the underground to send spam email, automatically craft convincing, targeted text when equipped with the right prompts, and scrape the Internet and social media for a particular target's information and connections. But a lot of these tools are still manual and require attackers to target one user or group at a time. Well-formatted procedural tasks like these are perfect for automation via AI/ML. During 2024, we expect to see at least one AI/ML-based tool to help automated spear phishing show up for sale on the underground.

AI-Based Vishing Takes Off in 2024

Voice phishing (vishing) increased over 550% YoY between the first quarter of 2021 and Q1 2022. Vishing is when a scammer calls you pretending to be a reputable company or organization or even a co-worker (or someone's boss) and tries to get you to do something they can monetize, such as buying gift cards or cryptocurrency on their behalf.

The only thing holding this attack back is its reliance on human power. While VoIP and automation technology make it easy to mass dial thousands of numbers and leave messages or redirect victims unlucky enough to answer, once they've been baited to get on the line, a human scammer must take over the call to reel them in (so to speak). Many of these vishing gangs end up being large call centers in particular areas of the world, very similar to support call centers, where many employees have fresh daily scripts that they follow to socially engineer you out of your money. This reliance on human capital is one of the few things limiting the scale of vishing operations.

We predict that the combination of convincing deepfake audio and large language models (LLMs) capable of carrying on conversations with unsuspecting victims will greatly increase the scale and volume of vishing calls we see in 2024. What's more, they may not even require a human threat actor's participation.

MSPs Double Security Services via Automated Platforms

The last full-year estimate pegged the global number of unfilled cybersecurity jobs at 3.4 million, a figure that surely grew substantially in 2023. Adding fuel to the fire, cybersecurity has a burnout problem (pun intended), which is why Gartner predicts nearly 50% of cybersecurity leaders will change jobs, contributing to a “great cybersecurity resignation.” With so many unfilled cybersecurity positions, how will the average small to midmarket company protect themselves?

The answer is managed service and security service providers (MSP/MSSPs). MSPs will enjoy significant growth in their managed detection and response (MDR) and security operations center (SOC) services

IF they can build the team and infrastructure to support it. We expect the number of companies who look to outsource security to double due to both the challenging economy and difficulty in finding cybersecurity professionals. To support this spike in demand for managed security services, MSPs/MSSPs will turn to unified security platforms with heavy automation (AI/ML), to lower their cost of operations, and offset the difficulty they may also have in filling cybersecurity technician roles

As these threats potentially evolve from predictions to reality, it's essential to ensure you have the solutions and assets to protect your business and your customers. To learn what other emerging threat trends and security techniques are lurking around the corner and how you can protect against them, check out the WatchGuard Threat Lab's complete list of 2024 Cybersecurity Predictions and accompanying videos here.

About the Author

Marc Laliberte is the Director of Security Operations at WatchGuard Technologies. Marc joined the WatchGuard team in 2012 and has spent much of the last decade helping shape WatchGuard’s internal security maturation from various roles and responsibilities. Marc’s responsibilities include leading WatchGuard’s security operations center as well as the WatchGuard Threat Lab, a research-focused thought leadership team that identifies and reports on modern information security trends. With regular speaking appearances and contributions to online IT publications, Marc is a leading thought leader providing security guidance to all levels of IT personnel.

Why Legacy MFA is DOA

By Kevin Surace, Chair, Token

Multi-Factor Authentication (MFA) has long been heralded as a cornerstone of secure digital practices. However, the traditional forms of MFA, now often referred to as "legacy MFA," are increasingly seen as outdated and inadequate in the face of evolving cyber threats. This article explores why legacy MFA is considered Dead on Arrival (DOA) in today's cybersecurity landscape.

The Evolution of Cyber Threats

The cyber threat landscape has dramatically evolved over the past few years. Cybercriminals have become more sophisticated, employing advanced tactics such as phishing, social engineering, and man-in-the-middle attacks to circumvent traditional security measures. Legacy MFA, which often relies on something you know (like a password) and something you have (like a text message code or authentication app), is no longer sufficient to thwart these advanced attacks. 90% of ransomware attacks occur using user credentials, and the vast majority of those now include a legacy MFA hack as well.

The Limitations of Legacy MFA

The overriding limitation to legacy MFA is the human in the middle. A human is given a code or an app to click to verify it's them. But humans are easy to trick into doing that action (or giving the code away) to a trusted party. Not every human…but if you have 1000 employees I can get perhaps 10% to give up their code or tap an app to stop it from bugging me. But. Don't need 10%, or even 1%. I need 0.1% and I am in. Can anyone guarantee to train their employees so well that not even 0.1% would fail the test? You know the answer already.

Roger Grimes (KnowB4) famously published the 11 ways all legacy MFA is compromised by bad actors today:

1. SMS-based man-in-the-middle attacks
2. Supply chain attacks
3. Compromised MFA authentication workflow bypass
4. Pass-the-cookie attacks
5. Server-side forgeries
6. Social Engineering
7. Stolen Phones
8. Human hand-over of SMS or other codes
9. Simple SMS text duplicate receive system
10. Stolen random number seeds
11. MFA fatigue attacks

USB keys also have serious issues which compromise their effectiveness:

1. Not secure or convenient
2. Easily hacked, easily stolen, easily left at home
3. Unsure who has possession at any time
4. Fake ones exist en masse
5. USB ports are the #1 security threat from rogue memory sticks with malware to rapid data theft
6. Open USB ports are not allowed for many government computer or most secure enterprises
7. USB keys are not allowed to be used by most USGOV agencies

And finally, tokens, such as codes which change every 20 seconds still have the human in the middle who can and will share a code with a bad actor unknowingly.

Legacy MFA methods, such as SMS-based authentication, are highly susceptible to phishing attacks. Cybercriminals can easily trick users into revealing their authentication codes through fake websites or emails. Once the code is obtained, attackers can gain access to the user's account, rendering the MFA process ineffective.

Another significant vulnerability of SMS-based MFA is SIM swapping. In this type of attack, a cybercriminal convinces a mobile carrier to transfer the victim's phone number to a new SIM card. Once the transfer is complete, the attacker receives all SMS messages intended for the victim, including authentication codes. This bypasses the MFA protection entirely.

As these well-known methods demonstrate, hackers easily gain access to accounts today knowing that a user will have legacy MFA that is now all too easy to get past.

The Rise of Next generation MFA Solutions

To address the shortcomings of legacy MFA, modern MFA solutions have emerged, leveraging advanced technologies and context-aware mechanisms to provide robust security.

Biometric authentication, such as fingerprint, facial recognition, and iris scans, offers a substantially higher level of security than traditional methods. Biometrics are unique to each individual and are difficult to replicate, making it much harder for attackers to bypass. Moreover, FIDO2 biometric devices keep the human out of the picture – meaning there is no code to hand over, no second app to click.

A wearable biometric authenticator guarantees that the wearer is the actual approved user. And in the case of a social engineering hack, the user would have no code to provide since a biometric device should ideally have no user readout. Nothing to hand over to a bad actor. And wearables are convenient and easy to use.

AI generated phishing attacks and MFA fatigue attacks do not thwart next generation MFA and only reinforce the need for immediate change.

With the rise of AI generated deepfakes, we are entering a world where that person you see and hear on Zoom or Teams may or may not be your actual boss. Next generation biometric MFA will become standard issue to be sure that the people on the call ARE who they say they are, and a wearable device locked to one's fingerprint (for example) will be required to continue the conversation. Since image and voice will not be enough to guarantee identity.

The Future of MFA

The future of MFA lies in embracing these modern biometric solutions and moving away from outdated, vulnerable methods. Organizations must adopt a proactive approach to cybersecurity, implementing MFA solutions that are resilient against evolving threats. This involves not only upgrading technology but also educating users on the importance of robust authentication practices.

Next generation MFA is a critical component of the Zero Trust security model, which operates on the principle of "never trust, always verify." In a Zero Trust architecture, continuous verification is required for all users, devices, and applications, ensuring that only authorized entities can access sensitive resources. By integrating next gen MFA into a Zero Trust framework, organizations can significantly enhance their security posture.

While security is paramount, user experience should not be overlooked. Next generation MFA solutions must strike a balance between robust security and user convenience. Biometric wearable authentication is an example of technology that provides high security without compromising user experience. As these technologies continue to evolve, they will become more seamless and user-friendly.

Conclusion

Legacy MFA is indeed DOA in the face of today's sophisticated cyber threats. Every hour a major ransomware attack occurs by hacking legacy MFA. Bad actors see it no more than a minor (and fun to exploit) roadblock. The vulnerabilities inherent in traditional MFA methods necessitate a shift towards more advanced, resilient authentication solutions. By adopting next generation MFA technologies, organizations can better protect their digital assets, maintain user trust, and stay ahead of cybercriminals. The future of MFA is here, and it's time to embrace it.

About the Author

Kevin Surace is Chair of Token, delivering the next generation of multi-factor authentication that is invulnerable to social engineering, malware, and tampering for organizations where breaches, data loss, and ransomware must be prevented. He is passionate about the power of AI to revolutionize businesses and drive innovation. With a track record of success in building billion-dollar ventures, he has harnessed his expertise as a speaker, consultant, and thought leader to help companies navigate the dynamic landscape of AI-driven transformation. Kevin can be reached online at LinkedIn or X and at our company website https://www.tokenring.com/.

Best Practices for Enterprise Security

By Anurag Lal, CEO & President of NetSfere

Cyberattacks and data breaches are running rampant in enterprises, causing havoc and interrupting business operations. These nuisances are the last thing an organization wants to experience and can cause long-lasting damage to client relations, company reputation, financial standing and more. In the past 12 months more than 80% of enterprises have experienced a data breach – a new all-time high.

There is no doubt these attacks are happening thanks to advances in technology that are creating new paths for threat-actors to gain access into an enterprise's networks. In order to minimize the likelihood of experiencing an attack or breach, and to put up the best security defenses, it is recommended that enterprises follow these five best practices:

Enlist fully encrypted communications

Not all enterprises are created equal – some have robust security protections and networks while others are outdated or weak to new-age technology like AI. While 77% of companies worldwide are using or exploring the use of AI in their operations (according to McKinsey), an EY 2024 study found 78% of people reported concerning feelings over AI causing an increase in cyberattacks. The best way to protect an enterprise today is to deploy the strongest encryption standards. This will protect sensitive data while it is in transit and at rest. When information is encrypted, it is turned into cipher text that can't be read or used without a proper encryption key, rendering it completely useless to the bad actors who gain access to it. Using encryption, enterprises can ensure private information doesn't land in the hands of unauthorized users.

Eliminate data collection

In a new era where vulnerability exploitation tripled in the last year, protecting data, the one thing attackers are after, is essential. In short, hackers aren't attracted to systems that don't have data stored on them. Therefore, one of the best ways to minimize an enterprise's risk of a cyberattack is to eliminate data collection. Make sure software and applications being used throughout the organization are not collecting and storing data on network devices. Storing data on the Cloud can oftentimes be a safer route than storing data on individual devices.

Protect BYOD Practices

Following the pandemic, many enterprises adopted Bring Your Own Device practices to allow employees to work remotely. Although BYOD allows for more efficient operations, the practice lends itself to threats such as data theft, malware and lost or stolen devices. In 2022, 43% of employees experienced work-related phishing attacks on their personal devices. Therefore, it is critically important that in allowing BYOD practices, IT leaders define what corporate data and assets are permitted on a BYOD device as well as which applications and software can be used when connected to company networks. Additionally, these devices must be equipped with end-to-end encryption protections to prevent third parties from accessing data while it's transferred from one device to another.

Enforce Cybersecurity Training

A study found that 74% of data breaches involved the human element, meaning employees are often the epicenter of data breaches. The best way to mitigate this denominator is to build a strong security culture. To do this, CISOs and IT leaders should enforce regular cybersecurity training that educates employees on the latest threats facing their organization. Employees should know how to identify a potential attack, report it to leadership and what to do if they fell victim to a hack.

Remain compliant

Compliance standards and regulations are something every enterprise must abide by and there's a whole alphabet soup of different kinds of industry-specific compliance regulations to be mindful of such as HIPAA, GDPR, FINRA and JCI. As these set of standards evolve each year to adapt to the current threat landscape, enterprises have a responsibility to remain up to date with the latest compliance standards. Oftentimes, compliance violations occur following the sharing of unauthorized information on unsecure messaging platforms. These violations could be detrimental to a company's financial status, client relationships and reputation.

These days, business leaders are aware of the growing frequency of data breaches and cyberattacks and are concerned that they aren't prepared enough to handle such situations. It is a team effort to secure an entire organization but with these kinds of practices and defenses in place, the risk should be extremely less.

About the Author

Anurag Lal is the President and CEO of NetSfere. With more than 25 years of experience in technology, cybersecurity, ransomware, broadband and mobile security services, Anurag leads a team of talented innovators who are creating secure and trusted enterprise-grade workplace communication technology to equip the enterprise with world-class secure communication solutions. Lal is an expert on global cybersecurity innovations, policies, and risks.

Previously Lal was appointed by the Obama administration to serve as Director of the U.S. National Broadband Task Force. His resume includes time at Meru, iPass, British Telecom and Sprint in leadership positions. Lal has received various industry accolades including recognition by the Wireless Broadband Industry Alliance in the U.K. Lal holds a B.A. in Economics from Delhi University and is based in Washington, D.C. Anurag can be reached online at @anuragl and https://www.netsfere.com/.

Cyber Threats vs. Risks: Building a Proactive Cyber Defense

By George Jones, Chief Information Security Officer at Critical Start

As cybersecurity threats continue to evolve in the ever-changing cyber landscape, organizations within every industry must implement a comprehensive security strategy to remain resilient in the face of attacks. While most security teams are focused on patching potential threats, lingering risks within organizations are leaving them vulnerable to attacks. Understanding the differences between cyber threats and cyber risks is crucial when building a proactive and reactive cyber defense strategy. In fact, if left unseen and unresolved, risks can result in data breaches or major operational disruptions. According to IBM's 2023 Cost of a Data Breach Report, the average cost of a data breach reached $4.5 million.

Additionally, security leaders must also stay informed on current trends and evolving developments such as generative AI that pose unique security risks and educate team members on how to safely navigate these tools. This article will uncover the important differences between cyber threats and risks, going beyond reactive to proactive measures, emerging cyber trends, and building a future-ready security culture to help safeguard organizations in today's digital age.

Distinguishing Between Threats And Risks

Cyber threats differ from risks in that they are generally related to the actors or actions that exploit vulnerabilities. Threats are multifaceted and can be located inside or outside an organization, intentional or unintentional, and executed by either a cybercriminal or internal employee. For example, an attacker might deploy malware through an organization’s vulnerable endpoints to try and breach the network. Alternatively, an employee might unknowingly release sensitive information or change security settings, creating an attack vector in the system.

Cyber risks refer to underlying weak spots located within the ecosystem of an organization which encompass network infrastructures, human factors and physical locations. These risks may be known or unknown to the security team. Often, when proactive risk strategies are in place, risks can be meticulously evaluated for their probability and the extent of their potential damage, painting a vivid picture of the organization's vulnerability landscape. Once these risks are assessed, decisions around whether to accept these risks based on the knowledge of the ease at which they can be mediated or remediated can be made. As threats and risks continue to advance, it is crucial for businesses to understand the difference between the two and develop security strategies accordingly.

Obstacles in Cyber Risk Assessment and Threat Response

One of the primary challenges in cybersecurity is distinguishing between risk assessment and threat response. On the risk side, cyber risk evaluation is more complex and labor-intensive, as it involves identifying potential vulnerabilities, assessing their likelihood and impact, and prioritizing them based on the organization’s risk appetite. It is a process that requires significant human effort and expertise, making it more challenging than automated threat response for example. In addition, quantifying these risks to communicate effectively with stakeholders, particularly at the executive level, adds another layer of complexity. In order to mitigate risks appropriately, organizations must present a clear cost-benefit analysis, illustrating how mitigating certain risks aligns with the company’s strategic goals and overall mission.

On the threat response front, responding to threats is often more straightforward because many organizations have established platforms and protocols to manage threat responses automatically. These systems, such as endpoint protection or firewalls, are designed to detect and neutralize threats in real-time.

Lastly, it is vital to establish a security-conscious culture within the organization in order to strike the right balance between proactive and reactive cybersecurity strategies. This involves educating team members at all levels the value of cybersecurity, as well as providing them with the appropriate tools to spot threats and identify risks so they are able to take appropriate action. Ultimately, this will improve cybersecurity posture by creating a culture where everyone takes responsibility for security. After all, businesses are only as strong as the weakest link. Providing all employees with the proper knowledge and tools to identify and quickly respond to risks is a crucial step to building a proactive cyber defense.

Identifying Emerging Cyber Risks

In the fast-paced cybersecurity landscape, organizations must also be well-educated on emerging cyber trends and associated risks their organizations may be susceptible to. The development of generative AI technology presents new risks and data privacy concerns that companies of all sizes and all industries must proactively address. For example, cybercriminals are increasingly using phishing campaigns and deepfakes to target vulnerable employees and gain access to a company's system and steal sensitive data.

Organizations must quickly harness generative AI before threat actors can use it to their advantage. Navigating these developments necessitates the formulation of comprehensive policies and diligent education initiatives to ensure safe and responsible utilization of AI tools.

Security leaders should create an acceptable use policy for AI within the organization and communicate to all levels of the organization. If employees are not properly guided on how to use AI tools, there is a risk of losing control over the organization's data and creating an insider threat or a vulnerability for bad actors to exploit. Establishing clear guidelines and guardrails ensures that employees can use AI productively while maintaining data security.

Organizations must embrace a proactive security approach that includes risk and threat management in order to transcend reactive tactics. The ability to adjust and take preventative action will be essential to resilience in the face of a future potential cyber-attack. Those that fail to prioritize both risk assessment and threat mitigation will fall behind in the rapidly evolving digital world.

About the Author

George Jones, Chief Information Officer, Critical Start: In his role as the CISO, George defines and drives the strategic direction of corporate IT, information security and compliance initiatives for the Critical Start, while ensuring adherence and delivery to the firm's massive growth plans. George was most recently the Head of Information Security and Infrastructure at Catalyst Health Group, responsible for all compliance efforts (NIST, PCI, HITRUST, SOC2) as well as vendor management for security-based programs. George brings more than 20 years of experience with technology, infrastructure, compliance, and assessment in multiple roles across different business verticals. Recently as Chief Information Officer and Founder of J-II Consulting Group, a security & compliance consultancy, George was responsible for the design and implementation of security and compliance programs for various organizations. He also delivered programs to implement Agile methodologies, DevSecOps programs, and Information Security Policy and Procedure Plans. During his time at Atlas Technical Consultants, George drove multiple M&A due diligence and integration efforts, consolidating nine acquired business units into a single operating entity, enabling the organization to leverage greater economies of scale and more efficient operations.

George grew up in Austin and is a recent transplant to the Plano area. He attended Texas A&M University and graduated Magna Cum Laude from St. Edward's University.

AI in Cybersecurity: Understanding Challenges, Opportunities and New Approaches

By Matthew Pines, Director of Intelligence, PinnacleOne

Artificial intelligence (AI) has rapidly reshaped the cybersecurity landscape and simultaneously presents both exciting advancements while also introducing new challenges. As AI's role in the tactics of both cyber attackers and defenders develops and becomes increasingly sophisticated, organizations must evolve alongside this shift, and create effective strategies that protect their assets and remain competitive. Cyber defenders must develop strategies that hone agility, proactivity, and iteration.

The Impact of AI on Cyber Threats and Defenses

AI has gained notoriety as a mixed blessing in cybersecurity. It indisputably offers significant benefits; it enhances security by recognising patterns, providing real-time monitoring, predicting threats, and streamlining threat detection processes. On the other hand, malicious actors, from state-sponsored groups to opportunistic hackers, are using AI to speed up their operations, improve their capabilities, refine their tactics, techniques, and procedures (TTPs), and carry out more sophisticated attacks.

In working to defend against these evolving threats, the cybersecurity industry is leveraging AI to develop advanced defensive strategies. AI maximizes security team's efforts, empowering them to keep pace with the ever-increasing volume and complexity of cyber attacks.

AI-Powered Cyber Defense

As security challenges become increasingly data-driven, traditional approaches to threat detection and response are proving insufficient. Security analysts often find themselves overwhelmed by the sheer volume of alerts and the complexity of the threat landscape, leading to alert fatigue and delayed response times.

Owing to an overwhelming number of alerts, coupled with the increasingly complex threat landscape, security analysts are experiencing higher levels of alert fatigue and slower response times.

One solution, becoming increasingly common in AI-powered cyber defense solutions, is the optimization of generative models and natural language processing. These technologies allow for analysts to interact with, and utilize data from threat intelligence and security data, with precise intuition.

By integrating AI into cyber defense solutions at a local level, threat hunting and response tactics become increasingly democratized, and empower even junior security teams to quickly detect and mitigate advanced threats that would previously have required insight from more experienced analysts. By leveling the playing field, organizations can regain autonomy when defending against sophisticated cyber adversaries, equipping them with the tools for an increased speedy and accurate response.

Managing AI's Cybersecurity Risks and Challenges

AI has the potential to significantly enhance cybersecurity, but deploying it across diverse enterprise applications introduces new risks and challenges that organizations must address. Managing these AI-related risks effectively requires a comprehensive strategy that covers regulatory compliance, technology and security protocols, data privacy, reputation management, legal issues, and operational resilience.

Ensuring AI safety and security extends beyond traditional information security measures. It demands a wider assessment that includes evaluating model fairness, bias, harmful content, and potential misuse. Security strategies must not only anticipate malicious tactics but also address unintended consequences of AI systems, such as inadvertent data leakage or improper usage by everyday users.

As AI systems evolve to greater autonomy and capability, it has become an imperative for organizations to establish stringent controls and governance frameworks for their responsible development and deployment. The geopolitical implications of AI in cybersecurity are significant, as nation-states vie for strategic advantage in this domain. Across the globe, new frameworks are being introduced to regulate

AI and ensure its ethical application. Organizations must stay vigilant in their compliance with these evolving regulations.

Adopting AI-powered solutions that prioritize transparency, adaptability, safety, and comprehensiveness empowers organizations to proactively combat evolving cyber threats. Achieving a balance between innovation and risk management demands ongoing collaboration, flexibility, and a dedication to ethical AI practices. Cultivating a culture of continuous learning, collaboration, and responsible innovation enables organizations to effectively navigate the complexities of AI in cybersecurity, fostering a more secure and resilient future.

About the Author

Matthew Pines, Director of Intelligence, PinnacleOne. Matthew Pines is the Director of Intelligence at PinnacleOne (SentinelOne's Strategic Advisory Group), where he leads analysis of how geopolitics, emerging technology, and cyber threats are shifting the risk landscape facing global enterprises. He also leads PinnacleOne's strategic intelligence advisory engagements to help executives understand and adapt to global change. Matt was previously the Director of Security Intelligence at the Krebs Stamos Group. Prior to joining KSG, he spent over ten years consulting for the government and the private sector on national preparedness, federal cybersecurity, and emerging technology challenges. He has designed and led operational experiments, exercises, and strategic assessments of critical programs relating to national continuity, emergency response, science and technology, and cybersecurity to drive risk-informed policy and acquisition decisions. He holds a M.Sc. in Philosophy and Public Policy from the London School of Economics and a B.A. in Physics and Philosophy from Johns Hopkins University. Matt can be found on X and at our company website, SentinelOne.

GDPR & CCPA: A CIO's Essential Guide to Email Compliance

From Regulations to Action, Implementing a Secure Email Strategy

By Shanky Gupta, Managing Director, yourDMARC

Imagine a world where your inbox isn't a monster overflowing with junk. A world where you can be confident your emails are safe and secure. That's the power of email compliance!

Think of compliance as a set of super-simple instructions - a secret handshake with the email world. It ensures your messages are safe and legal, and keeps everyone's privacy under wraps.

No more inbox monsters! With email compliance, you're sending and receiving messages like a superhero, confident your information is protected and your emails reach the right people.

Here's why email compliance is a super important tool for any business:

- **Avoid Big Fines:** Following the rules keeps your wallet happy and your company's reputation sparkling clean.

- **Become Your Customer's Email BFF:** Everyone wants their information kept safe. You build rock-solid trust with your customers when you show you care about privacy. ✌️
- **Future-Proof Your Inbox:** New privacy laws are like sneaky ninjas, popping up all the time. But with email compliance as your shield, you're always ready for whatever comes next!

Now, let's meet two important players in the data privacy game: GDPR (General Data Protection Regulation) and CCPA (California Consumer Privacy Act). These are like the rulebooks for how businesses handle personal information, including the stuff in your emails. We'll crack open these rulebooks (GDPR and CCPA) and see how they impact the way you send and receive emails. Get ready for some easy-to-understand info that will make you a master of email compliance! So, grab your tools and get ready to tame the inbox monster – let's make your emails safe, legal, and stress-free!

GDPR & CCPA Got You Confused? Let's Clear It Up!

Sending emails seems easy, but with GDPR and CCPA rules around, things can get confusing. We'll break it down below into simple terms for you!

1. Imagine GDPR and CCPA as **email safety manuals**. They say businesses should only collect the information they **need** (like a name for an order), not extra stuff. That's where **CISOs** (think email security chiefs) come in - they make sure emails follow these rules!
2. Next, picture asking someone before sending them a text. That's kind of like **consent** under these rules. CISOs need a clear way to get a **"yes"** from people before sending emails.
3. Imagine a high-tech vault for your emails - that's **data security**. These rules say companies need strong measures like encryption (fancy code) to keep bad guys out.
4. Finally, think of these rules as giving people control over their information. They can see it, fix it, or even erase it if they want. CISOs need to make sure it's easy for people to do this with their email info.

We'll show you more easy ways to follow these rules and keep your emails safe and legal!

Best Practices for CISOs

To enhance GDPR and CCPA compliance in email communication, CISOs should consider implementing the following best practices:

1. **Encryption Shield:** Imagine wrapping your emails in an unbreakable shield. Encryption protects sensitive information during transit, keeping bad guys out.
2. **Data Retention Time Machine**: Set clear rules for how long you store email data. Think of it like a time machine - after a set period, information gets "deleted" from the past!

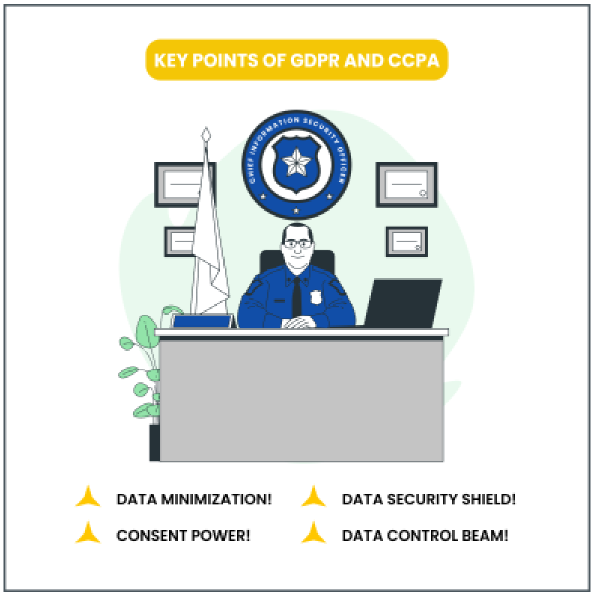
3. **Compliance Audit Patrol:** Regularly check your email systems for any weak spots. Think of it as a security patrol, ensuring everything is shipshape.
4. **Employee Training Bootcamp:** Empower your employees with email compliance knowledge. Train them on GDPR and CCPA rules, making them data privacy champions.
5. **Compliance Monitoring Watchtower:** Use tools to keep an eye on your email communication. These tools act like a watchtower, flagging any potential compliance issues.
6. **Data Breach Response Battle Plan:** Be prepared for the unexpected! Develop a plan to handle data breaches, including notifying everyone affected and minimizing the damage.

Preparing for Future Regulations

The world of data privacy is like a game of whack-a-mole – just when you think you've got all the rules down, another regulation pops up! That's why CISOS must be like ninjas – always aware of their surroundings and ready to adapt.

Here's the deal: new laws and tweaks to existing ones can throw a wrench into your email compliance plans. But fear not! Staying on top of these legislative changes, it's like having a cheat sheet for the game. There are even online communities, like industry forums, where CISOs can chat and share intel about upcoming challenges.

The real win here is being proactive. By updating your company's policies and procedures before new rules hit, you're showing everyone you take data privacy seriously. Not only does this keep your company out of hot water, but it also positions you as a leader in the data privacy game – pretty cool, right?



Conclusion

So, how do CISOs keep email communication safe and legal with all these data privacy rules? It's all about working together! Everyone in the company needs to understand the rules, use the right tech tools, and be committed to keeping everyone's information private. By focusing on keeping data safe, getting clear permission to use email, and following best practices, CISOs can protect people's privacy and avoid any trouble. For a complimentary compliance consultation, get in touch with weDMARC.

About the Author

Shanky Gupta is the Director and CEO of yourDMARC. He leads the charge in delivering top-tier email compliance services. With over 14 years in the tech industry, Shanky has a talent for innovation and a passion for client satisfaction. He has guided yourDMARC to become a recognized leader in email compliance, thanks to his expertise in operations management, marketing, team leadership, and industry research.

Shanky Gupta can be reached online at contact@yourdmarc.com and at our company website https://yourdmarc.com/

Spotlight on Oleria

By Dan K. Anderson vCISO and On-Call Roving Reporter, CyberDefense Magazine

Q&A with Oleria CEO Jim Alkove:

Identity is the keystone to the future of cybersecurity and a critical area for companies to focus on because it's where attackers are moving. Today 80% of all breaches involve compromised identities. Abusing valid accounts is also cybercriminals' most common entry point.

Essentially, attackers are no longer just hacking in – they're logging in. And they are doing so because identity security is one of the most challenging and under-funded areas of cybersecurity, leveraging legacy systems that can't keep up with today's modern cloud- and SaaS- centric organizations.

Even with a large budget and security team, it was difficult for me as a CISO to answer the questions of who has access to what, how that access was obtained, and how it's being utilized. This gap is one of the biggest weaknesses facing organizations today, so it's no wonder that bad actors have chosen to focus here. Security teams are challenged by the lack of access visibility and control due to the limitations of legacy Identity and Access Management (IAM) systems which rely on manual, costly and time-intensive workflows.

Oleria solves for this problem by providing enterprises with adaptive and autonomous identity security. Our product, Oleria Adaptive Security, provides first-of-its-kind fine-grained access visibility and access usage at an individual resource level – allowing CISOs and their teams to finally answer the critical questions: Who has access to what? How did they get it? What are they doing with it?

Oleria fills a critical gap for security teams by bringing together organization-wide access into a comprehensive access graph powered by the Oleria TrustFusion Platform. Our adaptive solution enables organizations to ensure that users have the right access at the right time only as long as they need it, so organizations can reduce risk, ensure compliance and reduce the cost of managing access.

Cybercrime statistics on the problem you solve:

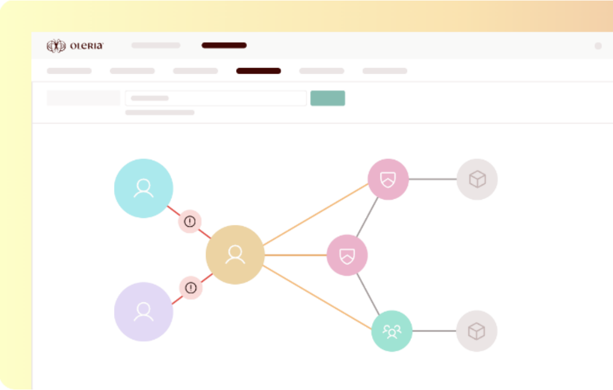
In the past year, we have seen a 71% increase in identity-related attacks. Incidents with Midnight Blizzard, Snowflake, SEC and Mandiant, all stemmed from issues with MFA coverage gaps. With the rise of AI and decentralized SaaS applications, the volume of cyber-attacks continues to increase, costing U.S. companies an average of $9.48 million per breach.

Despite this, the majority of organizations (66%) are not investing enough in IAM according to Gartner. This is particularly alarming when you consider that 80% of all breaches today use compromised identities.

The reality is today most CISOs and security teams are not equipped to deal with identity access related security threats – with many leveraging legacy security solutions that require manual, costly and time-intensive work flows. At the same time Microsoft reports that 95% of access goes unused. While this over-provisioned access provides no real value to the organization or the user, it provides an unnecessarily large attack surface for a bad actor that accesses any such account.

Oleria Adaptive Security product solves this problem for security teams by giving full clarity and control of access in a single view with unparalleled insights.

Dashboard:



CEO and Customer quote:

“Oleria was created by security operators for operators to propel identity security forward, eliminating the restrictive limitations of legacy IAM technology and their related manual intensive processes,” said Jim Alkove, co-founder and CEO of Oleria. “We’ve built the first adaptive identity security product to provide visibility to both centrally provisioned and de-centrally provisioned access, as well as fine-grained individual permissions and usage insights.”

“We began seeing value quickly after implementing Oleria Adaptive Security. I was impressed by the comprehensive visibility we had into our access, including over-provisioned accounts, unintended access, and our coverage of multi-factor authentication. Oleria’s simple user-friendly experience gave us both clarity and direction on where to focus our efforts and the tools to easily detect access issues.” - Mark Carter, CIO and CISO of Vimeo

Elevator pitch:

Today's identity technologies are holding businesses back. We started Oleria because we believe enterprises shouldn't have to choose between business agility and security.

Today’s approaches fail to reduce the significant security risks caused by over-provisioned and misconfigured access, while costing us all the fortune to manage access using multiple tools and enormous human effort.

At Oleria, we're building a solution in the cloud to get all your access in one place adaptively and autonomously. Oleria Adaptive Security provides first-of-its-kind access visibility across centrally and de-centrally managed applications and into access usage across all resources – allowing CISOs and their teams to finally answer the critical questions: Who has access to what? Where did they get it? How are they using it?

What does Gartner say about you? Why?

Gartner analysts have been actively engaged with Oleria, but nothing has yet been published about Oleria. We anticipate some exciting news on this front later this year.

Who are your competitors?

Oleria’s biggest competitor today is the status quo. While the issues we are solving have been painful and persistent for years, no one has yet been able to deliver a solution. So, CISOs and their teams spend countless hours and resources trying to combat the ever-growing threat of access-related cyber breaches leveraging a combination of legacy identity and access management systems coupled with significant manual administration and intervention and are not equipped for today’s threat environment.

Why is your solution better?

Oleria empowers CISOs and security teams by providing one place in the cloud to manage all of your access adaptively and autonomously. By adaptive, we mean that every account should have just the access that it needs at the right time for the right duration. By autonomous, we mean intelligent software managing access rather than humans clicking through automated workflows.

To achieve this, we deliver three things: visibility, insights and action.

Visibility: Oleria brings all of your access and usage information into a universal access graph so that you can understand who has access to what, how they got it, and what they're doing with it.

Insights: Once you have all of your access in one place, Oleria empowers your identity, incident response and compliance engineers with unparalleled insights, helping them explore your access graph, investigate access related incidents and identify unused or unintended access. Oleria makes intelligent recommendations to remediate access including removal of unused access without negatively impacting your business operations.

Action: Finally, CISOs and security teams are looking for a partner to help them fix problems accurately and quickly. Through action, Oleria provides a single control point for autonomously remediating access risks and managing access independent of applications.

How does your solution fit into a company's Cyber stack? What does it pair well with?

Oleria's adaptive and autonomous identity security solution seamlessly integrates into a company's cybersecurity stack providing one place to manage access across all cloud applications, identity and HR systems. Oleria brings all of your access and usage information into a universal access graph allowing CISOs and security teams to understand who has access to what, how they got it, and what they're doing with it.

Most organizations today have blind spots when it comes to de-centrally managed access and access usage. With Oleria, companies have complete visibility into all access types: centrally managed access (managed through identity providers like Okta or AD), de-centrally managed access, which is managed directly in applications or infrastructure, and fine-grained access control at the resource level.

By delivering a composite view of identity and access, Oleria empowers CISOs and security teams to identify and remediate over-provisioned or misconfigured access, significantly reducing security risks.

How are you funded?

Oleria has raised over $40 million from key investors including Evolution Equity Partners, Salesforce Ventures, Tapestry VC and Zscaler, and several notable individual investors including Assaf Rappaport, CEO, Wiz and Microsoft COO Kevin Turner.

How do you keep your Key Developers around?

Oleria retains its key developers by fostering a culture of trust and innovation. Our dev team is inspired by our mission and aligned to our values – which we created before a single line of code was ever written. We believe in creating a world where every organization is trusted to protect the data of all people. Oleria offers competitive compensation packages, professional development opportunities, and a collaborative environment that values input and creativity.

Oleria was also recently named a Built In Best Place to Work and Best Startup to Work For in Seattle. We believe in diversity and empowering our team. We are fostering a culture that empowers Olerians to do the best work of their careers. We emphasize work-life balance and provide incentives for long-term commitment, ensuring our developers feel valued and motivated.

Tell me about a customer who implemented your solution and what metrics show they are happy with the solution.

Oleria is quickly building momentum with partners and onboarding enterprise and Fortune 500 customers onto our Trustfusion Platform. Vimeo is one of our early customers. Below is a quote from Vimeo CISO Mark Carter on the impact Oleria has made for his team:

"We began seeing value quickly after implementing Oleria Adaptive Security. I was impressed by the comprehensive visibility we had into our access, including over-provisioned accounts, unintended access, and our coverage of multi-factor authentication. Oleria's simple user-friendly experience gave us both clarity and direction on where to focus our efforts and the tools to easily detect access issues." - Mark Carter, CIO and CISO of Vimeo

What is your 3-year product roadmap?

Oleria is building a solution in the cloud to control all of your access in one place, adaptively and autonomously. By adaptive, we mean that every account should have just the access that it needs at the right time for the right duration. By autonomous, we mean intelligent software managing access rather than humans clicking through automated workflows.

Oleria's TrustFusion platform and product roadmap spans identity and access governance, as well as identity security posture management and identity threat detection and response.

About the Author

Dan K. Anderson Bio, Winner Top Global CISO of the year 2023. Dan currently serves as a vCISO and On-Call Roving reporter for CyberDefense Magazine. BSEE, MS Computer Science, MBA Entrepreneurial focus, CISA, CRISC, CBCLA, C|EH, PCIP, and ITIL v3.

Dan's work includes consulting premier teaching hospitals such as Stanford Medical Center, Harvard's Boston Children's Hospital, University of Utah Hospital, and large Integrated Delivery Networks such as Sutter Health, Catholic Healthcare West, Kaiser Permanente, Veteran's Health Administration, Intermountain Healthcare and Banner Health.

Dan has served in positions as President, CEO, CIO, CISO, CTO, and Director, is currently CEO and Co-Founder of Mark V Security, and Cyber Advisor Board member for Graphite Health.

Dan is a USA Hockey level 5 Master Coach. Current volunteering by building the future of Cyber Security professionals through University Board work, the local hacking scene, and mentoring students, co-workers, and CISO's.

Dan lives in Littleton, Colorado and Salt Lake City, Utah

linkedin.com/in/dankanderson

Tips for Detecting and Preventing Multi-Channel Impersonation Attacks

The use of AI to defend deepfakes and scammers is becoming a business imperative

By Abhilash Garimella, Head of Research at Bolster

Recently, the CEO of the world's biggest advertising group, Mark Read, was the target of a deepfake scam using an AI-based voice clone. Read disclosed that scammers used a publicly available photo to create a fake WhatsApp account under his name, and that account was used to arrange a Microsoft Teams call between one of his agency heads, a senior executive, and the scammers. Once inside the Teams meeting, a voice clone with YouTube footage of the other executive was used, while the scammers impersonated him off-camera using the chat function.

While the scam was unsuccessful this time, deepfakes and impersonation attempts are becoming increasingly common and sophisticated, according to the Identity Theft Resource Center. Unfortunately, this example is among the most common applications of deepfakes, along with fraudulent videos of celebrities, politicians, or other public figures, that can spread misinformation, damage reputations, or incite conflicts.

In these instances, expertise becomes crucial in swiftly identifying and mitigating the threat. Deepening your understanding of the imposters and deploying effective countermeasures is imperative for maintaining a company's integrity in the digital landscape. Recognizing fraud and responding effectively to deceitful accounts is critical in shielding executives from harm and protecting the organization from potential reputational and financial repercussions.

As technology evolves and improves, detecting deepfakes will become increasingly difficult. But there is hope on the horizon, as AI can also be used for good, to build up defensive postures, and assist in flagging scams before they become problems. Keep reading to learn more about outsmarting the scammers.

Unmasked: Recognizing scammers to stop being victimized

The best way for executives to avoid becoming victims is to detect threats before they cause financial or data loss and damage. The incident mentioned earlier underscores just how simple and easy it is for attackers to set up fake profiles on multiple channels, including LinkedIn, Telegram, WhatsApp, and social media platforms, to establish legitimacy before contacting unsuspecting employees or partners to carry out their scam.

These impersonators build detailed profiles using publicly available information, including real photos of individuals and personal details, even mimicking their unique speaking style and tone, all lending greater legitimacy. Therefore, protecting against fake accounts and social media impersonation requires a multi-faceted approach, beyond just enforcing unique passwords.

The first step in defending against impersonation attacks is recognizing a fraudulent profile. Through close examination, impersonation accounts can display subtle, but telling anomalies compared to authentic profiles. For example, profile pictures may look generic, stock-like, or unnatural; bios may be too vague or oddly formal for social media; and often, account creation dates appear very recent. These clues will often give away imposter profiles, which are engineered for malicious activities, like phishing scams, installing malware, and orchestrating broader cyberattacks. Train employees to create a routine of scrutinizing profiles for completeness and authenticity. Encourage them to explore the digital footprint of suspicious accounts and cross-reference what they find with other public information where possible. Genuine accounts usually have a consistent history of posts and interactions, unlike fake accounts which may show minimal activity.

Secondly, it is much more difficult to fake your personal and professional connections. It is reasonable to expect that an accomplished executive will have a long list of contacts, current and former associates, customers, and friends following their profiles. So, examine followers and friends or connections lists to identify potential imbalances in the ratio of followers to following. Fake accounts will often follow many but conversely are only followed by a few. Such accounts may also follow a pattern of targeting high-profile or similar accounts disproportionately. You can also use analytics tools to assess the ratio of followers to following, and these tools can help visualize patterns to quickly flag accounts that deviate from the norm, especially those that target high-profile figures disproportionately.

Look and Listen: Using patterns and behaviors to spot scams

Moving beyond social connections, it’s important to scrutinize a profile’s content for authenticity. This involves evaluating the relevance and quality of what the user has posted. Imposter accounts might share spammy or irrelevant material that is often filled with suspicious links or promotional content that doesn’t align with the genuine persona or identity of the account. To defend against this threat, you can set alerts for keywords associated with spammy or promotional content within your network. This proactive measure will help to quickly identify and investigate accounts that are frequently using such terms inappropriately.

Once you have sorted out any red flags due to content, the next step is to employ social listening tools to track and analyze the profile’s engagement patterns over time. Look for anomalies such as sudden spikes in likes, comments, or shares, which could all indicate the use of automation or coordinated inauthentic behavior. Fake accounts will typically display abnormal engagement patterns aimed at fabricating authenticity. Monitoring these patterns can help identify and flag imposters.

Finally, utilizing third-party tools that use algorithms and machine learning to continuously monitor and analyze account behavior can significantly aid in detecting and efficiently blocking fake accounts. Using research and reputable third-party services that offer comprehensive monitoring and analysis features can ensure integration with existing security systems for seamless detection and response to fake accounts.

Automate: Strengthen cyber defenses to mitigate threats

The threat of imposter accounts on social media is real and ever evolving. To counter these attacks at scale, leveraging AI and machine learning can also be a powerful defense mechanism to proactively detect and remediate threats. Additionally, adopting the above strategies can protect organizations, their employees, and their online communities from the costly consequences of these fraudulent entities.

Sometimes, you can further insulate the organization from threats by building strong associations with reputable security thought leaders and communities. Build your awareness of the latest trends and tactics employed by malicious actors by subscribing to cybersecurity newsletters, or through participation in webinars and workshops to update your knowledge and skills, so you can recognize emerging threats built on impersonation schemes.

About the Author

Abhilash Garimella is the Head of Research at Bolster AI where he leads both the threat intelligence and SOC team to detect and take down digital threats. Abhilash has a master's in computer engineering and deep learning, and his work covers cybersecurity, online fraud detection, threat hunting, and applied machine learning. Prior to Bolster, Abhilash conducted threat research at McAfee and was the original scientist at Bolster in developing models for automated threat detection and response. Follow Abhilash on LinkedIn and at Bolster's blog https://www.bolster.ai/

Fortifying The Digital Frontier: Everyday Habits That Shape Your Company's Cybersecurity Posture

In The Digital Realm, Even Everyday Habits Play a Crucial Role in Defining An Organization's Security Posture

By Apu Pavithran, CEO And Founder, Hexnode

The importance of internet safety has never been more pronounced than in today's digital age, where the boundaries between our personal and professional lives are increasingly blurred. However, with this ever-increasing reliance on online platforms comes a heightened vulnerability to cyber threats. June marks National Internet Safety Month in the US, a timely reminder for businesses to re-evaluate their cybersecurity posture and identify potential weaknesses before they become exploited.

The truth is, many common workplace habits, often considered trivial, can unknowingly create significant security gaps. While sophisticated malware and zero-day attacks grab headlines, it's often the seemingly mundane that poses the greatest threat.

The Hidden Dangers in Everyday Digital Habits

As we navigate through our daily digital interactions, many seemingly innocuous habits can inadvertently expose organizations to significant cybersecurity risks. One of the most common issues is weak passwords. Despite widespread awareness, weak passwords and password reuse remain common. Employees often opt for convenience over security, using easily guessable passwords or the same password across multiple platforms. This practice can lead to catastrophic breaches if one account is compromised.

Unprotected devices pose another substantial threat. With the shift to remote work, employees frequently use personal devices for professional tasks. These devices may lack the robust security measures typically enforced on company-issued equipment. Personal devices often miss critical updates, have inadequate antivirus protection or network security, and are more susceptible to theft. When these unprotected devices connect to the corporate network, they can become the entry point for cybercriminals.

Shadow IT, the use of unauthorized software and applications, is another growing concern. Employees often resort to unapproved tools to enhance productivity, bypassing corporate security protocols. These shadow IT applications can harbor vulnerabilities that are unknown to IT departments, creating gaps in the organization's security defenses. The lack of visibility and control over these tools makes it challenging for IT teams to manage risks effectively.

The challenge lies in the fact that these everyday habits are deeply ingrained and often go unnoticed until they cause significant damage. Therefore, fostering a culture of cybersecurity awareness within the organization is critical to mitigating these risks.

Fostering a Culture of Cybersecurity Awareness

Creating a robust cybersecurity culture requires a multifaceted approach that extends beyond traditional training programs. It's about embedding security into the very fabric of the organization, making it a fundamental aspect of every employee's daily routine.

Education and continuous training are foundational. Employees must be regularly educated on the latest cyber threats and best practices. This education should be dynamic, incorporating real-world scenarios and hands-on exercises to ensure engagement and retention. Phishing simulations, for instance, can be particularly effective in teaching employees to recognize and respond to suspicious emails.

Beyond training, organizations should encourage open communication about cybersecurity. Employees should feel empowered to report potential security incidents without fear of retribution. This openness can help in early detection and swift response to potential threats, minimizing damage.

Incorporating cybersecurity into performance metrics and recognition programs can also drive behavioral change. Recognizing and rewarding employees who adhere to security protocols and contribute to the organization's security posture can reinforce positive habits. This approach not only incentivizes good behavior but also highlights the importance of cybersecurity at all levels of the organization.

Leadership plays a crucial role in fostering this culture. Executives and managers must lead by example, demonstrating a commitment to cybersecurity in their actions and decisions. When employees see their leaders prioritizing security, they are more likely to follow suit.

Building a Resilient Security Architecture

While fostering a culture of cybersecurity is essential, it must be complemented by a resilient security architecture. This architecture should be designed to anticipate, withstand, and recover from cyber threats, ensuring business continuity and data integrity.

At the core of a resilient security architecture is a robust identity and access management (IAM) system. Ensuring that only authorized individuals have access to sensitive data and systems is fundamental. This includes implementing multi-factor authentication (MFA) to add an additional layer of security. MFA requires users to verify their identity through multiple forms of evidence, making it significantly harder for cybercriminals to gain unauthorized access.

Unified Endpoint Management (UEM) solutions are another pivotal factor in enhancing an organization's cybersecurity posture, especially in the context of remote work and the increasing use of diverse devices. UEM platforms provide a centralized approach to managing and securing all endpoints—ranging from laptops and smartphones to tablets and IoT devices—ensuring that they adhere to the organization's security policies. For example, during the surge of remote work over the past few years, many organizations leveraged UEM solutions to secure their distributed workforce. This approach enabled businesses to maintain operational continuity while safeguarding their data against evolving cyber threats.

Endpoint security is another critical component. With employees accessing corporate networks from various devices, securing these endpoints is paramount. Endpoint protection platforms (EPP) and endpoint detection and response (EDR) tools can provide comprehensive security by detecting, analyzing, and responding to threats at the device level. Regularly updating and patching software on all devices can also close vulnerabilities that cybercriminals might exploit.

Moving on, network security measures, such as firewalls and intrusion detection systems (IDS), are essential for monitoring and controlling incoming and outgoing network traffic. These tools help detect and prevent malicious activities, ensuring that only legitimate traffic is allowed through.

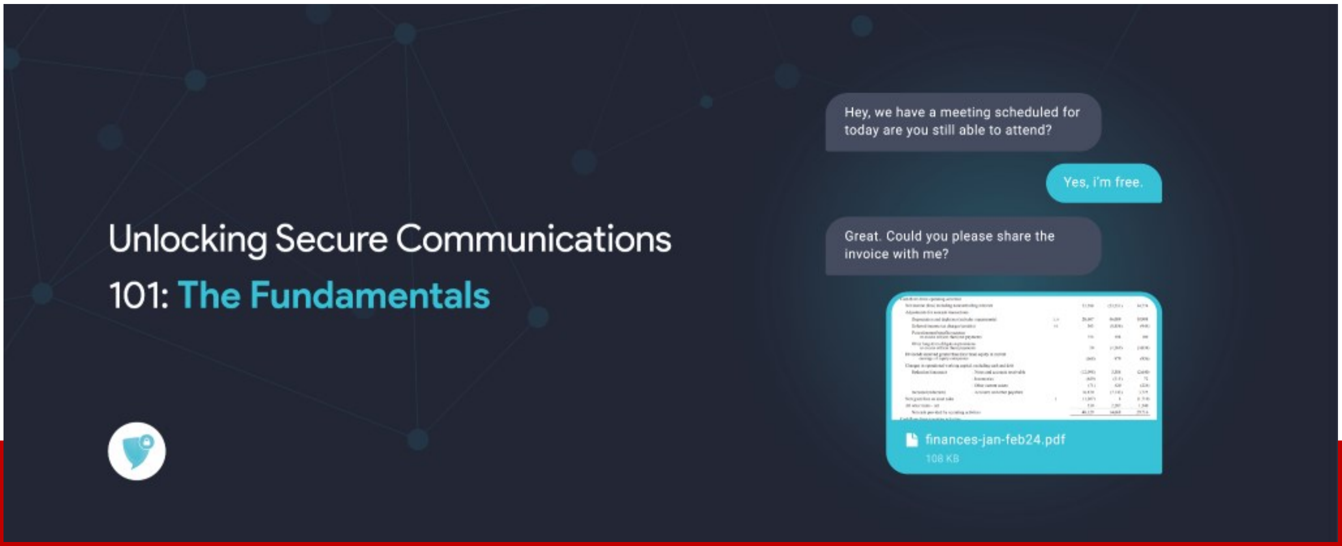
Data encryption, both at rest and in transit, is crucial for protecting sensitive information. Encrypting data ensures that even if it is intercepted or accessed by unauthorized individuals, it remains unreadable and unusable. Organizations should also implement regular data backups and a robust disaster recovery plan to ensure data can be restored in the event of a breach.

Finally, adopting a zero-trust security model can significantly enhance an organization’s defense posture. The zero-trust model operates on the principle that no entity, inside or outside the network, should be trusted by default. It requires continuous verification of user identities and device integrity, ensuring that access is granted only on a need-to-know basis.

In short, as we observe National Internet Safety Month, it's a timely reminder of the critical importance of safe practices and proper tools in our increasingly digital world. By addressing everyday digital habits, fostering a culture of cybersecurity awareness, and building a resilient security architecture, organizations can significantly enhance their defense against evolving cyber threats. As leaders in our respective fields, it's our responsibility to champion these initiatives and ensure a safer online environment for all.

About the Author

Apu Pavithran is the founder and CEO of Hexnode, the award-winning Unified Endpoint Management (UEM) platform. Hexnode helps businesses manage mobile, desktop and workplace IoT devices from a single place. Recognized in the IT management community as a consultant, speaker and thought leader, Apu has been a strong advocate for IT governance and Information security management. He is passionate about entrepreneurship and devotes a substantial amount of time to working with startups and encouraging aspiring entrepreneurs. He also finds time from his busy schedule to contribute articles and insights on topics he strongly feels about. Apu can be reached online via https://www.linkedin.com/in/apupavithran/ and at Hexnode's company website https://www.hexnode.com/ .



Hey, we have a meeting scheduled for today are you still able to attend?

Yes, I'm free.

Great. Could you please share the invoice with me?

Unlocking Secure Communications 101: The Fundamentals

By Nicole Heron, Marketing Manager at Salt Communications

Ensuring the protection of data and communications is of utmost importance for organisations adapting to the intricacies of the digital era. Are you knowledgeable about secure communications?

Whether you're new to security strategies or looking for a thorough review, acquaint yourself with the basics outlined below and delve deeper for comprehensive insights by researching analyst reports developed by Market Research giant Forrester who is led by Heidi Shey do regular reviews of the secure communications market, with 2024's edition found here.

Exploring the Foundations of Secure Communications

Secure communications involve safeguarding information shared between individuals to prevent unauthorised access to the information which has been exchanged. In real-world scenarios, unauthorised access could manifest as eavesdropping on conversations in public spaces, tampering with mail, or intercepting telephone conversations.

Within an organisational context, secure communications specifically entail ensuring that data exchanged among employees and/or clients remains accessible only to authorised users. Enterprise communication spans various channels such as messaging, voice calls and conference calls necessitating robust security measures to thwart unauthorised access.

The Importance of Secure Communications for Organisations

Effective communication is the cornerstone of any organisation, facilitating the exchange of critical information necessary for its operation and growth. Whether it's a face-to-face conversation, a virtual meeting, or a message sent through a secure messaging platform, every interaction carries valuable data. This data encompasses a wide array of sensitive information, including customer and employee data, contract details, financial figures, and strategic plans.

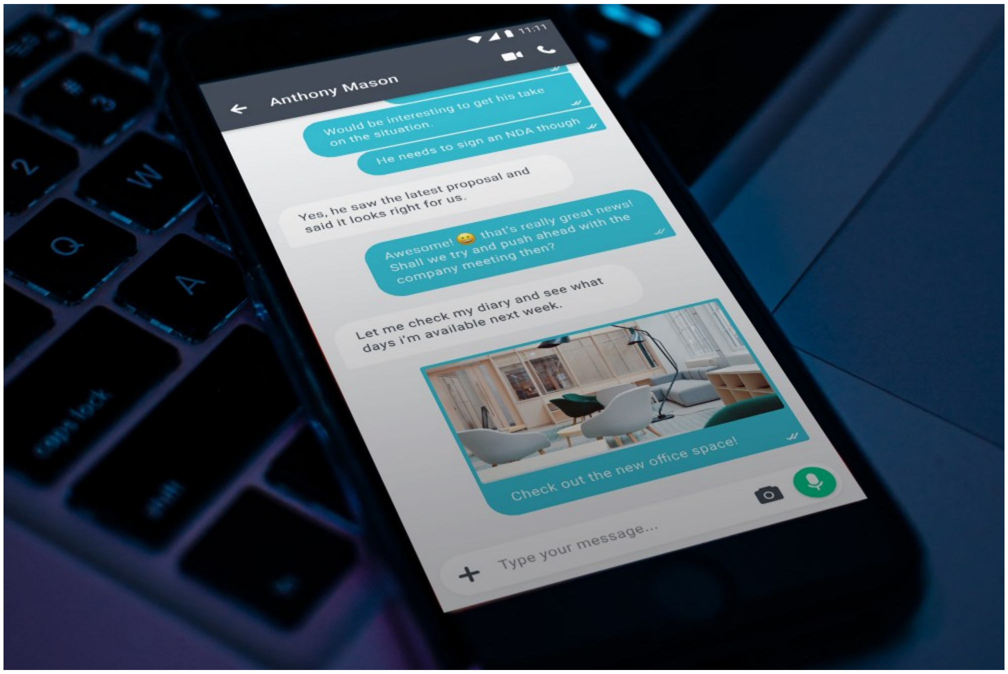
Protecting this information is paramount. Failure to utilise a secure messaging system can expose this data to unauthorised third parties, posing a significant threat to the integrity of your corporate network. Secure messaging protocols, encryption mechanisms, and authentication procedures play a crucial role in ensuring that information remains confidential and is only accessible to authorised parties. Regular audits and updates to security measures are essential to staying ahead of evolving threats in the digital landscape.

Furthermore, fostering a culture of awareness and accountability among employees is vital. Training programs on cybersecurity best practices and emphasising the importance of data protection can significantly reduce the likelihood of security breaches resulting from human error or negligence.

By investing in secure messaging technology and promoting a culture of cybersecurity awareness, organisations can effectively mitigate the risks associated with transmitting sensitive data, safeguarding their corporate network's integrity, and upholding the trust and confidence of customers, employees, and stakeholders alike.

Essential Components of a Secure Communications Strategy

Shielding against inadvertent sharing of sensitive information in personal conversations may be challenging due to the use of free consumer messaging apps which the user has zero control over. However, protecting official company communications against unauthorised access is achievable through various protective measures. Here are the essential components of a robust secure communications strategy:



Would be interesting to get his take on the situation.

He needs to sign an NDA though

Yes, he saw the latest proposal and said it looks right for us.

Awesome! 😀 that's really great news! Shall we try and push ahead with the company meeting then?

Let me check my diary and see what days i'm available next week.

Check out the new office space!

Type your message...

1. **Support for All Types of Communications:**

- Safeguarding messaging, voice calls, conference calls, secure file sharing and message broadcasting that can be integrated with internal systems to allow sensitive information to be securely pushed to selected personnel.

2. **Secure File Sharing:**

- Salt facilitates the secure transfer of confidential documents and sensitive images, ensuring end-to-end encryption for multiple attachments.

3. **End-to-End Encryption:**

- Utilising end-to-end encryption for various forms of communication to protect data at rest and in transit, while having an agnostic approach allows for the assurance that the latest technologies are always deployed.

4. **Data Retention Options:**

- Implementing message burn to automatically delete messages after they've been read or auto-delete to ensure information is wiped even if not read, reducing the risk of unauthorised access and facilitating control over data retention policies.

5. **Metadata Management**

- Salt enables organisations to effortlessly oversee their metadata, securely archiving conversations for highly regulated environments, storing statistical overviews, or instantly deleting all metadata.

6. **User and Security Management**

- Through the Salt management portal, trusted administrators can govern system invitations, communication channels, control in-app restrictions such as copy and paste and restrict users from taking screenshots for optimal internal security. If taken, users will be notified immediately. and group-wide security settings.

7. Flexible deployment
- Salt offers unbeatable, flexible deployment options tailored to your needs, with SaaS, Hybrid cloud instances and full on-premise installation options available.

8. Having a safe haven network:
- A secure preconfigured safe haven network is a dedicated, isolated network, under the control of the Risk and Security team within the organisation. Allowing for safe and secure communication within an organisation when its infrastructure becomes unavailable.

- Well-designed safe haven networks offer a refuge during crisis situations, ensuring continuity of essential business operations. This guarantees that critical functions persist even in adverse conditions, maintaining communication between internal decision-makers, key customers, and partners.

Elevating Communication Security with an Advanced System

When aiming to strengthen your organisation's communications, turn to trusted experts such as Salt Communications. Our secure communications platform incorporates military-grade security features like end-to-end encryption, message burn, and security for voice, messaging, and file sharing. Protect your communications today, before it's too late.

About the Author

Nicole Heron, 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.

Salt Communications is a multi-award winning cyber security company providing a fully enterprise-managed software solution giving absolute privacy in mobile communications. It is easy to deploy and uses multi-layered encryption techniques to meet the highest of security standards. Salt Communications offers 'Peace of Mind' for Organisations who value their privacy, by giving them complete control and secure communications, to protect their trusted relationships and stay safe. Salt Communications is headquartered in Belfast, N. Ireland, for more information visit Salt Communications.

Nicole can be reached online at (LINKEDIN, TWITTER or by emailing mailto:nicole.heron@saltcommunications.com) and at our company website https://saltcommunications.com/

Top Tips and Risks Ahead of the 2024 Olympic Games

By Narayana Pappu, CEO - Zendata

As buzz and excitement continues to build around the upcoming 2024 Summer Olympics, it is important to be aware of the potential cyberthreats that often target such large global events. The Tokyo Olympics in 2021 saw nearly 450 million cyber-attacks, a stark 2.5x increase from the London games. With nearly three million anticipated attendees at the Paris Olympics this year, and billions in revenue at stake, cybercriminals will not be slowing down.

What's more, with the significant advancements in technology in just the past three years since the Tokyo Olympics, cyberattacks have become even more sophisticated. The need for robust cybersecurity measures around this years' games is more critical than ever. Not only do security leaders, but all individuals need to be mindful of this - they must consider pre-event security risks, data collection during the event, the risks and benefits of AI at the event, but also best practices while attending the events.

Pre-event Security Risks

If you are heading out to the games in July and buying tickets, beware of scam websites attempting to sell fake resale tickets. In recent months, more than 300 scam websites have been identified, an extremely frightening number. So, how do you avoid falling victim to these scams? Be mindful that you are only purchasing tickets from the official Paris 2024 website: https://tickets.paris2024.org or https://ticket-resale.paris2024.org for resale tickets. Always double check the URL as there will be many variation URLs, apps and websites with very small differences that are fraudulent. Moreover, beware of buying tickets from individuals advertising on platforms such as WhatsApp, Instagram, Facebook and Telegram, as you can't ever be certain what the person is selling is actually real.

When it comes to your data, it is important to know that scam sites aim to capture your personal information. Bad actors will try to obtain your phone number and email, and tell you that they will be back in touch once the tickets you are looking for become available. On the official Olympics website, or via any genuine site, you will never be asked for your full login details and will only ever be asked for your payment details for tickets on real websites or the official Olympics app. If you are reading this too late and think you may have been duped, contact your bank, block your card immediately and report the scam.

Beware of Malicious Data Collection

With millions of people traveling to Paris this summer for the Olympic games, cybercriminals are preparing themselves to attack on all fronts, one of which is through guest Wi-Fi networks that can easily be corrupted. For all of you who think logging into public Wi-Fi networks is safe, think again. Cybercriminals can easily create open Wi-Fi hotspots disguised as legitimate and free networks, which if connected to, can compromise devices and install dangerous malware. To make matters worse, bad actors can also use these tactics to launch Man-in-the-Middle (MITM) attacks, where attackers interrupt an existing conversation or data transfer to steal login credentials, account details and credit card numbers. Once an unsuspecting user connects to the free, malicious Wi-Fi hotspot that the attacker created, the bad actor has full visibility into the exchange. The last thing anyone wants is to have to cancel credit cards and spend hours on the phone with banks, credit card companies while trying to enjoy the games.

What About Location Tracking and Biometric Data Collection?

It's no secret that the level of video surveillance across 41 venues at the 2024 Paris Olympic Games is predicted to be one of the biggest records broken this year, going way beyond previous Olympics. Why this level of surveillance you may be wondering? Despite its controversy, the French government sees it as a necessity to prevent terrorist attacks and help protect millions of attendees and athletes. Many have expressed concerns about how the data collected will be processed and used in the future. For many, they will feel at ease to know that facial recognition will not be applied to the footage at this year's games, rather reliance will be placed heavily on body scanners, according to officials.

The software that analyzes video streams will be used for threats in public spaces and the systems will flag eight different categories of events: abandoned objects, abnormally heavy crowds, crowd suggest, presence of use of weapons, a person on the ground, fire and contravening traffic direction. With a city that expects to receive millions of visitors, officials and law enforcement believe that by allowing artificial intelligence programs to look through video footage, suspicious and abnormal behavior will be easily detected, therefore making the games a safer place for all attendees.

Overall, with the games less than six weeks away, it is vital to be mindful of the security risks lingering before and during the events. Remember to play close attention to ticketing URLs and sites and stick to the official sale and resale pages. Steer clear of purchasing tickets from social media or apps like WhatsApp or Telegram, as the likelihood of them being scams is high. Beware of public Wi-Fi access points as bad actors will be creating open Wi-Fi hotspots disguised as legitimate and free networks. Lastly, familiarize yourself with the knowledge that the level of video surveillance at the games will be record breaking, but that at this time, there is no facial recognition where you run the risk of misidentification, though location data collected could be accessed by nefarious actors.

About the Author

Narayana Pappu is the CEO of Zendata. He started in Data Science at Fannie Mae before the term existed. He was tasked to build a better home price index than what was available in the market. For 15 years after that at PayPal, Coinbase, and Doctor on Demand, he built and scaled low-latency and high-volume internal investigation, graph, and entity resolution tools for risk management and compliance. He also launched consumer/merchant lending solutions in the US, UK, and Germany with over 5 billion dollars in annual transaction volumes each. And drove projects around data monetization with partnerships between PayPal, advertising, and payment networks; his expertise lies in building complex data solutions that are easy to implement, use, and generate incremental value.

Our company website: Data Protection, Privacy Observability and AI Governance Solutions | Zendata

Getting Out in Front of Post-Quantum Threats with Crypto Agility

By Dr. Avesta Hojjati, Vice President of Engineering at DigiCert

Ready or not, quantum computing technology is rapidly advancing, and its new capabilities will be available sooner than most think. Quantum technology has the potential to transform applications like materials sciences, drug discovery, financial transactions, and even climate change research. However, these revolutionary advances are also introducing substantial challenges to digital trust and encryption. Some experts have predicted that post-quantum computing technology will be powerful enough to break leading cryptographic security algorithms within a decade or less.

Organizations are taking the potential risks of post-quantum computing technology seriously, but their state of readiness remains shaky. According to a recent Ponemon Institute Report, 41 percent said they believe their organizations have less than five years to be ready for the new challenges. Yet only 23 percent of participants reported having a security strategy in place, and only 30 percent said their organizations are allocating budget for post-quantum readiness.

It's never too early to take a proactive stance

Why aren't organizations better prepared for new developments that could impact their most critical business processes? In informal conversations with customers, we've heard that many are more focused on short-term technology challenges like the rapid emergence of AI. Until a well-working quantum solution capable of cracking encryption actually appears, organizations prefer to focus on immediate security threats such as nation-state actors and other near-term IT priorities.

However, although current technology can't yet break today's encryption schemes, many organizations are concerned that attackers may be capturing encrypted packets now, with plans to crack them when new compute capabilities are available. According to the Ponemon Institute, 74 percent of survey participants worried that attackers might conduct these "harvest now, decrypt later" attacks.

Even if organizations aren't ready to directly address coming quantum computing challenges, they can still take steps to evaluate and be ready to rapidly deploy new encryption algorithms. That requires an organization with crypto-agility. Crypto-agility is the ability to discover a complete inventory of keys, certificates, algorithms, libraries, and protocols and then quickly switch to different encryption mechanisms. It requires understanding how cryptography is in use within an organization, and having the culture and tools required to rapidly update it.

Moving toward crypto-agility

Government and industry leaders have already taken some initial steps to help organizations address the coming post-quantum challenges. The National Institute of Standards and Technology (NIST) has already chosen four algorithms designed to withstand attacks by quantum computers, and is now in the process of standardizing these algorithms. Three new signature algorithms are expected to be ready for use in 2024, and organizations with implementations of crypto-agility will be best prepared to implement them.

Do an inventory

What are some steps that organizations can take to enhance crypto-agility today? Acquiring visibility is fundamental. All too often, IT and security staff have only limited insight into how and where cryptography is used in their infrastructure and business processes.

To understand which areas need attention, take steps to initiate a thorough inventory. Perform a complete scan of applications and systems that are now using public key cryptography. A reputable certificate discovery service can provide a current snapshot of your certificate environment.

Organizations should also extend the inventory beyond certificates, to examine components in their communications and hardware systems. Elements like Hardware Security Modules (HSMs) and Trusted Platform Modules (TPMs) do often hold cryptographic assets. In DevOps environments, code signing processes might also be vulnerable to advanced new attacks. To keep insights complete and current, organizations should perform discovery tasks on a frequent basis.

Automate for efficiency

After acquiring in-depth visibility into potentially risky areas, the next step is to ensure the organization is prepared to replace outdated cryptographic assets quickly, and at scale. These assets include any documents, servers, processes, users, and devices that utilize cryptography. Automation can play an important role in responding to new challenges on short notice. Individually managing cryptographic assets is error-prone, labor intensive, and time-consuming.

For a large enterprise organization with many thousands of cryptographic assets such as certificates, it's simply not practical to update crypto manually. The simplest way to ease certificate lifecycle management is to use PKI as a service, with an automation manager, which can enable organizations to rapidly roll out large numbers of certificates in just minutes, to cloud or on-premises environments.

Test for preparedness

Cryptographic elements often extend across a variety of applications and environments, so interoperability testing is another important step for improving crypto-agility. Many organizations, such as DevOps teams, routinely perform testing as part of their development cycles, so testing won't require major changes, but refinement of existing processes.

When it's time to update cryptographic algorithms, first check the interoperability of your infrastructure and applications before migrating at scale.

Solving for today's challenges, and preparing for the future

Although any strategic initiative can seem daunting, taking some steps to strengthen crypto-agility today can reassure key decision-makers that their organization is fully prepared for challenges that lie on the horizon. According to the Ponemon report, organizations that were considered high performers in the survey were more positive about their ability to achieve a safe post quantum computing future using the necessary cryptographic techniques. With the right culture, communication, tools, and technology partner, organizations can get on the fast track toward crypto-agility today.

For organizations and individuals wishing to learn more about how to become quantum ready or are on the fence about when to start a quantum strategy, DigiCert created World Quantum Readiness Day that will be on September 26, 2024. The event serves to drive awareness of the implications of quantum with a plethora of information on what companies can do today.

About the Author

Dr. Avesta Hojjati is VP of Engineering at DigiCert. Prior to joining DigiCert, Dr. Hojjati held a variety of roles at large enterprises such as Symantec and Yahoo, as well as being a founder and CEO of Security7 Inc., a penetration testing company. At DigiCert, Dr. Hojjati leads the advanced development of a suite of cybersecurity products, including embedded/IoT device security and post-quantum cryptography (PQC) solutions, in addition to influencing the broader product roadmap in conjunction with the M&A strategy.

Dr. Hojjati earned his Master's and Ph.D. in Computer Science from the University of Illinois at Urbana-Champaign, and his Bachelor's in Computer Science from Texas Tech University. He has authored over 20 journal/conference papers and is the inventor of 30 U.S. patents, both granted and pending.

Avesta can be reached online at https://www.linkedin.com/in/avestahojjati/ and at our company website https://www.digicert.com/

From Burnout to Balance: How AI Supports Cybersecurity Professionals

By Jason Lamar, SVP of Product at Cobalt

As technology advances, cyber threats are becoming more complex and harder to combat. According to Cobalt's State of Pentesting Report, this past year, the number of security vulnerabilities increased by 21%, putting organizations at greater risk than ever before. Because some of these vulnerabilities carry a high probability of exploitation, cybersecurity professionals are working overtime to reduce their exposure and give their organizations a fighting chance against cyber threats. Cyber professionals' day-to-day lives have always been plagued by long hours and high stress levels, but coupled with the growing number of cyber risks, industry leaders continue on the path to burnout.

While artificial intelligence (AI) has a reputation for contributing to the growing number of cybersecurity incidents, when used appropriately, this technology may provide cybersecurity professionals with some hope of relief from their immense workloads. Over the past 12 months, 75% of cybersecurity professionals have adopted new AI tools into their organization. With the growing accessibility of this technology, cybersecurity professionals have the opportunity to leverage these tools to speed up a multitude of tasks and better manage the always-on approach needed to stay secure in today's threat landscape.

Burnout From the Top Down

2024 has already set a new record for ransomware attacks as the number of new leak sites reached an all-time high for a single quarter. So far this year, the world has seen a number of high-profile ransomware attacks, including the Ascension Healthcare network and Change Healthcare attacks. These nationwide incidents forced cybersecurity teams nationwide into overdrive to protect their systems from similar vulnerabilities. On top of this, organizations are dealing with unsurmountable stress internally.

What's more, a recent SEC regulation now requires public companies to disclose cybersecurity incidents within four days of the incident being determined material, thrusting CISOs into the hot seat, nervously awaiting a cybersecurity blunder that could derail their careers. The mental and physical health of C-suite executives is dwindling, leaving some looking towards the exit. While C-suite professionals in the cybersecurity industry are 34% more likely than average respondents to say they currently want to quit their jobs, almost half of cybersecurity professionals at all levels are currently experiencing burnout.

Over the past six years, a third of cybersecurity teams have faced layoffs, with more internal shifts on the horizon. When layoffs occur, the uncertainty can have negative implications across the board. 67% of cybersecurity professionals agree that layoffs and resignations cause noticeable disruptions to their ability to maintain high-security standards. This is a 10% increase from 2023, demonstrating how cyber professionals are noticing these issues compound each year. The cybersecurity industry must find new ways to alleviate the burdensome workload currently on their plates or else they risk losing more talented professionals with each year to burnout.

Where AI Can Help

When put in the right hands, AI may provide immense benefits within the workplace. Our annual report found that 73% of cybersecurity professionals already view AI as a valuable tool rather than a threat to the organization. AI can help companies stay competitive by appealing to new generations of talent expecting the next tech, streamlining administrative tasks like reports, and monitoring data for irregularities.

From network traffic monitoring to checking for vulnerabilities, cybersecurity professionals have a multitude of items on their plate that could be alleviated by AI. Of course, that’s not to say this technology can fully take on the role of a trained cybersecurity professional or that it doesn’t cost something to begin to adopt AI. A new and ongoing learning burden exists for all who want the benefits. In fact, AI should be viewed as a new intern at the company. Colleagues should check its work for accuracy and jump in should issues arise, but ultimately, it can be trusted with a variety of lower-stake projects.

At Cobalt, for instance, we’re seeing an increased demand for pentests as companies incorporate offensive security strategies into their defense plans. Pentests can effectively uncover known and new vulnerabilities in various systems, making them a significant asset for cybersecurity teams. These tests are thorough, and with that, they’re also time-consuming. Our pentesters have found ways to leverage AI to automate report generation, free up time to address vulnerabilities and implement new security measures.

The cybersecurity industry is showing no signs of slowing down, and neither is AI’s role in our society. Cybersecurity professionals have been asked to battle large-scale cyber threats, internal disruption, and changing industry standards, forcing them to be on alert constantly. AI is no silver bullet, but it has the potential to provide much-needed relief for industry leaders who are desperate for more sustainable operations. If this past year has shown us anything, it’s that 2024 is shaping up to be a challenge like never before. Industry leaders should equip their teams today with emerging technologies to ensure they’re prepared for whatever this year throws their way and can better balance their workload.

About the Author

Jason Lamar is Cobalt's SVP of Product. In this role, Jason is responsible for product, product operations, and design teams pioneering Pentest as a Service (PtaaS) and building out the Offensive Security solution portfolio. Jason has made a career of building and launching innovative cybersecurity products, supporting from ideation to release to adoption success. With more than two decades of experience in the cybersecurity industry, Jason has worked with companies of all sizes to provide customers with the technology and knowledge to defend themselves in today’s dynamic risk landscape.

Jason can be reached on LinkedIn and at Cobalt’s website: https://www.cobalt.io/.

Modernizing and Applying FedRAMP Security Standards to Accelerate Safe AI

Numbers have shown the federal government has an appetite for AI. But how do technology companies become mission-ready for these needs?

By Gaurav (GP) Pal, stackArmor Founder and CEO

Often, technology develops faster than we can handle. This is especially true for the federal government and its partners — organizations that must adhere to strict security standards in the interest of national security.

The Federal Risk and Authorization Management Program, familiarly known as FedRAMP, is a clear case in point. FedRAMP provides a standardized and mandatory approach to security assessment, authorization and monitoring for cloud products and services. Commercial cloud service providers looking to do business with the government must be FedRAMP accredited and compliant.

But with emerging technology like artificial intelligence, new standards like this are just beginning to take shape.

Numbers have shown the federal government has an appetite for AI. According to a report from Stanford University, U.S. Defense and Federal Civilian agencies spent nearly $3B on AI solutions. This illustrates that the federal government recognizes the benefits and needs to adopt artificial intelligence to remain competitive and protect our national security. But how do technology companies become mission-ready for these needs?

The Intersection of Standards

There are a few recent mandates around the federal use of AI such as the Office of Management and Budget's newly released Memo M-24-10. This states government agencies must meet and implement mandatory AI safeguards that provide more reliability testing, transparency and testing of AI systems. Agencies must meet these standards by December 1, 2024.

This is where it gets complicated. Since many commercial AI solutions are delivered using cloud services, these AI solutions must be FedRAMP accredited.

With the rapid adoption of AI, there are now federal agency-specific use cases that detail the intersection of AI and cloud services. For example, the Department of Labor (DOL) has several projects utilizing cloud based commercial off the shelf NLP models for language translation, claims document processing and website chatbots. The United States Treasury has similar use cases.

These use cases, with both cloud and AI integration, are subject to FedRAMP compliance already.

Meeting New Benchmarks and Beyond

Regardless of whether a technology company is providing a cloud-based AI service or just a typical AI model, there are a few steps that can be taken now to accelerate the use of AI by building upon existing frameworks like FedRAMP.

Compliance can be achieved at a faster pace with an authority-to-operate (ATO) system to create an overlay for AI that is based on NIST AI RMF and NIST SP 800-53. By applying an ATO to AI, agencies can tailor, extend and augment existing guidelines and accelerate the integration of AI systems and safeguards.

Another helpful resource comes from the FedRAMP Program Management Office which recently published the Emerging Technology Prioritization Framework, designed to accelerate the availability of FedRAMP accredited Gen AI cloud solutions for federal agencies.

To jumpstart the availability of AI solutions, the FedRAMP PMO published a draft prioritization framework that defines the initial categories of Generative AI solutions and the benchmarks that will be used to drive selection. The initial focus is on Generative AI solutions for chat interfaces, code generation and prompt-based image generation.

Whether or not a company is subjected to FedRAMP or other similar standards, it's important to stay up to date with the latest guidance to ensure compliance. Having an awareness of these mandates and guidelines can make processes and development more efficient.

Government agencies should look for industry partners that are prioritizing security and thinking one step ahead. New regulations and standards are being rolled out frequently, so it's only a matter of time before some of these best practices become mandatory.

About the Author

Gaurav "GP" Pal is CEO and founder of stackArmor. He is an award-winning Senior Business Leader with a successful track record of growing and managing a secure cloud solutions practice with over $100 million in revenue focused on U.S. federal, Department of Defense, non-profit and financial services clients.GP can be reached at stackArmor's company website https://stackarmor.com/

The Great Ai Swindle

Why Fake Ai Is the Real Threat

By Peter Garraghan, Co-Founder & CEO at Mindgard, Professor in Computer Science at Lancaster University

AI washing, or making inflated or misleading claims about AI capabilities, is nothing new. In some ways it is to be expected when a new disruptive technology hits the limelight.

But since the launch of ChatGPT, it has gone into hyperdrive. In the scramble to seem innovative and capture market share, some companies are grossly overstating their AI prowess.

Nothing new here, surely, in a world where gaining attention is everything. However, the fallout of making such claims may go beyond marketing hype. AI washing is creating a false sense of security while masking serious threats.

AI is more than just ChatGPT

It’s important to cut through the hype: ChatGPT and Copilot are really exciting pieces of technology, but they’re just the latest chapter in an AI story spanning decades. What’s new here is the use of a specific type of neural network (that is, a mathematical model inspired by the structure of neurons in biological systems) called a transformer.

Because of the impact of ChatGPT, what most people today now mean when they refer to AI, is this sort of transformer-based neural network. These Large Language Models (LLMs) represent a groundbreaking advance, but they are merely the latest evolution of AI, not its totality.

Businesses have been using AI and machine learning (ML) for decades to spot anomalies, group data, give recommendations, and more. ML often doesn't use neural networks, and has been part of the software developer’s repertoire for many years.

Companies using ML in their products are technically correct stating they have AI, although possibly disingenuous. That’s because AI washing now takes place in this disconnect between what most of us on the research side mean when we use the term “AI”, and companies’ claims to be "AI-powered". What many actually mean is based on well-trodden ML methods or, worse, on the back of crude hard-coded logic masquerading as AI. In those cases, there are no AI characteristics, such as perceiving and learning from its environment.

The temptation to deceive

It's easy to see why companies might do this. In today's market, claiming AI capabilities carries serious weight. Numerous studies show consumers and business decision-makers view AI adoption as a competitive necessity. In one survey, 73% of consumers said that AI can have a positive impact on their customer experience.

Unsurprisingly, less scrupulous vendors are happy to slap the AI label on glorified IF statements in their code. It can help make sales and attract investors. However, bad-faith claims obscure real progress and push aside necessary conversations around the challenges of secure and responsible AI deployment.

Even well-meaning companies can succumb. We have seen cases where companies claimed to use AI although in reality many had yet to kick off their project in question. These companies felt they needed to claim an AI footprint in order to be seen as leading in their field, as they scramble to hire scarce and pricey AI talent.

Hidden risks

Disillusionment is a real risk, but AI washing brings dangers beyond disappointment. Fake AI claims obscure real progress and stifle important conversations around responsible AI use.

Companies touting "military-grade AI" with a straight face make it that much harder for genuine innovations to gain traction and trust. Hype drowns out expert calls for better data privacy, transparency, and fairness.

Most disturbingly, focusing on fictional AI diverts attention and resources from clear and present dangers. Ultimately AI is still software, and thus susceptible to cyber security risks that many professionals will be familiar with. Advanced generative AI models are already being incorporated into critical enterprise systems and customer-facing products. If built and deployed without security in mind, these models can be highly susceptible to cyber attacks. Indeed, it has been shown that bad actors can siphon sensitive data, reconstruct proprietary models, introduce malicious backdoors - all without a single line of hardcoded deception to tip off conventional cybersecurity.

The AI washing hype cycle doesn't just provide false comfort, it actively conceals genuine risk which businesses are struggling to navigate and manage. Overclaiming not only misleads consumers but can also lead businesses to make poorly informed decisions about AI adoption and investment. Companies may end up wasting resources on ineffective or insecure AI solutions, putting their data, intellectual property, and reputation at risk.

Earning trust in the age of democratized AI

To be clear, AI has the potential to be truly transformative for competitive businesses. But as complexity grows, so does the attack surface and the imperative for purpose-built, battle-tested AI security.

It is becoming increasingly difficult for a business to understand or manage AI security. To effectively navigate the AI landscape and make informed decisions, business leaders need to invest in AI literacy and education. This includes understanding the capabilities and limitations of different AI technologies, as well as best practices for secure and ethical AI deployment.

In the era of accessible deep learning, trust must be earned continuously with transparency, not bought with marketing fluff. Only by cutting through the AI-washing noise can enterprises build lasting value and safeguard the future.

About the Author

Peter Garraghan, CEO and Co-Founder of Mindgard, is an internationally recognised expert in AI infrastructure and security. He has pioneered research innovations that were implemented globally by a leading technology company used by over 1 billion people. As a professor at Lancaster University, he has raised over €11.6 million in research funding and published over 60 scientific papers. Mindgard is a deep-tech startup specialising in cybersecurity for any companies working with AI, GenAI and LLMs. Mindgard was founded in 2022 at world-renowned Lancaster University and is now based in London, UK. It has achieved €3.5 million in funding, backed by leading investors like IQ Capital and Lakestar. Mindgard's primary product – born from eight years of rigorous R&D in AI security – offers an automated platform for comprehensive security testing, red teaming, and rapid detection/response.

Peter Garraghan can be reached online at LinkedIn and at our company website https://mindgard.ai/

One Year Later: CISA's Secure by Design Initiative

By Joel Krooswyk, Federal CTO, GitLab Inc.

In April 2023, the Cybersecurity and Infrastructure Security Agency (CISA) unveiled the Secure by Design initiative, setting a new standard for security across the industry. The initiative urges vendors to create secure software before it goes to market, relieving end-users of the responsibility for product security.

CISA's Secure by Design initiative reflects the federal government's commitment to strengthening cybersecurity with three software security principles:

1. Take ownership of customer security outcomes.
2. Embrace radical transparency and accountability.
3. Build organizational structure and leadership to achieve these goals.

Now that it is entering its second year, vendors should expect more guidance from CISA and other agencies about how software is designed, developed, and delivered - and stay up-to-date on what's coming next, including the potential shift from product security being a voluntary commitment to a requirement.

Continuous Guidance and Requirements

Over 100 signatories have committed to making a good-faith effort to meet CISA's Secure by Design pledge goals, including increasing multi-factor authentication use, reducing default passwords, and reducing entire classes of vulnerabilities within one year. In the spirit of radical transparency, these organizations are encouraged to document their progress publicly.

In April 2024, CISA and the Office of Management and Budget (OMB) released a Secure Software Development Attestation Form, which CISA Senior Technical Advisor Jack Cable positions as another "key step" in ensuring federal contractors deliver secure products to the government.

These efforts aim to advance Secure by Design principles and enhance software supply chain security by providing more visibility and oversight into government agencies' software development and security practices.

Incentivizing secure software development

The White House is in talks with software makers to create frameworks that legally incentivize software development without exploitable flaws. This effort, coined Secure by Demand, is a significant component of the Biden administration's National Cyber Strategy.

Software liability is a complicated issue, especially in open-source software, which takes a community-based, collaborative approach to development. The focus on liability is a penalty-based approach for software vendors and the open-source community without consideration for its broader implications.

Some alternatives under discussion include requiring manufacturers to use open-source components to keep their tools updated to the latest versions or establishing shared liability between open-source maintainers and the companies that incorporate the tools into their products.

Regardless of future requirements, continued education on Secure by Design and Secure by Demand approaches is necessary to improve secure software development.

Developing Secure by Design software

A Secure by Design approach is the best way to avoid introducing vulnerabilities to an agency's software. All support agencies can move toward a Secure by Design framework by adopting DevSecOps practices, maintaining a software bill of materials (SBOM), and ensuring that AI incorporated into the software development process is secure.

Embedding security into software development from the start is best achieved through DevSecOps practices. Integrating security throughout every stage of the software development process allows fully automated security scanning to identify vulnerabilities rapidly, suggests remediation for vulnerabilities, and provides on-demand remediation training for developers.

Next, SBOMs can provide buyers and operators with additional visibility into a software package's origins, vulnerabilities, and risks. SBOMs are detailed inventories of software components, including versions, vulnerabilities, and licenses, that enable greater awareness of potential vulnerabilities and risks. While many agencies are now using SBOMs, they must be dynamic and continuously updated.

Finally, AI is one of the newest tools for helping ensure software is Secure by Design. AI can generate new code using natural language processing, identify the function of uncommented code, refactor legacy code bases into memory-safe languages, and understand and resolve vulnerabilities. However, before adopting any AI tools, agencies must ensure that their vendors have a published ethics statement, provide clarity around data learning and retention, and offer complete model transparency.

Secure by Design is a mindset shift toward radical transparency and truly embracing security as a priority. Those who work with the federal government understand that cybersecurity is essential to protect our nation’s critical services. We can all learn from the Secure by Design initiative and embrace a more secure and transparent future for software development, especially as the government’s guidance continues to evolve.

About the Author

Joel Krooswyk is the Federal CTO at GitLab Inc. He is a thought leader in software development, DevSecOps and other key IT practices within the public sector. In his current role, Joel ensures that GitLab has a voice in developing key DevSecOps practices coming from standards bodies, Congressional committees, industry working groups, and other influential organizations. He has 25 years of experience in the software industry spanning development, QA, product management, portfolio planning, and technical sales.

LinkedIn: https://www.linkedin.com/in/joelrkrooswyk/

GitLab Public Sector: https://about.gitlab.com/solutions/public-sector/

Spotlight on DeepKeep.ai

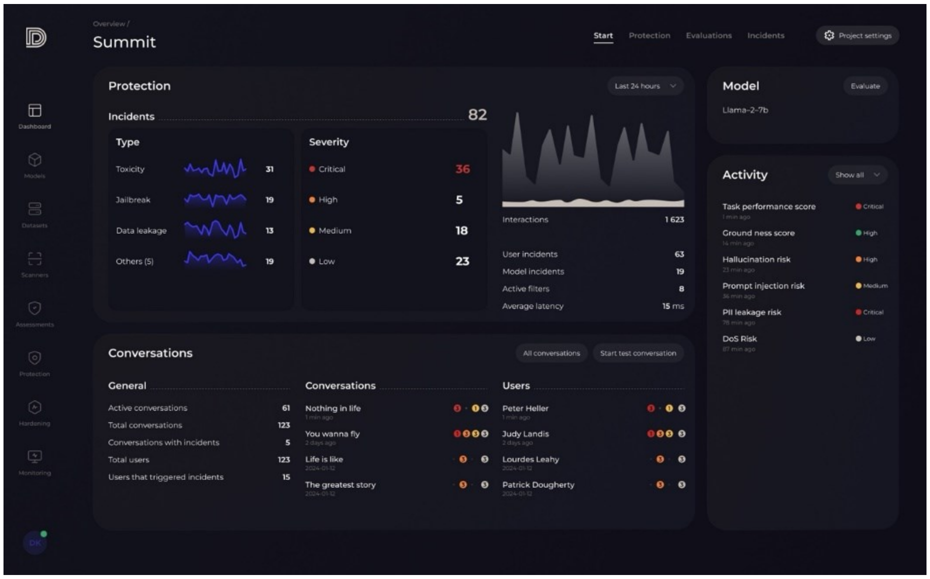
Spotlight on DeepKeep.ai

By Dan K. Anderson vCISO and On-Call Roving Reporter, CyberDefense Magazine

DeepKeep, the leading provider of AI-Native Trust, Risk, and Security Management (TRiSM), empowers large corporations that rely on AI, GenAI, and LLM technologies to manage risk and protect growth. Our model-agnostic, multi-layer platform ensures AI security and trustworthiness from the R&D phase of machine learning models through to deployment. This includes comprehensive risk assessment, prevention, detection, monitoring and mitigation.

"DeepKeep's technology and vision ensure the responsible and secure development, deployment, and use of AI technologies," says Rony Ohayon, CEO and Founder of DeepKeep. "We provide AI-native security and trustworthiness that safeguard AI throughout its entire lifecycle, allowing businesses to adopt AI confidently while protecting commercial and consumer data."

DeepKeep Dashboard:



Protection

Incidents 82

Type	
Toxicity	31
Jailbreak	19
Data leakage	13
Others (5)	19

Severity	
● Critical	36
● High	5
● Medium	18
● Low	23

Interactions	1 623
User incidents	63
Model incidents	19
Active filters	8
Average latency	15 ms

Model

Llama-2-7b

Activity

Task performance score 1 min ago	● Critical
Ground ness score 14 min ago	● High
Hallucination risk 23 min ago	● High
Prompt injection risk 36 min ago	● Medium
PII leakage risk 78 min ago	● Critical
DoS Risk 87 min ago	● Low

Conversations

General	
Active conversations	61
Total conversations	123
Conversations with incidents	5
Total users	123
Users that triggered incidents	15

Conversations
Nothing in life 1 min ago
You wanna fly 2 days ago
Life is like 2024-01-12
The greatest story 2024-01-12

Users
Peter Heller 1 min ago
Judy Landis 2 days ago
Lourdes Leahy 2024-01-12
Patrick Dougherty 2024-01-12

AI is becoming essential for businesses and everyday life. In 2023, 35% of businesses adopted AI, and 90% of leading businesses supported and invested in AI for competitive advantage. As the adoption of LLMs and generative AI surges across diverse applications and industries, organizational attack surfaces expand, introducing unique threats and weaknesses. New risks associated with LLMs go beyond traditional cyber-attacks and include Prompt Injection, Jailbreak, and PII Leakage, as well as the lack of trustworthiness due to biases, fairness, and vulnerabilities.

Gartner's new TRiSM category is a perfect fit for DeepKeep, as it ensures AI model governance, trustworthiness, fairness, reliability, robustness, efficacy, and data protection. This includes solutions and techniques for model interpretability and explainability, AI data protection, model operations, and adversarial attack resistance.

DeepKeep's unique use of Generative AI to secure Generative AI sets it apart from competitors like Hidden Layer and Robust Intelligence. We leverage GenAI to protect LLMs and computer vision models throughout the entire AI lifecycle. Our AI-native security solutions ensure businesses adopt AI safely, protecting both commercial and consumer data.

DeepKeep's expertise includes computer vision models, large language models (LLM) and multimodal scenarios. We prioritize implementing both trustworthiness and security to enable synergies equaling more than the sum of the parts, and also address both digital and physical threats, such as facial recognition and object detection, to ensure comprehensive protection.

DeepKeep raised $10M in seed funding in a round led by Canadian-Israeli VC Awz Ventures. Our roadmap includes expanding into multilingual natural language processing (NLP). As we collaborate with multinational companies globally, there is growing demand for support in multiple languages, with an initial focus on Japanese, driven by our partnerships with Japanese firms.

DeepKeep recently conducted an extensive evaluation of Meta's LlamaV2 7B LLM, summarized with the following weaknesses and strengths:

1. The LlamaV2 7B model is highly susceptible to both direct and indirect Prompt Injection (PI) attacks, with a majority of test attacks succeeding when exposing the model to contexts containing injected prompts.
2. The model is vulnerable to Adversarial Jailbreak attacks, provoking responses that violate ethical guidelines, with tests revealing a significant reduction in the model's refusal rate under such scenarios.
3. The model is highly susceptible to Denial-of-Service (DoS) attacks, with prompts containing transformations like word replacement, character substitution, and order switching leading to excessive token generation.
4. The model demonstrateד a high propensity for data leakage across diverse datasets, including finance, health, and generic PII.
5. The model has a significant tendency to hallucinate, challenging its reliability.
6. The model often opts out of answering questions related to sensitive topics like gender and age, suggesting it was trained to avoid potentially sensitive conversations rather than engage with them in an unbiased manner.

DeepKeep’s evaluation of data leakage and PII management demonstrates the model's struggle to balance user privacy with the utility of information provided. However, Meta’s LlamaV2 7B LLM shows a remarkable ability to identify and decline harmful content, boasting a 99% refusal rate in our tests. Yet, our investigations into hallucinations indicate a significant tendency to fabricate responses, challenging its reliability. Overall, the LlamaV2 7B model showcases strengths in task performance and ethical commitment, with areas for improvement in handling complex transformations, addressing bias, and enhancing security against sophisticated threats.

Dr. Rony Ohayon is the CEO and Founder of DeepKeep, the leading provider of AI-Native Trust, Risk, and Security Management (TRiSM). He has 20 years of experience within the high-tech industry with a rich and diverse career spanning development, technology, academia, business, and management. He has a Ph.D. in Communication Systems Engineering from Ben-Gurion University, a Post-Doctorate from ENST France, an MBA, and more than 30 registered patents in his name. Rony was the CEO and Founder of DriveU, where he oversaw the inception, establishment, and management. Additionally, he founded LiveU, a leading technology solutions company for broadcasting, managing, and distributing IP-based video content, where he also served as CTO until the company was acquired. In the education realm, Rony was a senior faculty member at the Faculty of Engineering at Bar-Ilan University (BIU), where he founded the field of Computer Communication and taught courses about algorithms, distributed computing, and cybersecurity in networks.

About the Author

Dan K. Anderson, CEO and Co-Founder Mark V Security.

Dan currently serves as a vCISO and On-Call Roving reporter for CyberDefense Magazine. Dan has spent his life developing and implementing communications between systems and developing systems and applications in Military, Healthcare, and Mining. He has a background in Electrical Engineering and Chemistry with emphasis in Healthcare Informatics, BSEE, MS Computer Science, MBA Entrepreneurial focus, and has specialized in Information Security and Assurance, earning his Certified Information System Auditor (CISA), Certified in Risk and Information Systems Control (CRISC), both from the Information Systems Audit and Control Association (ISACA). Additional certifications include: Certified Business Continuity Lead Auditor (CBCLA), Certified Ethical Hacker (C|EH), Payment Card Industry Internal Security Assessor (ISA and PCIP), and Information Technology Infrastructure Library (ITIL v3). Winner Top Global CISO of the year 2023.

Dan has worked for Healthcare IT Vendors such as Cerner, GE, and IDX, and consults globally in Information Systems Security, Regulatory Compliance, Information Systems Audit, and Intellectual Property Assurance.

Some of Dan's work includes consulting premier teaching hospitals such as Stanford Medical Center, Harvard's Boston Children's Hospital, University of Utah Hospital, and large Integrated Delivery Networks such as Sutter Health, Catholic Healthcare West, Kaiser Permanente, Veteran's Health Administration, and Intermountain Healthcare.

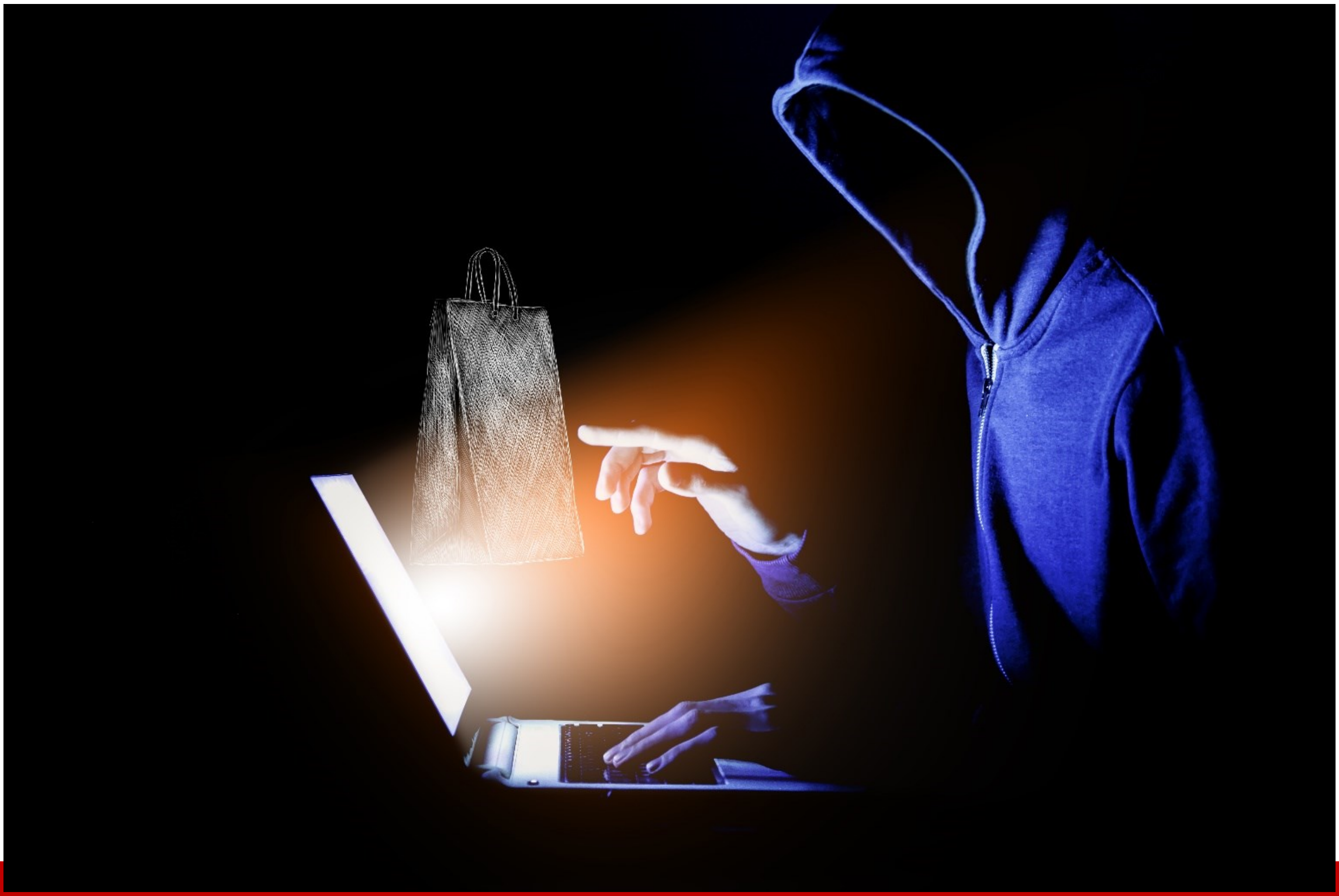
Dan is a Board member, Past President, and Academic Liaison Director of the Utah chapter of the Information Systems Audit and Control Association, (ISACA), a Board member of UtahSec.org, a Board member and Past President of FBI Infragard Salt Lake City Chapter, member of FBI Citizen's Academy Alumni Association, and member of the Security Technical Committee of Health Level Seven (HL7). Board Member, Center for Excellence in Higher Education Program Advisory Committee. Board Member, Utah Valley University Cyber Security Program Community Advisory Board. Board Member University of Utah Eccles School of Business Masters in Information Systems (MSIS) Program Advisory Board. Member BlackHat Network team. Healthcare Customer Advisory Board Member, Proofpoint. IEEE 2612 Cyber Medical Device Conformance founding member. 2023 Winner Global CISO of the Year.

Dan has served in positions as President, CEO, CIO, CISO, CTO, and Director for various companies, is currently CEO and Co-Founder of Mark V Security, Chief Information Security Officer, and Senior Management Consultant for Spectra Consulting Group, Current Cyber Advisor Board member for Graphite Health, and Former Chief Information Security and Privacy Officer for Lifescan Global, Inc.

In his spare time Dan has previously volunteered as an Ice Hockey coach for over 14 years in various youth hockey associations in Utah, High School-Midget Major AA travel teams, earning USA Hockey's highest coaching level 5 Master Coach. Current volunteer efforts in building the future of infosec security professionals through University Board work, involvement in the local hacking scene, and mentoring students and co-workers.

Dan lives in Littleton, Colorado and Salt Lake City, Utah

Dan can be reached online at (EMAIL, TWITTER, etc..) dan.anderson@markvsecurity.com, @Z0lton, and at info@markvsecurity.com



Spotlight On Riskassure

Riskaware by Riskassure Solves a Unique Problem

By Dan K. Anderson vCISO and On-Call Roving Reporter, Cyber Defense Magazine

In preparing for this article, I met with Larry Faragalli, Keith Huckaby, and Duane Tursi, Founders of Riskassure. They have created a unique product to address a significant deficiency in the Cyber Insurance Underwriting space. Why it resonated with me personally is that I've had to answer many Cyber Insurers' questionnaires, which have gone from a dozen questions to more than 250 questions in the last 5 years.

The lack of standardization on the questions, what evidence is collected, etc., can be difficult for CISO's and their teams, not to mention the inherent fear that a question answered incorrectly may invalidate the Cyber Insurance or make it not able to be used when needed.

Here is what I learned from the Founders of Riskassure:

Our Solution is Two-fold: one for businesses, one for cyber insurance carriers. We try to help them work collaboratively:

The central issue is that no business can tell you how much cyber information risk they have, what its value is, or where it lives.

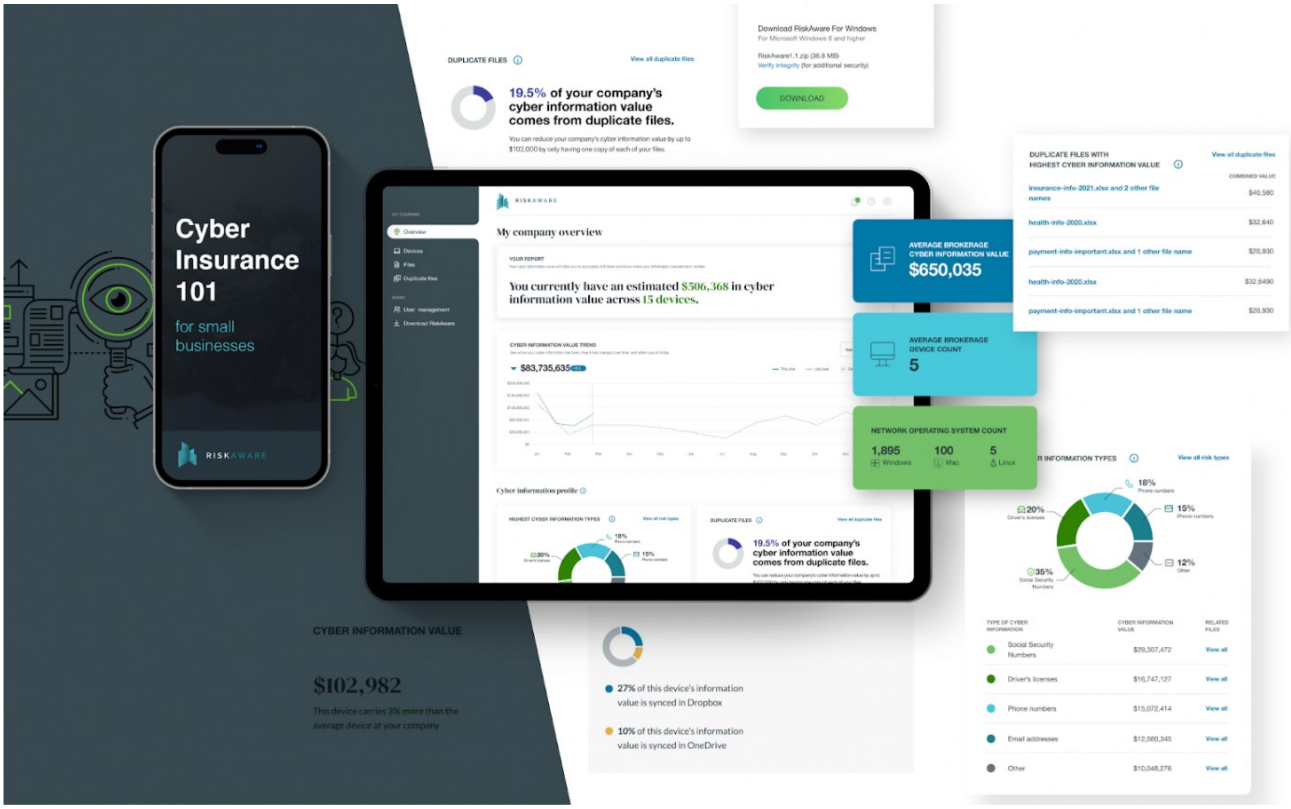
With this lack of visibility, it is impossible to make informed decisions about how much cyber insurance you need, leaving most businesses profoundly underinsured and vulnerable to business-ending cyber events.

The fundamental problem with today's cybersecurity insurance offerings, is that neither insurance companies nor their business customers have accurate data about sensitive information risk to make or buy truly relevant products.

This problem is the result of a deep data deficiency on behalf of cyber insurance carriers.

Unlike other lines of business, carrier cyber security practices have little tangible knowledge about their customer's data footprint, history, information risk value and rely heavily on customer attestation throughout the underwriting process. At the same time, it's difficult for cyber insurers to understand demand when the buyers themselves are still trying to figure out both their exposure and their buying appetites.

Furthermore, creating differentiated products that customers actually want remains elusive.



19.5% of your company's cyber information value comes from duplicate files.

You can reduce your company's cyber information value by up to $102,000 by only having one copy of each of your files.

You currently have an estimated $506,368 in cyber information value across 15 devices.

DUPLICATE FILES WITH HIGHEST CYBER INFORMATION VALUE

	COMBINED VALUE
insurance-info-2021.xlsx and 2 other file names	$40,580
health-info-2020.xlsx	$32,640
payment-info-important.xlsx and 1 other file name	$20,930
health-info-2020.xlsx	$32,6490
payment-info-important.xlsx and 1 other file name	$20,930

TYPE OF CYBER INFORMATION	CYBER INFORMATION VALUE	RELATED FILES
● Social Security Numbers	$29,307,472	View all
● Driver's licenses	$16,747,127	View all
● Phone numbers	$15,072,414	View all
● Email addresses	$12,560,345	View all
● Other	$10,048,276	View all

$102,982

This device carries 3% more than the average device at your company

27% of this device's information value is synced in Dropbox

10% of this device's information value is synced in OneDrive

Simply put: Do you know how much sensitive information you have and how much it would cost if it were found outside your custody? Riskassure does.

Several years ago, we identified a significant data deficiency in the cyber insurance underwriting space. We believe that businesses and insurance companies need to understand the amount or value of the data they want to insure or protect. With today's standard practices and available tools, at best, they are guessing the appropriate amount of insurance coverage they need. This uncertainty has resulted in many businesses needing help to obtain cyber insurance or in being drastically under- or over-insured.

RiskAssure's work has identified a substantial amount of "off-balance sheet" liability that businesses maintain in the form of sensitive information value, should their data be breached and found outside their custody by regulators.

To address this issue, we developed RiskAware, which can be installed for free, or with a nominal annual per-device cost for our most frequent and robust reporting features. All subscription types can be mixed and matched to cover your specific needs and budget. Our solution, designed with simplicity and affordability in mind, helps you scan every machine it is installed on, identifying every instance of PII and PHI and calculating the precise finable value of that data down to the penny. Depending on the subscription level, our software can perform scans every six months, weekly, or in real-time, giving business leaders control over their data valuation and protection level. We're balancing scanning frequency, which increases computational cost, against budget, making our solution extraordinarily accessible and affordable to every business size. This granular resolution down to the device level gives insurance underwriters the ability to deliver unique and innovative insurance products like key-device, department-level or even variable cyber policies rather than today's 'all-or-nothing' offerings.

RiskAware also identifies duplicates of sensitive information (files) and local repositories of cloud files, and provides precise file path locations that enables users to find and delete data that is less frequently used. It includes capabilities for detecting anomalous activity, such as significant movements of sensitive data on and off a monitored device, and alerts users to potential issues. Fully secure and end-to-end encrypted, our solution does not duplicate data or create additional potential breach liability, ensuring that data transmission is completely protected.

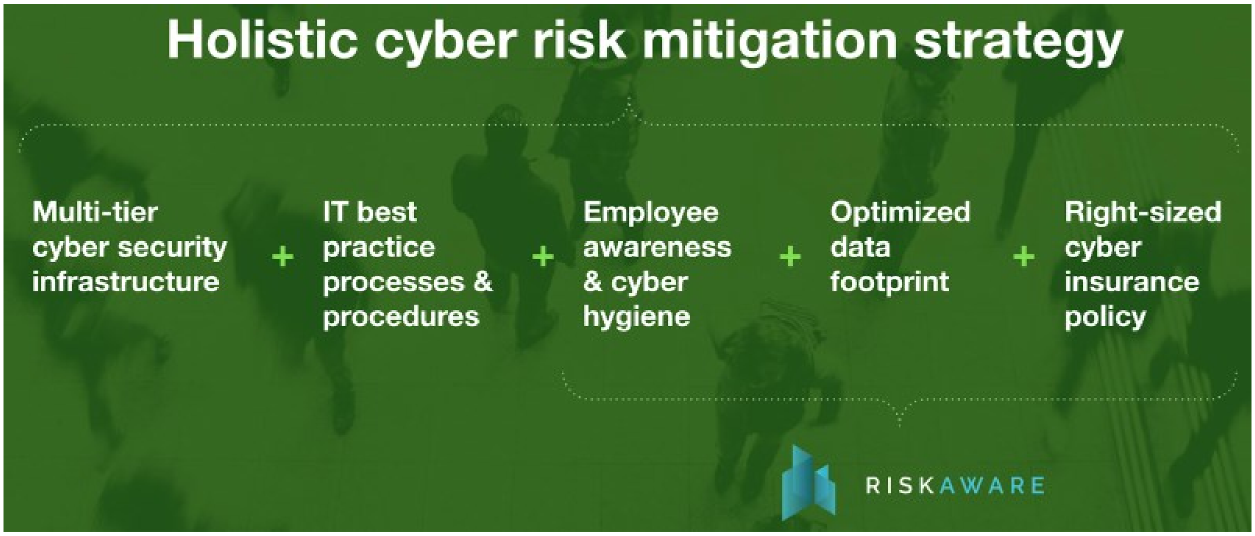
Dan: What is the nature of the problem you solve? What should we be worried about?

In today's digital landscape, cybersecurity fears are at an all-time high, with the frequency and sophistication of cyberattacks continually rising. RiskAware directly addresses these concerns, providing robust analysis and a much-needed peace of mind. The total cost of cybercrime globally reached $8 trillion in 2023 â€" and is predicted to hit $10.5 trillion by 2025, per the 2023 Ipsos Poll. Furthermore, the global average cost of a single data breach is at $4.45M, according to IBM. These attacks not only cause immediate financial damage but also inflict long-term reputational harm.

Our solution not only empowers carrier underwriters up-front during a discovery and underwriting process, but also empowers business leaders on an ongoing basis by offering continuous monitoring and real-time updates on the volume and value of a company's sensitive data. This proactive approach ensures that they are always prepared and protected, putting them in control of their sensitive information while driving user-based cyber hygiene behavior. Businesses can manage their data footprint to an intentionally decided upon amount of value (baseline) and empower the team to manage to that value.

Ransomware has become one of the most dreaded forms of cybercrime. Once considered a separate issue from data breaches, the two have now converged. Over the past year, cybercriminals have increasingly used data breaches as extortion, threatening to leak sensitive information unless a ransom is paid. This change in tactics has made it even more critical for businesses to have comprehensive cybersecurity measures in place. By inspiring action and behavior changes, our tool helps mitigate damage if an attack occurs, giving business leaders the confidence to operate without the constant fear of a cyber incident.

By offering targeted device coverage and the ability for cyber risk carriers to insure specific departments, our innovative approach to surfacing detailed underwriting information for cyber insurance provides a much-needed solution in an uncertain digital-first world. Businesses can no longer afford to view cybersecurity as a secondary concern. With our tool, you can implement a holistic multi-tiered cyber defense strategy that ensures your organization has the appropriate protocols in place.


Holistic cyber risk mitigation strategy
Multi-tier cyber security infrastructure
+
IT best practice processes & procedures
+
Employee awareness & cyber hygiene
+
Optimized data footprint
+
Right-sized cyber insurance policy
RISKAWARE

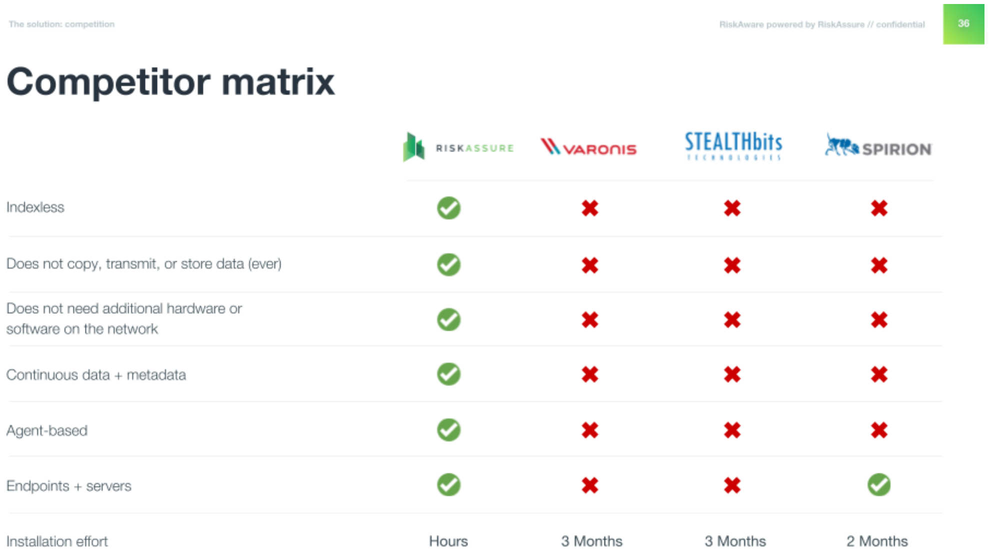
Dan: What does Gartner say about you? Why?

We have not yet engaged in analyst relationships, yet, but we are open to it.

Dan: Why is your solution better?

The state of today’s cybersecurity policy underwriting involves a series of questions, attestation, and possibly interviews focused on operational processes and procedures. This is an analog approach to a digital problem. RiskAware helps identify sensitive information and quantifies its value.

The RiskAware solution leverages a frictionless implementation approach by end users or silent enterprise deployments, that delivers results in minutes and hours (very short time to value - TTV). Most of the available solutions in the market require weeks and months of implementation with expensive consulting services, complex license models, etc.



The solution: competition

RiskAware powered by RiskAssure // confidential

36

Competitor matrix

	RISKASSURE	VARONIS	STEALTHbits TECHNOLOGIES	SPIRION
Indexless	✓	✗	✗	✗
Does not copy, transmit, or store data (ever)	✓	✗	✗	✗
Does not need additional hardware or software on the network	✓	✗	✗	✗
Continuous data + metadata	✓	✗	✗	✗
Agent-based	✓	✗	✗	✗
Endpoints + servers	✓	✗	✗	✓
Installation effort	Hours	3 Months	3 Months	2 Months

Dan: How does your solution fit into a company's Cyber stack? What does it pair well with?

RiskAssure is a stand-alone solution today. Today's cybersecurity defense strategy needs to be holistic and tiered. The tools and processes implemented by most businesses are good, and we did not seek to re-implement those, instead, we intentionally filled what we believed to be a gap: employee awareness & cyber hygiene, optimization (reduction) of sensitive information footprint, + a right-sized cyber insurance policy. As you see below, the first two are generally well-implemented, while we believe there remains opportunities for improvement in the latter 3, and RiskAware addresses this perceived gap.

As such, RiskAware pairs well with end user cyber hygiene initiatives, optimizing sensitive information footprints and businesses seeking right-sized cyber policies.

Dan: How are you funded?

We are proudly founder-funded, which has given us the freedom and flexibility to develop our product and achieve significant indications of market traction. As a group of seasoned leaders who run other successful businesses, we've been able to approach this venture with patience and thoroughness. This isn't just another project for us â€" it's a passion driven by our genuine belief that we can transform the cyber insurance industry.

As we now contemplate what our capitalization will look like, we've been doing our homework to ensure we're making the best decisions for RiskAssure's future. We've seen the impact we can have and the demand for innovative solutions in the cyber insurance sector. This solid foundation and our commitment to innovation position us well for the next phase of growth, where we can continue to push boundaries and set new standards in the industry. We suspect this will entail a level of partnership with industry, capital, or both.

Dan: What is your 3 year product roadmap?

Currently, we are focused on serving small and medium-sized businesses, but we are increasingly being pulled into the enterprise market. Larger organizations have shown strong interest in RiskAware, especially as they seek more advanced features and better segmentation of devices. This shift validates the versatility and scalability of our product. We recently completed a robust implementation of our subscription model, which now allows businesses to mix and match different tiers to suit their specific needs and budget. This flexibility ensures that our customers can optimize their cybersecurity strategies in the best way for their business.

Looking ahead, our vision is to incorporate enterprise- and carrier-specific features and explore international markets, while maintaining our strong US base. We envision leveraging large language models (LLMs) to underwrite the cyber insurance process once our network has sufficient devices. This advancement will significantly enhance the precision and efficiency of our offerings. We are currently providing an admin view on the enterprise side, but we are considering the benefits of giving every user their own view to drive better and proactive cybersecurity hygiene practices. This end-user perspective could empower employees to take a more active role in maintaining their device security, thereby strengthening the organization's overall cybersecurity posture. Businesses are only as strong as their weakest link; and that may include their supply chain and customers.

Another critical aspect of our work is addressing cyber insurance carriers' lack of historical data. We plan to do this by amassing comprehensive information on end-user behavior and cyber hygiene. Our approach involves deploying advanced data collection tools and techniques that respect user privacy and comply with data protection regulations. We aim to influence positive practices and demonstrate our ability to maintain and even improve the security of sensitive information.

Dan: How do you keep your Keyman developers around?

We retain our key developers by creating an environment where they can thrive both professionally and personally. Our team gets to work on innovative and exciting projects that hold their interest and allow them to exercise their creativity. We believe in giving our developers the space to take chances and experiment, which not only keeps them engaged but also fosters a culture of innovation and continuous improvement.

We also support hybrid and flexible work models, empowering our team to balance their professional and personal lives effectively. We've implemented a four-day workweek, which has been a significant factor in maintaining high morale and productivity. Our company culture emphasizes work-life balance, collaboration, and mutual respect, making it an attractive place for our devs to grow and stay committed.

Dan: Tell me about a customer who implemented your solution and what metrics show they are happy with the solution.

Customer A:

Small business in the medical space was in the market to add a cyber insurance policy to further bolster their security posture. They solicited quotes from a variety of carriers and chose not to purchase due to the cost of premiums. Six months after the quotes, they learned about RiskAware and decided to deploy it on their devices. Equipped with new information about their environment and the old quotes, they reengaged the carriers and selected and purchased a policy with the same coverage for 39% lower premium! The carriers factored the new information they had, and saw that the customer reduced their information footprint (before/after) since deploying RiskAware.

Customer B:

One of RiskAware's major success stories involves an insurance carrier with thousands of agents. This carrier faced significant challenges due to the diverse levels of IT sophistication among its non-exclusive agents, who also sell other types of insurance. This variation in IT capabilities led to frequent breaches, approximately one per month, causing considerable concern for the carrier regarding its brand reputation and the security of its sensitive information.

Before implementing RiskAware, the carrier needed help determining how much of its sensitive data was exposed in environments beyond its control. It also needed a robust system to monitor and manage these risks effectively. Our solution provided them with the required comprehensive oversight, significantly enhancing the organization's ability to track and protect its data across all agents and brokers.

The results have been outstanding. With our tool in place, the carrier has seen a dramatic reduction in the amount of sensitive information carried among their brokers. They now have real-time insights into the security status of their sensitive information, which has helped mitigate the risk of exposure and strengthen their overall cybersecurity posture. This newfound visibility has protected their brand reputation and provided peace of mind, knowing that their data is secure. The carrier's satisfaction is evident in their continued use of our solution and the positive feedback we receive.

Additional Background Info

Where we are currently:

Our company recently emerged from stealth mode after a few years of intensive research, development, and beta testing. Our solution is now installed on several thousand machines. We successfully completed a seven-figure paid pilot with a large carrier network, assisting them in determining the appropriate amount of cyber insurance to mandate for their brokers and agents. Additionally, we are an endorsed and advertised member benefit for more than 30,000 members of a prominent Michigan-based professional organization.

We are actively engaged in discussions with various insurance and reinsurance companies to integrate our tool with existing cyber policies and to develop innovative new cyber insurance products, similar to a blood test for life insurance policies or the Progressive safe driver program for auto insurance. These new products include cyber plans for “key devices”, department-level policies and even policies that flex seasonally to meet changing needs. Furthermore, we are in discussions with government officials regarding the deployment of our solution to state-owned machines, ensuring comprehensive cybersecurity measures across public sector devices.

Recently, we declined a generous offer from a capital group. Despite the attractive terms, we felt that the group misunderstood our platform and would not have been good stewards of our vision and mission. We remain committed to finding partners who align with our goals and values, ensuring that our innovative solutions continue to advance and protect the industry effectively.

“A couple technology experts met with an insurance specialist who pinpointed a significant problem within a certain domain that had been overlooked. It turned out to be a much larger issue than initially realized. We collaborated and discovered an opportunity to streamline and automate a complex problem and workflow using technology.” - Keith Huckaby, Co-founder & Partner

In conclusion, Riskaware by Riskassure solves a unique problem and there is nobody else that I’ve been able to find addressing this space. Its, timely, innovative, and needed. Hats off to the Riskassure Team!

About the Author

Dan K. Anderson Bio, Winner Top Global CISO of the year 2023. Dan currently serves as a vCISO and On-Call Roving reporter for CyberDefense Magazine. BSEE, MS Computer Science, MBA Entrepreneurial focus, CISA, CRISC, CBCLA, C|EH, PCIP, and ITIL v3.

Dan’s work includes consulting premier teaching hospitals such as Stanford Medical Center, Harvard’s Boston Children’s Hospital, University of Utah Hospital, and large Integrated Delivery Networks such as Sutter Health, Catholic Healthcare West, Kaiser Permanente, Veteran’s Health Administration, Intermountain Healthcare and Banner Health.

Dan has served in positions as President, CEO, CIO, CISO, CTO, and Director, is currently CEO and Co-Founder of Mark V Security, and Cyber Advisor Board member for Graphite Health.

Dan is a USA Hockey level 5 Master Coach. Current volunteering by building the future of Cyber Security professionals through University Board work, the local hacking scene, and mentoring students, co-workers, and CISO’s.

Dan lives in Littleton, Colorado and Salt Lake City, Utah

linkedin.com/in/dankanderson

Rsa Conference 2024 Highlights: Cutting-Edge Cybersecurity Innovations

AI in Action: Real-World Breakthroughs and Innovations

By Samridhi Agarwal, Masters Student, CMU

Attending the RSA Conference for the first time was an incredible experience! Ever since I began my journey in cybersecurity, attending the RSA Conference had been a major goal. The excitement still hasn't worn off—RSA week was truly amazing. Having a press pass was a highlight, allowing me to interact with CISOs, CTOs, CEOs, and other leaders from cutting-edge cybersecurity organizations. The conversations were eye-opening and deeply motivating, reinforcing my passion for cybersecurity and the collective effort of thousands of organizations working to safeguard our data.

The conference featured an impressive lineup of speakers, and as soon as I got the schedule booklet, I plunged into planning mode. Everything sounded fascinating, and I wanted to attend as much as possible during those four days. Balancing my time between the Expo, speaker sessions, and networking events, I met incredible people and learned about their groundbreaking work and organizations. A few organizations particularly stood out for their innovative contributions to the field. In this trip report, I'll be giving a shoutout to these organizations and the amazing people behind their work.

SafeBase: Transforming Trust Management with an Innovative Platform

In discussion with Al Yang, CEO and co-founder of SafeBase, we explored how their ***Trust Center Platform*** is revolutionizing the way businesses handle security reviews between buyers and vendors. Traditional security reviews are often plagued with inefficiencies and delays, leading to prolonged sales cycles and eroded trust. SafeBase addresses these challenges head-on by providing a centralized and automated method for trust management. With SafeBase, buyers can easily access a vendor's security posture, certifications, policies, and audit reports, significantly streamlining the review process and ensuring compliance standards are met without the usual friction.

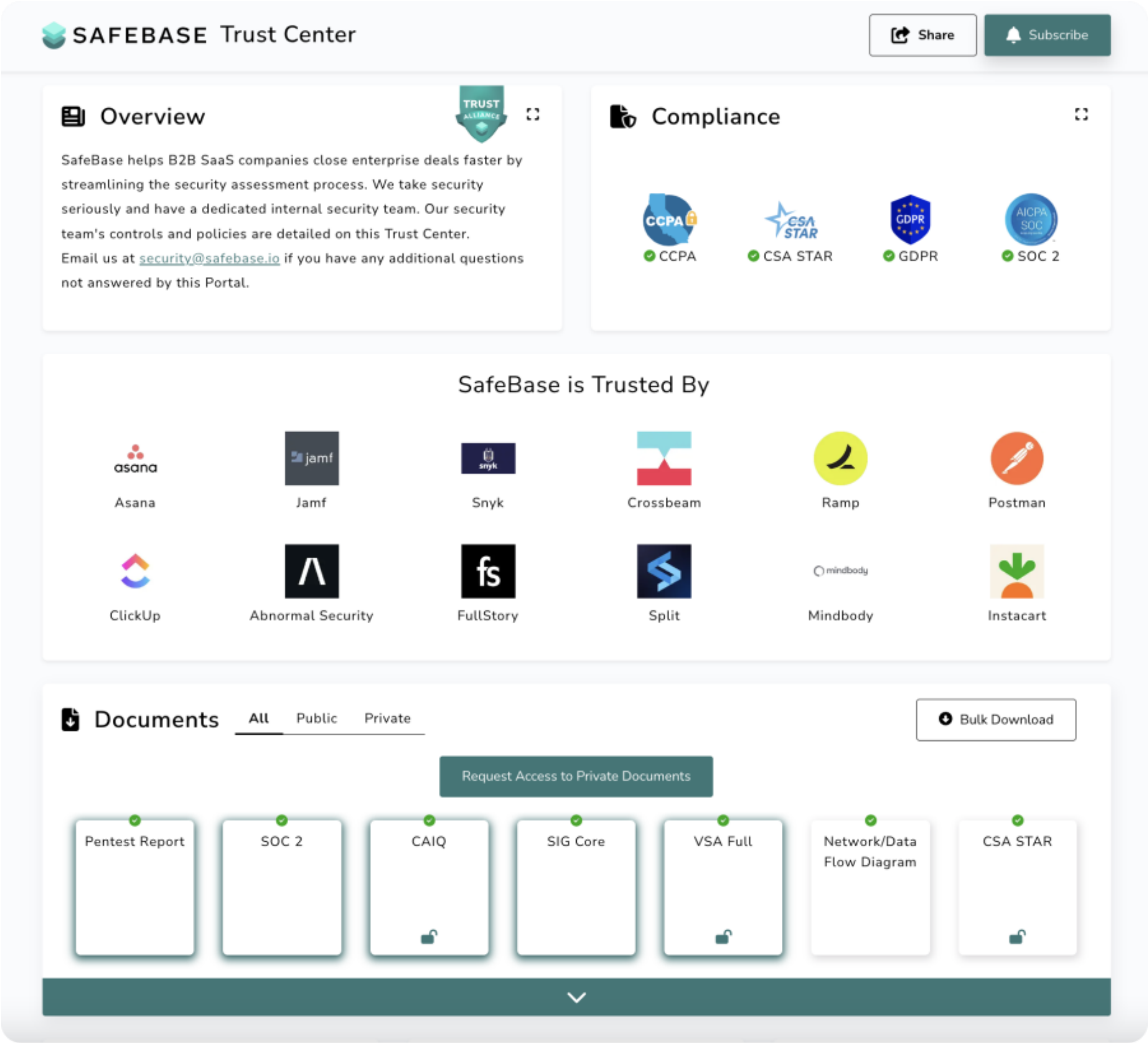
This innovation is particularly timely, given that third-party breaches have surged by 68% year over year. Additionally, 91% of organizations reported a software supply chain incident in the past year, emphasizing the critical need for robust supply chain security. SafeBase's Trust Centers offer a comprehensive solution by serving as a transparent source of truth for customers evaluating vendor security and compliance with regulations such as HIPAA and GDPR.

"Our goal has always been to change the way companies manage their trust posture," said Al Yang, CEO and co-founder of SafeBase. "Businesses must make their supply chain security a priority, and this

means building trust through transparency with their vendors and third-party partners. Prioritizing a company's security and trust posture is a critical step in protecting sensitive data, and centralizing those efforts in a connected digital ecosystem benefits businesses, vendors, and everyday people, and helps mend today's broken approach to security reviews."

Notably, SafeBase is trusted by high-profile companies like Abnormal Security, Amplitude, Asana, Axonius, ClickUp, Datadog, Gigamon, GitLab, Jamf, LinkedIn, OpenAI, and Plaid. The platform continues to evolve with features like AI Questionnaire Assistance, which uses artificial intelligence to expedite security questionnaires, and new integrations with Salesforce and G2. These enhancements demonstrate SafeBase's commitment to helping businesses communicate their security posture proactively and effectively.

Overall, SafeBase is setting new benchmarks in trust management by providing an efficient, accurate, and secure solution that combines human expertise with advanced automation, paving the way for businesses to effectively display and manage their security and trust posture.



SafeBase helps B2B SaaS companies close enterprise deals faster by streamlining the security assessment process. We take security seriously and have a dedicated internal security team. Our security team's controls and policies are detailed on this Trust Center. Email us at security@safebase.io if you have any additional questions not answered by this Portal.

Figure 1: *SafeBase Platform*

InviGrid: Redefining Cloud Security with Intelligent Automation

In a conversation with Yogita Parulekar, CEO of InviGrid, we delved into how InviGrid is transforming cloud security by integrating robust automation and intelligent design into their platform. Cloud security failures often result from cloud resource misconfiguration, with an alarming 99% of these failures being attributed to the customer's end. Traditional cloud provisioning tasks are not only mundane but also error-prone, contributing to significant security risks. InviGrid addresses these critical issues with their ***Intelligent Cloud platform***, which ensures security is embedded from day zero, freeing developers to focus on innovation rather than compliance.

Yogita Parulekar emphasized, “Invi Grid AI envisions a future where cloud deployments are secure and well governed by design day zero and self heal to stay secure at all times. Invi Grid provides day zero security on all cloud implementations with intelligence, expertise and ease of architectures and single click secure deployment to support rapid innovation.” This proactive approach is crucial, especially in a landscape where 52% of developers feel that security policies stifle innovation, and only 22% fully understand the security policies they must comply with.

InviGrid’s platform is engineered to tackle these challenges head-on. By automating mundane tasks, it allows developers to concentrate on core activities, accelerating time-to-market and enhancing business agility. The impact of InviGrid’s innovations is evident in their growing client base, which includes industry leaders across various sectors. Their commitment to security and efficiency has made them a preferred partner for companies looking to strengthen their cloud operations. “With InviGrid, we've transformed our cloud security posture,” noted a satisfied customer, “The platform's automation and ease of use have saved us time and significantly reduced our risk of breaches.”

InviGrid’s Intelligent Cloud platform stands out by offering a secure, well-governed cloud infrastructure. By focusing on proactive security measures and continuous innovation, InviGrid is setting new standards in cloud security. Their vision is clear: to make cloud security seamless and integral, ensuring that businesses can operate with confidence and agility in an increasingly complex digital landscape.

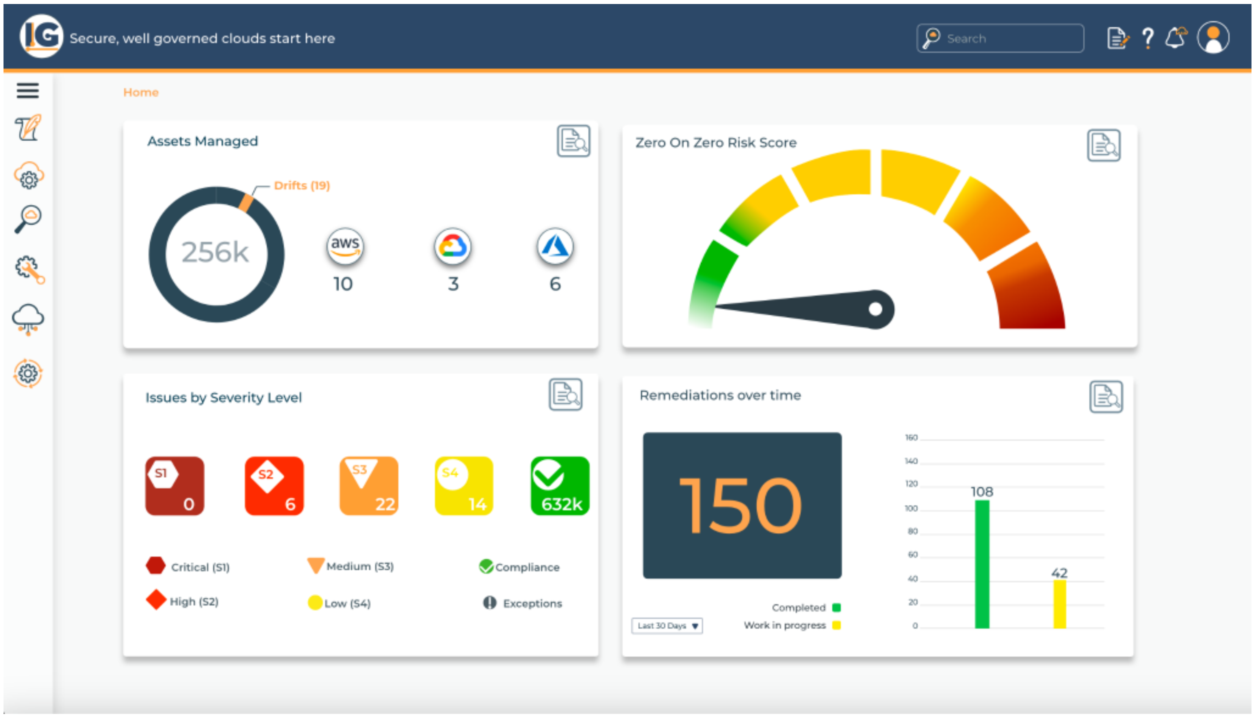


Figure 2: *InviGrid Dashboard*

AuthX: Elevating Enterprise Security with Seamless Authentication

In a conversation with Preetham Gowda, President of Technology at AuthX, we delved into how AuthX is transforming enterprise security by simplifying and enhancing identity and access management. AuthX's platform stands out for its comprehensive approach to securing devices, data, and workforce through advanced multi-factor authentication (MFA) and identity access management (IAM) solutions. By implementing these methods, AuthX ensures that enterprises can manage user and device identities with ease, enhancing both security and efficiency.

Preetham Gowda highlighted the significance of AuthX's solutions in today's security landscape. "Our goal is to provide businesses with a seamless and secure authentication experience," he said. "With rising security threats and compliance requirements, it's crucial for companies to adopt robust, user-friendly solutions." AuthX addresses these challenges by offering an array of authentication options, including biometrics, mobile authentication, hardware tokens, and RFID. This flexibility allows users to authenticate from anywhere, ensuring secure access across hybrid cloud architectures.

One of the standout features of AuthX is its commitment to security certifications. The platform is ISO 27001, HITRUST, and PCI-DSS compliant, underscoring its dedication to maintaining the highest security standards. This compliance not only enhances enterprise security but also aids in risk management, making it easier for businesses to adopt a Zero Trust security model. The platform's cost-effectiveness further adds to its appeal, providing scalable solutions without hefty startup costs, making it accessible to enterprises of all sizes.

AuthX's Single Sign-On (SSO) capability exemplifies their focus on secure and seamless user experiences. With support for open connectors like SAML, OpenID, and OAuth, users can securely access multiple web applications without the risk of breaches. This functionality, combined with robust device management features, ensures a secure and efficient BYOD (Bring Your Own Device) environment.

Overall, AuthX is redefining enterprise security by providing innovative, efficient, and user-friendly authentication solutions. By focusing on automation and compliance, AuthX enables businesses to safeguard their digital assets effectively, ensuring a secure and agile operational environment.

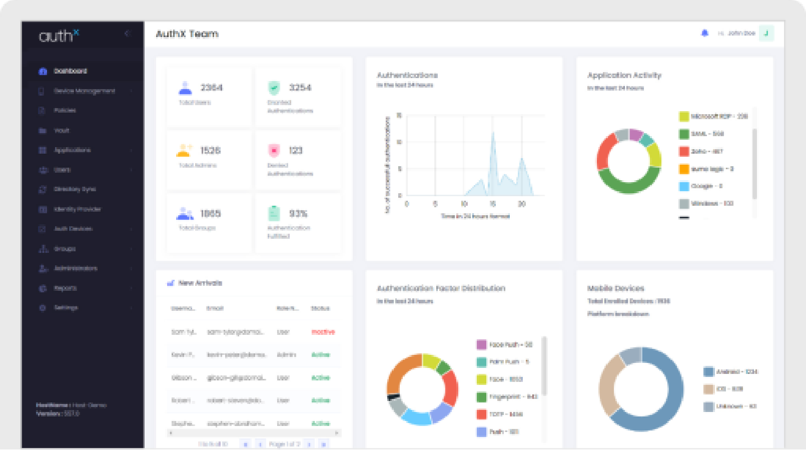


Figure 2: *AuthX Dashboard*

Reflecting on an Unforgettable RSA Conference 2024

RSA Conference 2024 was an incredible experience! A big thank you to Cyber Defense Magazine for making this dream come true. The conference felt like a grand festival where everyone shared a common mission: to secure our digital world and push technological boundaries. I was blown away by the collective effort and brilliant minds that made RSA week a success. From innovative product launches and enlightening sessions to vibrant networking events, every moment was awe-inspiring. It was truly uplifting to see the passion, creativity, and relentless determination of industry leaders and innovators dedicated to strengthening our digital defenses. I left the conference feeling inspired and optimistic about the endless possibilities in the dynamic field of cybersecurity.

About the Author

Samridhi is an award-winning woman in cybersecurity, reporter for Cyber Defense Magazine and currently pursuing a Master's degree in Information Security at Carnegie Mellon University. She is passionate about emerging technology and cybersecurity, with four years of industry experience as a cybersecurity associate and solution advisor. Throughout her career, she has collaborated with various clients and industries, analyzing their security infrastructure and implementing measures to address vulnerabilities in alignment with industry standards such as NIST and ISO27001. She is committed to continuous learning and exploring advancements to enhance global security and safeguard data.

Samridhi can be reached online at sam@cyberdefensemagazine.com

EVENTS

black hat® USA 2024

AUGUST 3-8, 2024

MANDALAY BAY/LAS VEGAS

informatech

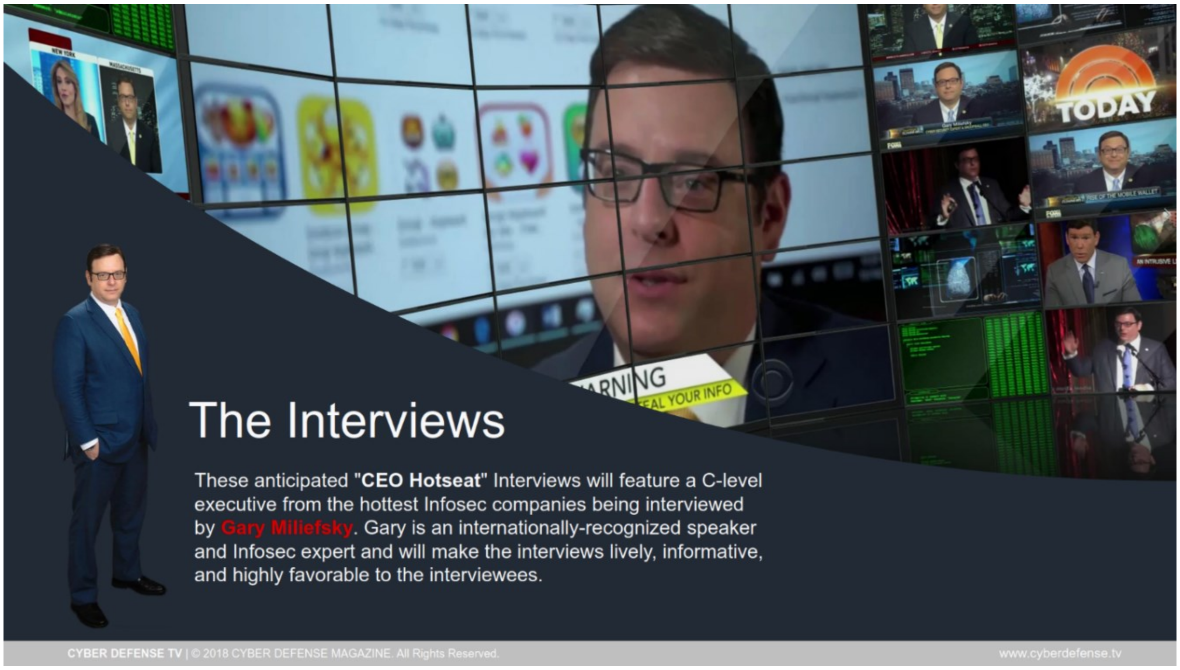
CYBER DEFENSE TV

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.



The Interviews

These anticipated "**CEO Hotseat**" Interviews will feature a C-level executive from the hottest Infosec companies being interviewed by Gary Miliefsky. Gary is an internationally-recognized speaker and Infosec expert and will make the interviews lively, informative, and highly favorable to the interviewees.

CYBER DEFENSE TV | © 2018 CYBER DEFENSE MAGAZINE. All Rights Reserved. www.cyberdefense.tv

---

Copyright (C) 2024, Cyber Defense Magazine, a division of CYBER DEFENSE MEDIA GROUP (STEVEN G. SAMUELS LLC. d/b/a) 276 Fifth Avenue, Suite 704, New York, NY 10001, Toll Free (USA): 1-833-844-9468 d/b/a CyberDefenseAwards.com, CyberDefenseConferences.com, CyberDefenseMagazine.com, CyberDefenseNewswire.com, CyberDefenseProfessionals.com, CyberDefenseRadio.com,and CyberDefenseTV.com, is a Limited Liability Corporation (LLC) originally incorporated in the United States of America. Our Tax ID (EIN) is: 45-4188465, Cyber Defense Magazine® is a registered trademark of Cyber Defense Media Group. EIN: 454-18-8465, DUNS# 078358935. All rights reserved worldwide. marketing@cyberdefensemagazine.com

Cyber Defense Magazine

276 Fifth Avenue, Suite 704, New York, NY 1000

EIN: 454-18-8465, DUNS# 078358935.

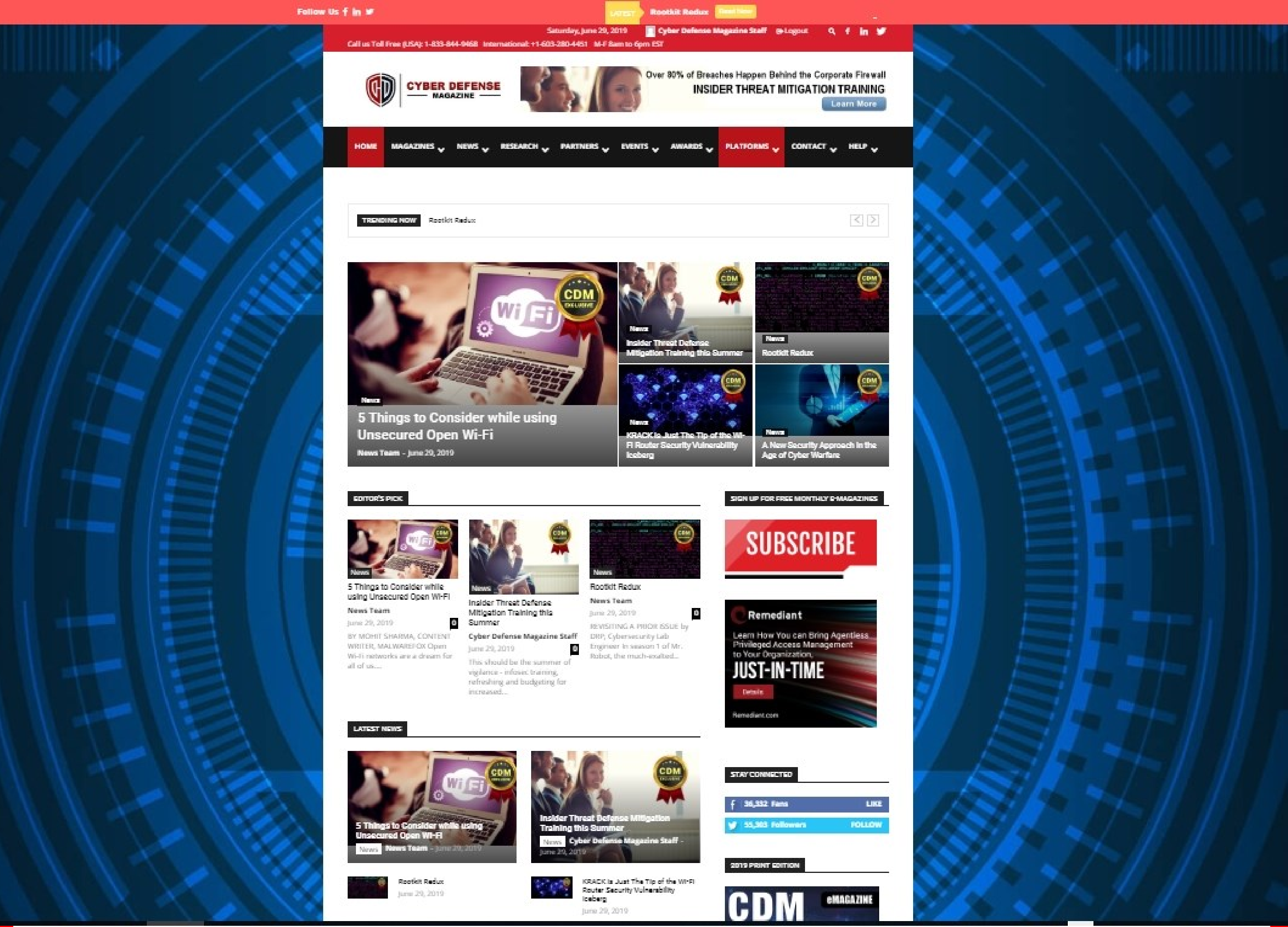
All rights reserved worldwide.

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: 07/02/2024



Call us Toll Free (USA): 1-833-844-9468 International: +1-603-280-4451 M-F 8am to 6pm EST

Trending Now: Rootkit Redux

5 Things to Consider while using Unsecured Open Wi-Fi
News Team - June 29, 2019

Insider Threat Defense Mitigation Training this Summer

Rootkit Redux

KRACK Is Just The Tip of the Wi-Fi Router Security Vulnerability Iceberg

A New Security Approach in the Age of Cyber Warfare

5 Things to Consider while using Unsecured Open Wi-Fi
News Team
June 29, 2019 0
BY MOHIT SHARMA, CONTENT WRITER, MALWAREFOX Open Wi-Fi networks are a dream for all of us....

Insider Threat Defense Mitigation Training this Summer
Cyber Defense Magazine Staff
June 29, 2019 0
This should be the summer of vigilance - infosec training, refreshing and budgeting for increased...

Rootkit Redux
News Team
June 29, 2019 0
REVISITING A PRIOR ISSUE by DRP, Cybersecurity Lab Engineer In season 1 of Mr. Robot, the much-exalted...

5 Things to Consider while using Unsecured Open Wi-Fi
News News Team - June 29, 2019

Insider Threat Defense Mitigation Training this Summer
News Cyber Defense Magazine Staff - June 29, 2019

Rootkit Redux
June 29, 2019

KRACK Is Just The Tip of the Wi-Fi Router Security Vulnerability Iceberg
June 29, 2019

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/]()

CBS NEWS
abc
AS SEEN ON TV
CNN
FOX NEWS channel
NBC
FOX
MSNBC
USA TODAY
Inc.
The New York Times
Bloomberg NEWS
The Washington Post
FOX BUSINESS
BusinessWeek
YAHOO!
Forbes
Entrepreneur
REUTERS
The Boston Globe
ALWAYS FREE
NO STRINGS ATTACHED

* with help from writers
and friends all over the Globe.