CYBER DEFENSE MAGAZINE

eMAGAZINE

MARCH 2024

In This Edition

Unlocking the Power of Governance in Cybersecurity: NIST CSF 2.0 Introduces 'Govern' to Redefine CISO Leadership in 2024

Cybersecurity or Cyber Resilience: Which Matters More?

A Consolidated Approach to Fraud: Bringing Together Risk Insights, Organizations and Technology

...and much more...

MORE INSIDE!

CONTENTS

@MILIEFSKY

From the

Publisher…

Dear Friends,

In my capacity as CEO of Cyber Defense Media Group (CDMG), parent of Cyber Defense Magazine, I'm pleased to observe that we continue the trend of broadening readership, as well as expanding the services of CDMG.

A current example is the recent interview on CyberDefense TV, with author Jeffrey Stephens. During the interview, Jeff recounted his experience of identity theft involving the hijacking of his FB account. His efforts to reclaim ownership of the account were spurned by the website operator. Upon seeing the interview, one of our CDMG executives took the pro-active route of introducing Jeff to a magazine contributor, who has the capability of reestablishing Jeff's ownership and control of the account. It's an ongoing effort, which we'll report on next month.

We also feature the CDMG Global Awards program at https://cyberdefenseawards.com/ , and the many participating professionals who have earned this important recognition for their contributions to the cybersecurity industry. Reflecting the expansion of cybersecurity-related activities, readers will note the addition of several new award categories.

We would like to remind our contributors and supporters that the 2024 RSAC Conference will take place in San Francisco, CA, May 6-9, 2024. The theme is The Art of the Possible, and online registration is available at https://www.rsaconference.com/usa?utm_source=mb-cyberdefense&utm_medium=referral&utm_campaign=v-digitalad-register-us2024 Submissions Are Now Open for RSAC Innovation Sandbox and RSAC Launch Pad. Learn More

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.

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

@CYBERDEFENSEMAG

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 March 2024 Issue

From the Editor-in-Chief

From the Editor's desk, we are seeing a subtle shift in a delicate balance. Although we have always concentrated on fairly technical topics for use by seasoned CISOs, we are now attracting a growing audience of up-and-coming professionals. This trend is reflected in both the nature of the many unsolicited submissions and the breadth of our readership.

We also perceive a changing balance between cyber job openings and qualified applicants. For some years, we have seen reports of hundreds of thousands of job openings for cyber professionals. The reported shortage of qualified cyber workers has not always been accurate, especially in the over-hyped availability of 6-figure starting salaries. More recently, industry reports have begun to feature both more stringent budget considerations and modifications to priorities, both leading to more demanding criteria for cyber professionals, especially in starting positions.

Since our editorial practices both reflect the market changes and provide guidance for our readers to prepare for the future, we are pleased to offer a recommendation in particular to employers and prospective employees. It should come as no surprise that we recommend that you read our publication thoroughly and use the actionable information to tune up both resumes and interview topics.

Overall, the trends show an expected expansion of role of CISO, as well as some expansion of need for CISOs to include services of other specialized professionals. Our readers will notice this broader representation of disciplines of value to CISOs.

Wishing you all success in your cybersecurity endeavors,

Yan Ross
Editor-in-Chief
Cyber Defense Magazine

About the US Editor-in-Chief

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


SPONSORS

RSAConference™2024

San Francisco | May 6 – 9 | Moscone Center

LEARNING.
NETWORKING.
INNOVATION.

THE TRIPLE THREAT FOR CYBERSECURITY SUCCESS.

RSA Conference 2024 will bring the cybersecurity community together again in San Francisco for four industry-shaping days, and you can be a part of that important conversation.

From May 6 – 9, you'll be able to:

- See what the future holds with the hottest industry topics and emerging trends
- Expand your knowledge and be inspired by forward-thinking Keynotes
- Demo the latest products to find real-world solutions from over 600 companies
- Enhance your career through valuable networking opportunities

Let's redefine The Art of Possible by shaping solutions, tackling challenges, and encouraging the collective strength of coming together as a community.

Act now for the biggest discount!

Visit www.rsaconference.com/cyberdefense24 to learn more and register.

#RSAC

FOLLOW US

THE ART OF POSSIBLE

CionSystems

Next Generation Enterprise Identity Management (EIM)™

THE SECRETS OF HARDENING ACTIVE DIRECTORY

• Deploy. • Manage. • Tune up. • Audit. • Defend. Report.

GET YOUR FREE eBook

Get https://cionsystems.com/

DAKOTA STATE UNIVERSITY

CYBER 27 INITIATIVE

< mission_BestCyberAnywhere />

The Cyber 27 Initiative is what's next for Dakota State University. Over the next five years, we're building new labs, forming new partnerships and pushing the limits of what a STEM university can do.

It's not just what's next for DSU.
It's the next chapter for cyber everywhere.

DSUcyber27.com

NIGHTDRAGON

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

-David DeWalt

Managing Director and Founder NightDragon Security

ADVISE

WE DELIVER SOUND ADVICE AS YOUR FINANCIAL PARTNERS

INVEST

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

ACCELERATE

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

www.nightdragon.com

UNKNOWN
CYBER

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

Not by us. We detect the unknowns.

www.unknowncyber.com

2001 2024

ALLEGIS CYBER CAPITAL

The first dedicated cybersecurity venture firm in the world.

AN INTEGRATED GLOBAL, STAGE-AGNOSTIC CYBERSECURITY INVESTMENT PLATFORM SPANNING SEED THROUGH GROWTH.

For 20 years, AllegisCyber Capital has offered a proven investment platform that actively engages with the most promising entrepreneurs in cyber and delivers the market access, team building, and operating experience essential to their success.

BUILDING AND FUNDING THE MOST INNOVATIVE COMPANIES IN CYBER

Signifyd | SAFEGUARD CYBER | ELISITY | panaseer | Synack

SkyHive | cyber GRX | DRAGOS | CONCEAL | vArmour

ALLEGISCYBER CAPITAL

www.allegiscyber.com


DATATRIBE
CYBER STARTUP FOUNDRY
Forging dominant companies from nation-state domain expertise
CAPITAL | RESOURCES | GUIDANCE | SUCCESS
HOME TO THE WORLD'S FASTEST GROWING CYBERSECURITY AND DATA SCIENCE COMPANIES
quickcode
DRAGOS
ENVEIL
INERTIALSENSE
PREVAILION
the cyberwire
Ntrinsec
SIXMAP
STRIDER
CONTRAFORCE
BLACKCLOAK
SightGain
JOIN THE TRIBE
DATATRIBE.COM

CYDERES

We will focus on your cybersecurity, so you can focus on your business.

We have the right mix of people, processes, and technology to build your robust security program and respond successfully to any threat that comes your way.

Cyber **De**fense
& **Res**ponse.

It's what we do.

cyderes.com


ARTICLES

Unlocking the Power of Governance in Cybersecurity: NIST CSF 2.0 Introduces 'Govern' to Redefine CISO Leadership in 2024

By Shirley Salzman, CEO and Co-Founder, SeeMetrics

As all eyes are towards the updated NIST CSF 2.0 publication, some of the spoilers have already been published – now security leaders not only need to identify, protect, detect, respond and recover; they also need to govern.

Most of the CISO's C-Suite peers already govern with a dedicated management platform, while the CISO's team still struggles with piles of fragmented data, spreadsheets, and perhaps consultancy firms that create.. well.. more spreadsheets..

Things have transformed in a decade: think about the approach towards governance in 2014 and now in 2024. In the past, the CISO needed to check the box of the functions' controls. Today, efficient governance means understanding how well the controls are implemented and maintained on a routine basis. This means, cybersecurity is taking a big step forward and security leaders will have a completely new way of doing their jobs.

How does this translate to practice?

Until now, it's been like buying all the ingredients for a delicious cake but not taking charge of making one. The ingredients were left in the cupboard, some used, some not, some redundant, some expired, with no oversight as to what was needed, how they were ultimately used and if the cake, in the end, was good or not.

In security terms, this means the CISO's office procures all the needed controls such as endpoint protection tools or code protection, but the security leadership doesn't have the ability to understand if they have been implemented, and if they have – how well they are working. That's because more often than not, today's security teams have no visibility into how their policies are being enforced. They have no way to measure their activation (have they been deployed?), their scan cycles (at what pace are they working?) and whether critical events are resolved (how well are they performing against our policy?).

The ability for a CISO or a security leader to govern, manage, and measure how their operations are performing is getting bigger and top of mind. Finally, the industry is recognizing that CISOs do not have the tools they need in order to do the management part of their job.

There are many drivers for this, beginning with the complexity of their operations. Every company that needs to be compliant with SoC2/type is likely to manage at least 15 different security tools. The stack can reach over 100 tools when it comes to major enterprises. Even mid-size companies that might have gone through an M&A process are likely to have a few dozens of segregated tools.

Secondly, accountability is on the rise for the CISO and with it new liabilities and expectations. In May 2023, Uber's CISO Joe Sullivan became the first CISO to be convicted for a US company breach and a new definition of accountability unsettled the CISO community. Six months later the Solarwinds CISO was convicted of fraud, accused of failing to implement adequate security controls, among other things.

And lastly, new technologies around security data consolidation for management purposes are introducing the pathway for data-driven insights and therefore data-driven security leadership.

I believe the NIST CSF 2.0's new govern function will further foster a new data-driven security management approach that entails several key and practical changes:

- Transparency to the operational tools – whereas an ops leader or an analyst looks inwards to remediating an event or a vulnerability, security leaders ask themselves several different questions. For instance: how well are the recent tools we procured enrolled, or which business unit needs my assistance to better adopt the new controls?

- Multi-disciplinary mindset – today a CISO's office oversees between 10 to 14 different security programs, each one with very distinctive languages, capabilities and measurements that are led by dedicated SMEs. In the CISO's office, one needs to adopt simple and clear language, measurements and policies that would be agnostic to the tools, easy to comprehend, and offer a clear understanding of what the needed action items are when the security policies aren't met.

- Eye on ROI – with todays' budget cuts and recession, executive boards are asking more and more questions about the significant investment going into the security field. For most laymen, there's absolutely no way to understand the nuances among the dozens of security tools. This is when the CISO's office needs to adopt a simple way to translate their cumbersome stack to the board and reflect the security gaps in a way that will help the board understand why following the previous quarter's budget increase, there's still further need for investment.

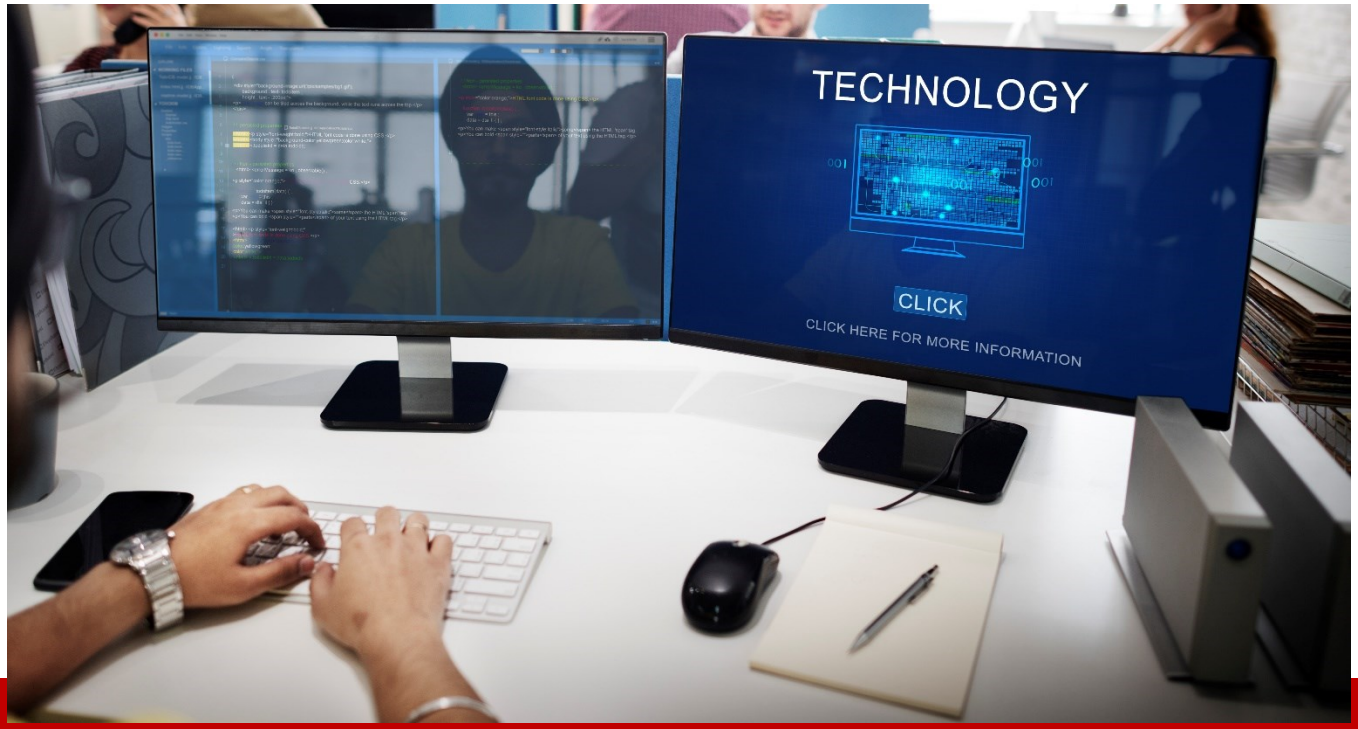
- Effectiveness of policy enforcement – It's one thing to work hard towards improving performance but it's a whole other thing to not even be aware of how the policies the CISO has set are trending. Adopting a simple, continuous view into this is the first step for much stronger governance.

To sum it up, the official addition of "govern" into the NIST framework is a great opportunity for the CISO offices to upgrade the way they lead.

About the Author

Shirley Salzman, CEO and Co-Founder of SeeMetrics, a Cybersecurity Performance Management (CPM) platform that transforms the way security leaders measure, track, and improve stack performance. Unlike today's manual processes, SeeMetrics' cockpit-like dashboard instantly answers key questions around performance. Shirley brings over a decade of experience in commercial leadership (Percepto, Contguard, and Logic Industries). Prior to her high-tech career, Shirley worked for global policy and strategy firms such as the German Marshall Fund of the U.S. and the Institute for Policy and Strategy at the Interdisciplinary Center, Herzliya, Israel. Shirley holds an MA with honors in International Security and Non-Proliferation from King's College, London.

Shirley can be reached online at shirley@seemetrics.com and at our company website https://seemetrics.co/



Cybersecurity or Cyber Resilience: Which Matters More?

Planning Beyond an Enterprise Security Posture and Toward Reliable Business Continuity

By Amanda Satterwhite, Managing Director of Cyber Growth & Strategy, Accenture Federal Services

Cybercrimes in the United States have resulted in hundreds of billions of dollars in losses. The threats are expanding exponentially endangering our national and economic security.

With off-the-shelf malware readily available, minimal expense and effort is needed for nation-state actors and cyber criminals to disrupt governmental operations for financial and political gain. The rise of AI-based attack vectors has only complicated federal agencies' efforts to safeguard critical systems.

In this ever-challenging 'new normal', the federal government needs more than cybersecurity. Cyber resilience is now also essential. What's more, of the two, resilience may ultimately prove more important.

Cyber resilience ensures that an enterprise can not only adapt to and recover from *known* threats and vulnerabilities, but can also anticipate, withstand, and recover from an evolving array of threats, attacks, and vulnerabilities borne out of emerging technologies.

Why Cyber Resilience Matters

A cyber resilience mindset recognizes that no cybersecurity solution is perfect — that even the best cybersecurity tools and strategies cannot protect against every form of cyber threat. For every new defensive strategy, a new attack vector emerges. CISOs and their teams can (and must) engage in what amounts to an endless game of whack-a-mole. You can't win outright, but neither can you afford to lose.

Recognizing these limitations, cyber resilience strategies deliver robust mitigation plans in the face of these ever-evolving threats. They focus on supporting the continuity of operations, as well as the ability to "return to normal" following an attack.

As federal agencies pursue their modernization goals, a proactive emphasis on cyber resilience ensures they can evolve their defenses as new technologies emerge. Resilience recognizes that there will be new attack vectors as technology evolves, and that incident response and remediation capabilities can and must be able to adapt.

To create a powerful cyber resilience strategy, CISOs and their teams need to develop a risk-based strategy, one that is integrated with the organization's cybersecurity plans and that supports the ability to identify, protect, detect, respond, and recover. This includes developing detailed incident response, business continuity, and disaster recovery sub-plans and processes.

Why Cyber Resilience Complements Cybersecurity

Cyber resilience should be used in conjunction with fundamental cybersecurity practices.

A strong cybersecurity program deploys the right mix of policies and tools to protect organizations from data breaches, exploited vulnerabilities, malware attacks, and insider threats, as well as phishing attacks that could escalate into ransomware attacks. These will likely include intrusion detection systems, threat monitoring and log collection platforms, end point detection, SIEMs, firewalls, and data loss prevention.

Cyber resilience complements these strategies. With attack simulations, adaptive detection and response, crisis response, and threat intelligence, resilience tools and strategies enable organizations to recover swiftly from a cyberattack. They empower agencies to restore data and systems to their previous state, minimizing the impact of an attack on business operations.

For those already familiar with cyber resilience, there's a common misconception that cybersecurity planning and cyber resilience planning are mutually exclusive. In fact, they are two sides of the same coin. Cyber plans should look to apply both security measures *and* cyber resilience for the most effective overall security posture.

Some may erroneously believe that traditional backup solutions are all that's needed to ensure mission resilience. In fact, while these solutions might be adequate for restoring data in the event of hardware failure or accidental deletion, they're not designed to ensure full recovery from cyberattacks.

For federal agencies to truly ensure mission success in the face of near constant threats, cyber resilience, or a comprehensive approach to restoring and maintaining operations following a cyberattack, is critical.

Why Cyber Resilience Aligns with Zero Trust

Federal agencies are leaning hard toward adopting Zero Trust security architectures under mandate to do so from the President's 2021 Executive Order on Improving the Nation's Cybersecurity, as well as other guidance. They also *need* to do so, as Zero Trust is proving a robust means of keeping cyber-attackers at bay.

When it comes to cyber resilience, adopting a Zero Trust mentality and architecture is an excellent place to start. Zero Trust assumes that access and networking within an organization can never be trusted. It calls for users, devices, and systems to be authenticated first before connecting, and then re-verified at multiple points before accessing networks, systems, and data.

For those transitioning to a Zero Trust architecture, CISA's Zero Trust Maturity Model offers a framework of five foundational pillars covering: Identity (and access), Devices (e.g., Bring Your Own Device policies), Networks, Applications, and Data. It then builds in Governance and Analytics, to help measure, monitor, and develop automations to assist with fatigue and mistakes that result from manual updates.

This level of cybersecurity in turn gives a firm grounding to cyber resilience, by preventing many of the most common attacks before they can infiltrate or impact critical data and systems. Again: cyber security and cyber resilience go hand in hand.

As the federal government pursues Zero Trust goals, it should view this effort as a foundation for an expanded view of what security entails. Zero Trust is the bedrock upon which to move beyond mere defense and to layer in cyber resilience so agencies can meet the main objective of security: operational continuity.

Like cybersecurity, cyber resilience is a means to an end. Both look to safeguard critical data and systems, but cyber resilience takes it one step further. Recognizing that even the best defenses can be breached, cyber resilience looks to ensure that agencies can continue to meet the needs of citizens and stakeholders, uphold national security, and accomplish the myriad other vital tasks of government, regardless of what the bad actors may try next.

About the Author

Amanda Satterwhite, Managing Director of Cyber Growth & Strategy at Accenture Federal Services, is responsible for growth, innovation, and go-to-market strategy. Satterwhite leads cyber mission and enablement for the company's National Security Portfolio, managing a team responsible for creating cutting-edge solutions for national security missions.

Amanda can be reached online at https://www.linkedin.com/in/mandysatterwhite and via the company website https://www.accenture.com/us-en/industries/afs-index

A Consolidated Approach to Fraud: Bringing Together Risk Insights, Organizations and Technology

By Kimberly Sutherland, vice president, fraud and identity strategy, LexisNexis® Risk Solutions

Digital fraud has seen a substantial increase in recent years, mainly due to the sharp rise in digital transactions. The proliferation of various digital channels and payment formats, including those employed for in-store purchases as consumers return to physical shopping locations, has provided added convenience for consumers and enhanced flexibility for businesses.

Nevertheless, fraudsters are keeping pace and have devised new methods to target both consumers and businesses with progressively sophisticated fraud attacks. Their operations have evolved into intricate networks, where every piece of information is interconnected, forming a valuable link in a vast global chain.

To effectively counter fraud, businesses need to gain a deep understanding of their trusted customers. This empowers organizations to enhance the digital experience for legitimate customers while focusing their efforts on scrutinizing other activities to spot potential attacks. Achieving this goal entails augmenting fraud intelligence by developing a comprehensive perspective of each customer's journey and fostering collaboration and information exchange with other entities.

360-Degree View of Your Digital Customer Base

A 360-degree view requires gaining a comprehensive and holistic understanding of customers by incorporating risk insights from various touchpoints throughout their digital interactions with a business. The objective is to seamlessly integrate and analyze seemingly disparate information from diverse sources to construct a unified customer profile. This includes information gathered from websites, mobile apps, social media, email communications, customer support interactions, online purchases and other digital channels.

As an illustration, financial institutions often draw a distinction between digital banking risk and Card-Not-Present (CNP) transaction risk assessments, even though there is no inherent necessity for this differentiation.

According to findings from the LexisNexis Risk Solutions Cybercrime Report, an average of 82% of consumers who engage in online shopping with their credit cards are also active users of online banking services provided by the same bank. This presents an opportunity to share digital identity intelligence seamlessly across channels, fostering trust and preventing more intricate forms of fraud.

Consequently, this approach enables a comprehensive understanding of each customer's interactions, preferences and behaviors, irrespective of the channel they choose.

Ensuring precision in the digital intelligence gathered from these diverse channels is paramount. This involves seamless integration of information collected from each touchpoint rather than compartmentalizing it within disparate systems. In the realm of ecommerce, this also entails leveraging the same digital intelligence for risk assessments across digital channels and extending its use to physical stores where customers can access digital payment methods via an app.

The real-time amalgamation of offline and online insights can prove instrumental in identifying potential attacks during their nascent stages, enabling swift responses. Furthermore, organizations should transition from single, point-in-time risk assessments to developing risk profiles that encompass all three pivotal stages of a customer's lifecycle, including new account creations, logins and payments.

Crafting a comprehensive customer profile serves as a deterrent to fraudsters seeking to exploit vulnerabilities through multi-channel attacks. For example, delivering a real-time, in-app message to the end-user or customer can confirm an unusual payment, verify that no coercion is involved and facilitate a final sanity check to thwart attacks. By maintaining a holistic perspective on customer interactions, businesses gain the ability to detect potentially fraudulent behavior in its infancy at every juncture of the customer's journey.

Collaboration and Information Sharing

Fraudsters frequently set their sights on multiple organizations at the same time and their activities can extend across various industries and sectors. To counter this threat effectively, organizations can engage in collaboration and information-sharing among themselves, exchanging insights regarding known fraudsters, attack patterns and emerging threats.

By uniting risk insights through a consortium, organizations and technology, businesses can establish a stronger defense against fraudulent activities. Integrating insights from diverse sources and organizations facilitates the development of a cohesive fraud detection system. This approach empowers businesses to scrutinize risk signals from numerous touchpoints to uncover fraudulent activities that might otherwise elude detection when analyzed in isolation.

The prompt exchange of risk intelligence plays a pivotal role in swiftly detecting and responding to fraud. Leveraging technology to enable real-time sharing empowers organizations to take immediate actions against potential threats, minimizing the impact of fraudulent activities.

Advanced machine learning algorithms and artificial intelligence-powered models continually evolve by learning and adapting to new fraud tactics in real time. The challenge frequently centers on guaranteeing the availability of all signals throughout the user journey within the same system as the fraud detection models, while also ensuring access to consortium intelligence. Only through this integrated approach can these features collaboratively function, with appropriate weightage assigned to each, without adversely affecting genuine customers.

The heightened attack rates we observe at present are unlikely to diminish, although investments in public education regarding the risks of scams, increased regulatory oversight, and ongoing technical innovation hold the promise of stabilizing these attack levels, potentially leading to a plateau.

The challenge facing organizations, industries and the U.S. financial ecosystem lies in the ability to seamlessly integrate digital intelligence. This involves identifying interconnected signals within the intricate web of a complex fraud attack as it unfolds, comprehending the behavioral anomalies it unveils and tracing the subsequent financial transactions.

The encouraging news is that there are already instances of success, including machine learning-optimized scam detection models achieving high detection rates, organizations collaborating to share real-time intelligence to prevent repeated attacks by organized fraud rings and the apprehension of mule herders leading to the closure of mule accounts. However, it is imperative to expedite these initiatives and actively engage in the battle against cybercriminals.

About the Author

Kimberly Sutherland is vice president of fraud and identity strategy at LexisNexis® Risk Solutions. Based in Alpharetta, Georgia, she leads the commercial market strategy for consumer fraud analytics, identity verification, authentication and fraud investigations for LexisNexis Risk Solutions in the U.S. and Canada.

Sutherland has more than 20 years of experience leading business strategy and product management with responsibilities spanning from building global professional services practices to developing cross-industry best practices and technical standards.

Sutherland was recognized as one of the Top 100 World Leaders in Identity and served as the past Plenary Chair of the Identity Ecosystem Steering Group (IDESG), a White House initiative under President Obama to improve the trust and security when transacting online. Sutherland also serves as the vice chair of the Open Identity Exchange (OIX) and on the boards of Women in Identity and the University of Texas – Center for Identity. Recently Sutherland was recognized as one of the Top 50 Women in SaaS by The Software Group and Cybersecurity Woman of the Year in North America by the Cybersecurity Excellence Awards.

Sutherland is a graduate of Vanderbilt University and Otterbein University.

Fortifying Digital Health Against Cyber Attacks

By Nissim Ben-Saadon, Director of Innovation, CYREBRO

In today's digital era, the healthcare industry stands at the forefront of technological adoption, heavily relying on digital systems such as Electronic Health Records (EHRs) to enhance patient care and operational efficiency. This rapid digitization has also escalated the industry's vulnerability to cyber threats, posing significant risks to patient privacy, data security, and overall healthcare delivery.

The Attractiveness of Healthcare Data to Cybercriminals

Healthcare organizations are treasure troves of sensitive data, including patient records, medical histories, and financial information. This makes them ideal targets for cybercriminals who exploit vulnerabilities to gain unauthorized access, often holding this valuable data for ransom. The consequences of a successful cyberattack in healthcare are multifaceted, ranging from compromised patient care and damaged reputations to financial losses and legal repercussions.

In 2023, the healthcare sector experienced a significant escalation in cyberattacks. Since the start of the year, 327 data breaches have been reported to the US Department of Health and Human Services' Office

for Civil Rights. That figure is up more than 104% from 160 breaches as of mid-2022 and shows “no signs of abating,” according to a report from Fortified Health Security.

The breach of Fortra's GoAnywhere secure file transfer software in February 2023 was particularly severe, affecting over 5 million healthcare records. Additionally, healthcare business associates, who play a vital role in the healthcare ecosystem, have also become increasingly targeted, with reported breaches jumping from 22 to 82, a 273% increase compared to the previous year.

HIPAA and GDPR: A Shield Yet Insufficient

To counter these risks, the U.S. healthcare industry adheres to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which governs the security of electronically protected health information (ePHI). HIPAA's key components include the Security Rule, the Privacy Rule, and the Breach Notification Rule. The European healthcare industry is protected by GDPR which provides safeguards for personal health data.

Despite these rigorous regulations, the healthcare sector has witnessed an increase in cyberattacks. The dependence on interconnected systems and IoT devices, alongside the critical nature of healthcare services, makes these institutions particularly vulnerable. The NIS2 Directive in Europe, which is set to take effect in October 2024, will mandate that healthcare organizations protect patient data from cyber threats to help address these issues. This includes implementing cyber risk management measures, establishing a clear incident-reporting process and securing patient data with proper storage and handling practices.

The Rising Menace of Ransomware Attacks

Ransomware attacks in particular, where cybercriminals encrypt critical data and systems, have become increasingly common and devastating in healthcare. In 2022, a survey by the Ponemon Institute revealed that 45% of healthcare IT professionals reported ransomware attacks impacting patient care. A striking example of the vulnerability of healthcare systems to cyber threats occurred in 2023, when Prospect Medical Holdings, a healthcare system operating 16 hospitals and over 165 clinics and outpatient centers across Connecticut, Pennsylvania, Rhode Island, and Southern California, fell victim to a ransomware attack. This cyberattack forced the closure of some facilities and left others relying on paper records, significantly disrupting healthcare services.

Proactive Measures for Enhanced Cybersecurity

Given these challenges, healthcare organizations need to take a proactive and comprehensive approach to cybersecurity. Despite huge advances in medical technology, limited budgets and a hesitancy to learn new systems means that not every aspect of the healthcare industry has kept pace. It’s critical for hospitals using techniques that still release system updates to keep all software equipped with the most recent version. This measure keeps systems reasonably secure but eventually vendors will stop providing updates as the software moves into “end-of-life” status.

Cyberattacks can be better minimized by adding extra layers of security. If a system is compromised, a multi-factor authentication (MFA) solution can help limit the lateral movement of an attacker through the network since they can't log in to other protected systems. Other key strategies include disconnecting legacy systems from the internet, and implementing advanced security solutions like Endpoint Detection and Response (EDR). Additionally, healthcare providers should conduct regular risk assessments to identify and address vulnerabilities in their systems and networks. Employee training and awareness programs are also crucial, as human error can often lead to security breaches. Educating staff on recognizing phishing attempts and safe data handling practices can significantly reduce the risk of a successful cyberattack.

Building a Resilient Cyber Defense Infrastructure

Healthcare organizations can further strengthen their cyber defenses by establishing strict access controls and ensuring that only authorized personnel have access to sensitive data. Implementing a strong password policy and using encryption for data at rest and in transit are essential steps in protecting patient information. Regularly backing up critical data and having a robust disaster recovery plan can ensure continuity of operations in the event of an attack. In addition, collaborating with cybersecurity experts and investing in state-of-the-art security technologies can provide healthcare organizations with the tools and insights needed to stay ahead of evolving cyber threats.

A Call to Action for Robust Cyber Defense

As the healthcare sector continues to embrace digital solutions, the importance of robust cybersecurity measures cannot be overstated. The industry must prioritize investment in cybersecurity to protect against the evolving threat landscape. By implementing comprehensive security strategies, healthcare organizations can safeguard sensitive patient data, ensure operational resilience, and maintain the trust of those they serve. This commitment to cybersecurity is not just a regulatory compliance issue but a fundamental aspect of providing safe and reliable healthcare in the digital age.

About the Author

Nissim has over 10 years' experience serving in a variety of cybersecurity functions including being a CISO, and providing DFIR, malware analysis and SIEM professional services for private companies, military organizations and government. He also occasionally creates and teaches cybersecurity courses for professionals. He currently serves as CYREBRO's Director of Innovation. Nissim can be reach via LinkedIn at https://www.linkedin.com/in/nissim-ben-saadon-0ba173bb/ and at CYREBRO via www.cyrebro.io.

6 Factors to Consider When Choosing a SIEM Solution

Don't Settle for Less | Make an Informed Decision

By Krunal Mendapara, Chief Technology Officer, Sattrix Group

In today's world, cyber threats are more rampant than ever before. It's no wonder that organizations are looking for ways to monitor their network activity for any signs of malicious activity. And here is where Security Information and Event Management (SIEM) solutions come into play.

SIEM solutions offer a great way to detect security threats in real-time, which is why they have become an indispensable component of any modern security strategy. However, finding the right SIEM solution for your business can be a bit of an overwhelming task. There are so many factors to consider, including the size of your organization, the complexity of your network, your budget, and your specific security needs.

To select the perfect SIEM solution for your business, it is essential to have a clear understanding of your specific needs. To ensure you choose the right one, consider the following factors:

- Determine the size of your business

- Identify the specific type of data you need to collect and monitor

- Determine the level of security you require

- Evaluate your budget to ensure you stay within your means.

Once you have a solid grasp of your specific needs, you can begin exploring a range of Security Information & Event Management (SIEM) solutions and compare them side-by-side. With a plethora of options available on the market, it is imperative to take your time to find the SIEM solution that is the perfect fit for you.

Are you looking for the best SIEM (Security Information and Event Management) solution for your organization? There are several factors to consider when making your choice:

1. Ease of Use: When choosing a SIEM solution, ease of use is essential. A user-friendly UI can save you time and resources and help your team monitor and identify security incidents quickly. Look for a cybersecurity tool that is easy to set up and use.

2. Scalability: As your business grows, you need a SIEM solution that can keep up. Make sure the security tool you choose can handle more data and users as your organization expands. Scalability is critical to ensure that the tool can keep up with the growth of the business.

3. Log Management: Your SIEM solution should be able to collect diverse logs from various sources, store them in one place, and handle the data based on your team's requirements. This helps ensure that your team can analyze the data efficiently and effectively. With proper log management, you can identify potential security incidents quickly.

4. Correlation of Security Incidents: A good SIEM solution should be capable of correlating security events and identifying threats based on the provided correlation equations. This enables the tool to identify serious attacks early on and issue high-level warnings. Correlation of security incidents is essential to ensure that your team can take swift action against potential threats.

5. Timely Detection: Cybersecurity is critical, and any downtime can cause harm to your business's reputation and revenue. Thus, timely detection of security incidents is crucial. Choose a SIEM solution that delivers prompt detection and response and helps keep the potential damage caused by threats at a minimum. The tool should be able to detect security incidents quickly and enable your team to take swift action.

6. Event and Activity Tracking: Your SIEM solution should identify addresses, behavior, and websites related to malicious attacks and dangerous third parties. The tool should provide accurate and up-to-date information to help your team prevent attacks and damage to your organization's system. Event and

activity tracking is a critical component of the SIEM solution you choose to ensure that your team can monitor and identify potential threats effectively.

Conclusion

In conclusion, selecting the right SIEM solution for your business can be a daunting task. However, by understanding your specific needs and evaluating the factors listed above, you can make an informed decision. Remember that the ideal SIEM solution should be easy to use, scalable, have robust log management, correlate security incidents, detect threats in a timely manner, and track events and activities. By finding the right SIEM solution that meets your needs, you can enhance your organization's security posture and better protect against cyber threats.

About the Author

I am Krunal Mendapara, the CTO at Sattrix Group, and I have over a decade of experience in the field. Over the years, I have played various roles, such as Security Consultant and Solution Architect. Presently, I lead the development of cutting-edge security solutions to safeguard our clients' environments against advanced security threats. Additionally, I have been instrumental in introducing advanced analytics software to our company. My expertise and leadership have been critical in shaping Sattrix and ensuring that we stay ahead of the curve in cybersecurity. I can be reached at Krunal.mendapara@sattrix.com. Also, please visit https://www.newevol.io.

NewEvol's SIEM solution offers advanced security analytics for rapid threat detection and response, all within a single, integrated platform. Partner with NewEvol for a customizable SIEM solution.

2024: The Year of Secure Design

By Stephen de Vries, CEO, IriusRisk

In 2023, we saw governments and global cybersecurity agencies begin to put the building blocks in place for secure design and take cyber defense to the software and system vendors. The US took significant strides in developing legislation and guidance for software manufacturers, and across Europe we saw further tightening on cybersecurity requirements for all hardware and software products with the Cyber Resilience Act.

This year it is about action. In 2024, organizations need to respond to the guidance and regulations and ensure the implementation of security by design in software development and architecture to protect against the cyber threat.

It is vital that cybersecurity professionals understand how to implement security by design and how to approach some of the organizational challenges they may need to overcome. But before we examine what businesses need to do, let's remind ourselves of what was introduced.

A changing regulatory landscape

The US took the lead and introduced the National Cyber Security Strategy in March 2023 which committed to developing legislation to make software developers liable for security. This was followed by the QUAD nations (Australia, India, Japan and the United States) releasing the "Joint Principles for Secure Software" which included an agreement to require security-by-design within government software procurement rules.

Later in the year, the White House published its Implementation Plan for the National Cyber Security Strategy which put in place a public-private partnership to drive the development and adoption of software that is secure-by-design and default. CISA also published recommendations on how software manufacturers can implement secure design.

This raft of regulation and guidance in 2023 clearly set out the direction of travel for governments and legislators; the future is security built right into the design of systems themselves, rather than added after the fact.

So, what is security-by-design and how can organizations begin to put it into practice?

Secure Design and Threat Modeling

To create software that is secure-by-design, we need to identify threats to the security of the data and assets, and assess and mitigate the risks before we begin building the software.

No software manufacturer sets out to build software that is insecure. But the reality is that developers are incentivized to get software to market as quickly as possible and worry about security later. However, trying to fix flaws after software has been built is both time consuming and expensive. So we need to tackle this issue from the very beginning before a single line of code is written. Threat modeling is how we do this.

Threat modeling is the process of analyzing software for potential threats and determining the most effective ways to mitigate them and is fundamental to secure design. Originally developed by Microsoft in 2005, the threat modeling process can easily be understood using Adam Shostack's four question framework designed to help teams build more secure systems:

1. What are we working on?
2. What can go wrong?
3. What are we going to do about it?
4. Did we do a good enough job?

In the past, threat modeling has been done on a whiteboard as a collaboration between cybersecurity teams and developers. However, at a time when organizations are building thousands of applications, this manual process of identifying threats is becoming increasingly impractical.

This is where automated threat modeling can make things easier. Developers can input the data of "what are we working on" into a tool, and then rely on automation to generate a threat model containing relevant threats ("what can go wrong") and countermeasures ("what are we going to do about it"). Hence, reducing the time and effort for security teams so they do not have to start from scratch with every new piece of software.

Implementing secure design in your organization

For it to be effective, we need developers and software architects to engage with secure design and threat modeling. However, it is not as simple as asking developers to focus more on security because they do not always have the right skills or experience to be able to identify vulnerabilities. Most developers graduate without having learnt the technical knowledge needed to build secure software or how to threat model. Whilst they are highly skilled at developing the functionality of a web application, they are not always equipped to think about how threat actors would exploit security flaws in that functionality.

As a result, in many organizations the onus falls on security teams to test software for vulnerabilities with security testing tools. The problem is they usually get involved once the software code has already been written. This is too late for designing secure software because the design flaws are already embedded at this stage.

Instead security and developer teams must work together collaboratively from the very beginning of the software development process in order to develop software more efficiently and safely. Only then can software flaws be identified and mitigated before software is built.

Unfortunately, we often see a lack of clarity over responsibility for security by design meaning that it can fall through the cracks. This is when senior leaders need to get involved to ensure threat modeling is prioritized as a strategically important activity. If the raft of rules and regulations coming out of government isn't enough for senior leaders to take note, then nothing will be.

A rapidly changing environment

Within a year we have seen a vast amount of regulation and guidance around cybersecurity and how organizations can protect themselves against cyber attacks and threats. Not only in the US, but globally.

Add into the mix the emergence of new technology, such as machine learning and artificial intelligence, which is already having a significant impact on the cyber threat landscape – and it becomes more important to ensure security is prioritized from the start of the development process.

This is the year for organizations to take action and get ahead of this to implement secure design and threat modeling into software development from the early stages. It is more important than ever for businesses to be on the front foot, otherwise they will get left behind.

About the Author

Stephen de Vries is the Co-Founder and CEO at IriusRisk. He started his career as a C, C++ and Java developer, before moving into software security. He's an active contributor to a number of OWASP projects and has helped FTSE 100 companies to build security into their development processes through threat modeling and integrated security testing. Stephen can be reached online at linkedin.com/in/stephen-de-vries-4185a8 and on our company website https://www.iriusrisk.com/.

A Transformative Landscape in Legal Technology: From the Past to AI-Powered Future

By Rob Scott, Chief Innovator – Monjur

The modern digital era, ripe with unparalleled technological evolutions, is remolding our perceptions and expectations at a pace once thought inconceivable. Among all the sectors witnessing this metamorphosis, the legal sector, long viewed as the stronghold of traditionalism, is both an architect and subject of these groundbreaking shifts.

Historical Technological Transformations in Legal Services

The journey of technology integration in the legal sector is an interesting tapestry of innovations. From the days of typewriters and fax machines to the emergence of the internet, electronic databases, and now AI and machine learning, each phase has progressively facilitated better service delivery. While earlier adaptations improved the speed and accuracy of legal tasks, AI stands to be the game changer, bringing intelligent automation, predictive analysis, and unprecedented efficiency to legal processes.

Digital Transformation and Legal Services Today

Gone are the days of purely paper-based processes and face-to-face consultations. Cloud computing, artificial intelligence, and machine learning now underpin legal research, document analysis, and grant remote access to vital case files, ensuring efficiency and matching the evolving client expectations for transparency, security, and promptness.

One powerful way in which artificial intelligence models have been used in the legal industry is to power e-discovery platforms. It's worth noting that some of the most recognized and frequently used e-discovery platforms — like Relativity and LexisNexis — have long used AI to power some of their functions. However, SaaS options have arisen that use artificial intelligence for purposes like document reviews and legal research.

Like professionals in many industries, lawyers can also train widely available AI platforms to better fit their needs. For example, lawyers can use large language models to analyze an agreement against a template in a faster amount of time, allowing them to handle more volume. Although it is still important for a trained legal expert to be involved — both to formulate the criteria upon which the AI will analyze a document, and to advise their clients on the anomaly the AI detects.

Embracing Responsible AI in Legal

However, the integration of AI in legal processes brings forth considerations beyond mere efficiency. Responsible AI — an emerging paradigm — insists on AI being transparent, accountable, ethical, and user-centric. For legal professionals, this means ensuring that AI tools are transparent in their decision-making, are held accountable for predictions or suggestions, are employed ethically, and finally, are always used in the best interest of clients.

Transparency is an essential facet of a responsible AI system. Particularly for use cases involving sensitive data — which is always the case in the legal profession — it is essential that AI platforms are transparent with their terms of use (and that lawyers are diligent in reading them) to ensure that the data fed into the model is secure and used only as intended. This level of transparency will ensure that the correct party is held accountable if there is abuse or misuse.

Lawyers must also understand the ethical implications of AI use in their occupation. For one, there are several regulations that lawyers will be expected to follow at both the state and federal levels, as well as additional compliance policies that should be put in place for user and client security at the firm level. Beyond that, lawyers should also understand the obligation they have to their clients to provide competent service. If they use AI responsibly — as a tool to improve their efficiency and quality of output — they are fulfilling this obligation. However, if it is applied irresponsibly, without the proper checks and balances, it could hurt the client.

One thing about the use of generative AI in the legal field that virtually any lawyer will tell you is that these models are prone to mistakes. However, when dealing with technically complex information — such as

that explored in the legal field — unless one is an expert themselves, it is virtually impossible to recognize these errors. Thus, human oversight is not only advisable, but necessary to responsibly integrate artificial intelligence into your legal practice.

International, Federal, and State Regulatory Challenges

The rampant deployment of AI technologies inevitably brushes against various regulatory frameworks. From General Data Protection Regulation (GDPR) in Europe to the California Consumer Privacy Act (CCPA) in the U.S., legal professionals must navigate a labyrinth of regulations when employing AI, especially concerning data privacy and protection. These laws not only have implications for how firms handle client data, but also dictate how AI tools, which inherently rely on vast datasets, are developed and refined.

For example, the European Union is becoming one of the first major jurisdictions to implement a clear, comprehensive regulatory framework for the use of AI. This law, set to take effect in the spring of 2024, classifies AI systems and imposes appropriate associated safeguards — essentially creating different rules for different risk levels. The goal of laws like this is to allow industries to take advantage of the numerous benefits of artificial intelligence without endangering the safety of consumers.

Reimagining the Image of Legal Professionals

A common sentiment resonates among many small business owners is that legal services are often too complex and too expensive. Emerging legal technology, especially SaaS-enabled platforms have the potential to transform the narrative. By making legal processes more intuitive, transparent, and user-friendly, these platforms can elevate the image of the profession. Early adopters are likely to witness improved client satisfaction and loyalty.

The conjunction of advanced platforms, efficient utilization of intellectual property, and the adoption of long-term subscription models marks the onset of a redefined era in legal services. This era beckons not just enhanced value creation and client engagement, but also a holistic reimagination of service delivery.

As we stride forward, embracing this transformation is more than a mere survival strategy. It's the roadmap to pioneering innovations and establishing unparalleled benchmarks for future legal mavens.

About the Author

Robert Scott is Chief Innovator at Monjur. He provides a cloud-enabled, AI-powered legal services platform allowing law firms to offer long-term recurring revenue services and unlock the potential of their legal templates and other firm IP. redefines legal services in managed services and cloud law. Recognized as Technology Lawyer of the Year, he has led strategic IT matters for major corporations, specializing in cloud transactions, data privacy, and cybersecurity. He has an AV Rating from Martindale Hubbell, is licensed in Texas, and actively contributes through the MSP Zone podcast and industry conferences. The Monjur platform was recently voted Best New Solution by ChannelPro SMB Forum. As a trusted advisor, Robert navigates the evolving technology law landscape, delivering insights and expertise.

Robert can be reached online at https://www.linkedin.com/company/monjur/ and at our company website https://monjur.com/

The Critical Role of Training and Phishing Testing in Safeguarding Financial Data

Empowering the Human Firewall: The Bedrock of Cyber Defense

By Michael Cocanower, CEO, AdviserCyber

The Evolving Cybersecurity Landscape for RIAs and Professionals

For Registered Investment Advisers (RIAs) and cybersecurity professionals who work in the space, navigating the ever-changing cybersecurity landscape is a continuous and evolving journey. One that is set to become even more complex with the impending SEC cybersecurity regulations.

These evolving regulations stress the need for continuous cybersecurity education including regular testing of security protocols. Such a commitment is crucial not only for compliance but also for embedding deep cybersecurity awareness within the very fabric of an organization's operations. Greater education of cybersecurity complexity will not only reduce the likelihood of external threats, but will also allow

workforces to recognize internal threats, such as employee negligence and use of unauthorized devices or software.

The key to all of this education is proactivity. Don't wait until you've experienced some sort of breach. In this article, I'll explore strategies and approaches that align with both existing and proposed SEC regulations.

Transforming Cybersecurity Challenges into Educational Opportunities

Proofpoint's 2023 State of the Phish Report revealed that 84% of organizations experienced at least one successful phishing attack in 2022, highlighting the critical need for improved cybersecurity measures. In response to this growing threat and under proposed regulation from the SEC regarding reporting, RIAs may be required to disclose any breaches in security. To avoid potential reputation damage from a breach disclosure and ensure compliance, organizations must develop comprehensive training programs and adopt a robust approach to cybersecurity training and phishing testing, which will better prepare them to protect against increasingly sophisticated cyber threats.

What does this look like in practice? It requires a significant shift in perspective on how cybersecurity challenges, such as encountering a phishing simulation, are perceived. Instead of viewing an employee's inability to recognize a phishing simulation as a failure, it should be embraced as a valuable, interactive learning opportunity that can be shared with the entire organization so the entire team can learn how to spot similar attempts in the future.

By transforming every cybersecurity challenge into a teachable moment, RIAs create an environment where continuous learning is not just encouraged but is integral to each employee's professional development. This approach demonstrates a commitment to ongoing improvement and actively engages employees in risk management practices, emphasizing the importance of vigilance and continuous education in cybersecurity protocols.

In the dynamic world of cybersecurity, especially for RIAs and professionals in the field, cultivating a knowledgeable and adaptable workforce is just the beginning. As cyber threats evolve, so must our strategies to combat them. This means going beyond basic training to implement more proactive measures, such as regular integrated training sessions and tests. These steps are essential to ensure that teams are not only well-equipped to tackle future challenges but also remain compliant with the latest regulatory requirements. This proactive approach is crucial in addressing advanced cyber threats, such as identity impersonation and spear phishing, which leverage personal relationships and trust.

As we delve deeper into the complexities of cybersecurity, it becomes clear that a multifaceted strategy is necessary to build a resilient defense against these sophisticated threats.

Addressing Advanced Cyber Threats

Identity impersonation and spear phishing represent advanced tactics in the cybercriminal arsenal, leveraging the personal relationships and trust that form the bedrock of all businesses. In a business

context, where communications and requests from colleagues and partners are routine, attackers take advantage of this trust. With the rapid development of AI technology, cybercriminals now have an easier path to more convincing phishing attacks. Recognizing this vulnerability, regulatory bodies will require financial institutions to confidentially report significant cybersecurity incidents, underscoring the critical importance of comprehensive and ongoing training to counteract these sophisticated threats — broad educational initiatives including routine training sessions, and phishing simulation tests — are crucial in equipping employees with the skills to identify and counteract these threats, and reinforce an organization's defense against sophisticated cyber adversaries.

On top of increased educational initiatives, organizations can increase resilience against constantly evolving digital threats by nurturing a security culture dedicated to specific preventative measures like proactive identification, detailed analysis, and strategic management of cyber risks as well as adding real time detection to their arsenal. This consists of emphasizing the need to maintain detailed records of cybersecurity efforts as a critical complement to defensive measures themselves. This approach helps organizations go beyond mere compliance; they cultivate a forward-looking cybersecurity stance.

The Human Element and Measuring Training Effectiveness

The effectiveness of cybersecurity training programs can be quantified through various metrics, such as phishing click rates and the rate of training completion. These data points offer tangible evidence of a cybersecurity program's reach and immediate impact. In the realm of finance, failing to meet these metrics significantly increases the risk to financial resources. Yet, the ultimate barometer of success lies in the sustained behavioral change among employees — the kind that leads to a tangible reduction in cybersecurity risk.

To gauge behavioral change in a workforce, managers will need to regularly monitor employees' adherence to cybersecurity policies and practices over an extended period. It’s important to note that supervisors will need to strike a balance between effective observation and respecting employee privacy and maintaining a positive work environment. The objective is not to create a climate of fear but to cultivate an organizational culture deeply rooted in cybersecurity awareness.

This approach advocates for a well-informed workforce capable of contributing to the overall security posture of their organization, suggesting a blueprint for compliance and beyond. They serve to empower individuals within an organization to make informed decisions, recognize deceptive tactics, and take appropriate action when faced with potential cybersecurity threats, thus taking a few more steps closer to fostering a dynamic cybersecurity culture.

Cultivating a Dynamic Cybersecurity Culture

A robust approach to cybersecurity training and phishing testing must reflect a commitment to ongoing improvement and active participation in risk management. The shift from static policies to a dynamic, culture-driven defense strategy is only possible when all members of a firm prioritize cybersecurity equally. One of the best strategies is actively managing systems and configurations, which involves

inventorying network devices and software, eliminating unnecessary components to minimize the attack surface, and continuously adapting and streamlining these elements to meet evolving security threats and enhance operational efficiency.

While embedding cybersecurity awareness internally is foundational, the complexity and sophistication of threats often necessitate leveraging external expertise to augment defenses, providing fresh insights and specialized skills that are critical for staying ahead of potential vulnerabilities.

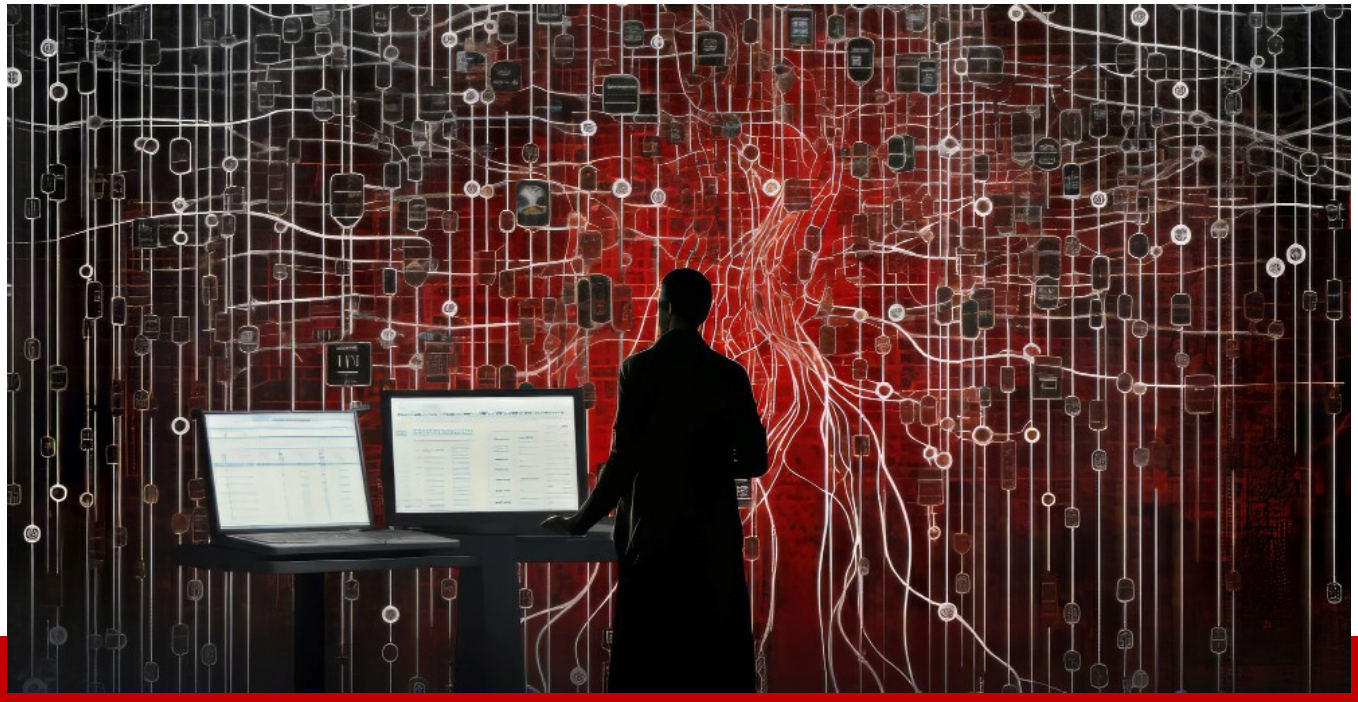
According to Mandiant's M-Trends 2023 report, 63% of organizations were notified of breaches by external entities in 2022—an increase from 47% the previous year, which means more companies are relying on external partners for cybersecurity expertise. Engaging with external cybersecurity experts allows for an impartial view and a continuously refreshed approach that matches the ever-changing landscape of cyber threats a critical consideration for sectors such as finance. These levels of vigilance and preparedness are not just about meeting compliance standards; it's about fostering a cautionary security culture that prioritizes the identification, analysis, and management of cyber risks as an integral part of business resilience.

The Cornerstone of Cyber Defense

A comprehensive suite of cybersecurity tools and compliance consulting establishes a strong defense against cyber threats. Yet, the true cornerstone lies in empowering employees through consistent training and phishing tests. Such empowerment is crucial, as it turns every team member into a vigilant guardian of the organization's digital frontiers. The SEC's evolving regulations on cybersecurity risk management underscore the critical nature of this empowerment. They serve as a reminder that while technology is a powerful ally, the human element remains irreplaceable. Strengthening this human firewall is not a one-time event but a continuous process. The ideal time to have fortified this aspect of cybersecurity was in the past, and the second-best time is now — reflecting the urgency with which the industry must adapt to the changing regulatory and cyber threat landscapes to maintain operational integrity.

About the Author

Michael Cocanower is Founder and Chief Executive Officer of AdviserCyber, a Phoenix-based cybersecurity consultancy serving Registered Investment Advisers (RIAs). A graduate of Arizona State University with degrees in finance and computer science, he has worked more than 25 years in the IT sector. Michael, a recognized author and subject matter expert, has earned certifications as both an Investment Adviser Certified Compliance Professional and as a Certified Ethical Hacker. He is frequently quoted in leading international publications and has served on the United States Board of Directors of the International Association of Microsoft Certified Partners and the International Board of the same organization for many years. He also served on the Microsoft Infrastructure Partner Advisory Council.



Anatomy Of an Endpoint Attack: How A Cyberattack Can Compromise an Enterprise Network

By Guillermo Gomez, Vice President of Endpoint Product, WatchGuard Technologies

For truly effective network security posture, it's crucial to protect all of your company's devices as cyber adversaries can turn any endpoint – phones, computers, virtual machines, embedded devices, servers, POS terminals – into an entry point into your organization. Unprotected endpoints are a leading attack vector for malicious actors, who often move from one to another until they find a way to penetrate more deeply into a network. That's why it's so critical to have visibility across all endpoints in your organization.

However, establishing this comprehensive visibility and ensuring all endpoints are protected isn't always easy. Knowing how to properly lock down the myriad devices within your company's network and maintain protection first requires knowledge of how a cyberattack typically begins and spreads through your systems. Below, we'll walk through what the stages of an endpoint attack look like and provide tips on how to stop these threats in their tracks.

The anatomy of an endpoint attack

There are countless ways for a threat actor to conduct an attack and move laterally through your network. One common method is to conduct a spam or phishing campaign sending emails with a dangerous attachment to unsuspecting users throughout an organization. An end user within your network might click on the attachment and launch an initial malware payload. If their device isn't equipped with an

endpoint security solution, that malicious element will start running. The incident might result in an infection with lesser impacts to your network. However, it is common that the malicious element is a command-and-control link to a remote cell that connects to an operator who is waiting to compromise the device. They will attempt to access the environment in which the device is running and begin analyzing your network for vulnerabilities and valuable assets.

The malicious actor will then start querying the network the same way that security professionals do to discover other devices. Attackers have grown more sophisticated; depending on their findings or how far they get in your network, they likely won't trigger many alerts nor be in a hurry to launch the attack. They'll move carefully through the network, scanning for additional devices they can access and credentials they can steal. For instance, if remote desktop protocol (RDP) services are enabled, the attacker will leverage those RDP connections with the credentials they have stolen to try accessing a different device. They will continue using different exploits to access more devices, gather more credentials and gain more knowledge about the network. If they can get the device's security domain, the adversary may sell that information via the dark web to a different threat group that may be interested in orchestrating a larger attack.

Attackers often operate unnoticed for days or weeks, waiting patiently to launch the attack until they have stolen all the data they want. Those managing the network must be aware that, if the attacker has accessed it for a while and notices the network operator is implementing additional security measures, they may immediately launch their attack while they still have access.

Increasing visibility to secure endpoints

There are several steps that security teams can take to protect their endpoints and mitigate risk, even in the event of a breach. Some best practices that teams should adopt to strengthen their network security include:

- **Establish comprehensive visibility across all endpoints.** As mentioned, an essential measure for security teams is to have extensive visibility of all endpoints. Advanced security tools with sophisticated discovery capabilities will help increase visibility by identifying those endpoints that are unprotected and inform the necessary steps for installing protection and continued monitoring. For instance, if you have a network of 100 computers and 10 are unprotected, a security tool with advanced discovery can identify all endpoints attached to the network and show which 10 remain unprotected, allowing you to manage those unmanaged endpoints

- **Employ multi-factor authentication.** Malicious actors will try various methods, including brute force attacks, to gain access to security credentials and use them throughout your network. If an attacker can steal the security administrator's credentials and log into the security product's console, they will try to uninstall or disable the security product from the admin console. Requiring multi-factor authentication (MFA) in all these critical services can prevent an attacker from disabling the security measures from the code itself. Measures like MFA can mitigate much of the risk and limit the extent of an attack.

- **Implement a vulnerability management process.** Security teams must ensure that all software being used is updated. A notable way that threat actors move laterally within a network is by exploiting known vulnerabilities in existing software. Organizations can significantly reduce their risk by implementing a vulnerability management process that is designed to regularly patch software, operating system and third-party vulnerabilities. Removing this "easy button" for attackers makes their job much harder and can prevent many common attacks from succeeding.

- **Hire a managed service provider.** Maintaining security effectively is a service. Managed service providers (MSPs) are valuable resources who can provide comprehensive, dedicated services to significantly reduce the security risks that companies face. They can manage the appropriate security configuration and operation of protected devices. The work of MSPs is critical for protecting end users.

- **Consider an MDR service.** As cyberthreats have grown increasingly complex, many organizations – especially small and midmarket companies – have come to realize that they don't have the resources or expertise to defend themselves on their own. As a result, managed detection and response (MDR) services have become increasingly popular. Consider employing an MDR service to help with providing 24/7 threat detection and response services. If your company isn't ready to go the MDR route, you should at least consider using a security solution that includes advanced security services – such as services that classify 100% of the executables, for instance – with its usage license.

An important concept to understand is that effective security requires more than a technology solution; what is needed is a combination of technology and security services managed by a team of experts. Organizations shouldn't simply deploy a security solution, they need to manage that security solution and put people in place to analyze the activity and anomalies that their security tools uncover. If your organization doesn't have a security operations team, it's probably worth subscribing to an MDR service instead of trying to do the work by yourself. Because ultimately, effective security requires constant monitoring. With the right people, products and processes, you can protect your endpoints and your entire network.

About Guillermo Gómez

Guillermo Gómez, Market Owner for Endpoint Security, is responsible for leading the evolution and success of the Endpoint product line at WatchGuard. With 25 years of experience in the Endpoint Security space. He started his career as an engineer, though he moved to management positions to initially lead Product Development and, finally, to be responsible for Product Management, Product Development, IT, and Support areas at Panda Security.

Becoming Resilient to The Cyber Incidents of Today and Tomorrow

By Theresa Le, Chief Claims Officer, Cowbell

As cyber threats escalate and evolve worldwide, businesses must ensure their foundations are solid to withstand potential cyber incidents. Developing organizational resilience involves creating an environment capable of adapting and recovering both operationally and reputationally from a cyberattack. Today, threat actors are not only refining methods to infiltrate systems through the exploitation of both technical and human vulnerabilities but also enhancing their post-infiltration strategies. This heightened sophistication requires organizations to deploy a combination of diverse protective measures and strategic partners.

The Future of Ransomware Means Evolving Threats and Increased Risks

Threat actors are becoming more sophisticated and evolving their tactics to inflict the maximum damage. Specifically, threat actors are intensifying their research efforts by delving deeper into the organizations

they target. There's been a discernible shift from focusing on the quantity of data to now focusing on the quality of stolen information. By gaining access to and extracting the most valuable information, threat actors can command higher prices for the organization's most sensitive data.

Beyond monetary extortion, tactics include public shaming on dedicated sites or within industries, or disclosing the breach to the victim's customers and business partners. The personalization of attacks has escalated, with threats extending to victims' families or a company's board of directors. Recent instances reveal threat actor groups even involving government entities, contacting regulatory bodies like the SEC. The strategies seek to exploit the victims in sometimes bespoke disruptive personal, as well as professional ways.

Additionally, threat actor groups are demonstrating collective adaptability through the utilization of impersonation tactics or by emerging as secondary actors in hijacking activities. This collective adaptability poses a significant risk, as it can result in negotiations being taken over, leading organizations to unintentionally pay the wrong entities, or be forced to pay a ransom twice. Given the 97% surge in ransomware attacks throughout 2023 compared to the previous year, as reported by BlackFrog, it is imperative to adopt a proactive and resilient approach to mitigate evolving and increasingly impactful threats.

Addressing and Overcoming Threats

Organizations must conduct a risk assessment to pinpoint vulnerabilities and take action to shape their cybersecurity strategy to achieve optimal cyber hygiene. This process offers a snapshot of an organization's current vulnerabilities and architecture, identifies any cybersecurity gaps, and then creates a strategy to address those gaps and implement measures to build resilience. Addressing identified weaknesses from these assessments is pivotal for better preparedness against potential ransomware and cyber incidents.

While cybersecurity strategies should align with an organization's risk assessment, companies can enhance their defenses by adhering to fundamental best practices. This involves adopting Multi-Factor Authentication (MFA), deploying a Managed Detection and Response e (MDR) solution, keeping up with patching, maintaining good password hygiene, and having offline, regularly tested backups of data.

Additionally, an Incident Response Plan (IRP) should be implemented to outline all the steps that organizations need to take after a cyber incident occurs. Having an IRP will significantly reduce response time and help guide businesses in times of chaos. It is important to tailor the IRP to the organization's structure and processes and test it regularly.

Utilizing a cyber insurance provider is a practical and strategic tool for cyber preparedness and response. The cyber insurance market is rapidly growing, projected to reach $29.2 billion by 2027. Cyber insurance providers are essential partners in preventing and addressing cyber incidents and ransomware attacks. They offer continuous support throughout the policy period, providing educational resources, solutions based on risk profiles, and alerts on vulnerabilities. In the event of an incident, these providers leverage their expertise to guide organizations strategically and efficiently, mitigating business interruption, liability exposure, and commercial impact.

Bringing it all Together

The cyber threat landscape is becoming more vast and dynamic every day, which presents challenges for organizations trying to keep up with best practices and trends. Staying ahead of these threats requires understanding the current landscape and adopting good cyber practices. Today, deploying smart cybersecurity strategies isn't just a good idea – it's crucial for keeping a business running smoothly and protecting its value.

About the Author

Theresa Le, Chief Claims Officer at Cowbell is well-versed thought leaders in the insurance space, and together, these ambitious women bring over 30 years of experience in claims and underwriting. Theresa's educational background in cyber law laid the groundwork for her career. Starting as a litigator, she eventually became VP at Swiss Re, as well as a Senior Claims Counsel at AXA XL. Theresa has extensive knowledge in claims, establishing robust claims strategies for companies in cyber, technology, and insurance over the past 5 years. As an established thought leader in the cyber insurance/claims space, Theresa makes it a priority to share her knowledge of the growing risks that insureds are facing as well as the steps organizations can take to recover from a cybersecurity incident. With Theresa's leadership and in-depth expertise in cyber claims, Cowbell has established a vigorous cyber claims counsel and risk engineering team focused on helping customers assess and process their claims and mitigate any exposure that was faced. For more information, please visit https://cowbell.insure/.

Best Password Generators of 2024 to Secure Your Accounts

Overview of best password generators to secure online accounts

By Mia Naumoska, CMO at Internxt

Despite the current advances in technology, one thing that has stood the test of time to protect our accounts and confidential information is passwords. When implemented correctly, strong passwords are an effective defense system to prevent hacks that can lead to data leaks, fraud, identity theft, and other devastating consequences.

Although we have several methods to log in to our accounts, including face ID, fingerprinting, and passcodes, we should not compromise on creating strong passwords to safeguard our accounts. Fortunately, we have various password generators to help us protect our accounts and practical barriers to protect our sensitive information.

But which one should you choose? We will look at five of the most popular password generators of 2024 that you can use and add additional layers of strength to your accounts.

The 5 Best Password Generators of 2024

We have compiled this list of the best password generators of 2024 that will instantly give you the characteristics of a robust password that can effectively defend against dictionary and brute force attacks. Let's take a look!

1. Best free password generator — Internxt

Internxt values the privacy of its users and provides people with secure, encrypted cloud storage to keep their confidential files safe. Internxt's mission for a safer, secure internet is reflected in its suite of free privacy tools, including a strong password generator.

Internxt's password generator covers everything you need to create a strong password instantly. Its simple interface and design allow you to generate a password or passphrase, and you can easily add or subtract

- Length
- Upper or lower cases
- Numbers or symbols
- Separate phrases with special characters

If your generated password meets the requirements, you will get visual confirmation under the password generator via five green bars. You can also use Internxt's password checker to confirm your password strength and estimate how long it would take to crack your password.

Because of Internxt's zero-knowledge approach, Internxt will never store or share your passwords, keeping your accounts safe from data breaches. So, if you want a free tool in your internet safety arsenal that's fast, easy, and secure, you can't go wrong with Internxt's free password generator.

Best password generator for shared access — Dashlane

Dashlane's password generator is part of its service as a password manager. You can store passwords using Dashlane's zero-knowledge and patented encryption service if you have numerous passwords across multiple accounts.

Dashlane's password generator is included for free in its paid plan, and you can easily change the character length up to 40 characters and include symbols or similar characters. There is also visual and written confirmation of your password strength: red shows a weak or relatively strong password, and green confirms a strong password.

If you want to use a password generator with Dashlane's other services, including its password manager and VPN, prices start at $3 for an individual premium plan. Although there is no option for a passphrase with Dashlane, it is still a great way to generate strong passwords quickly, although there is currently no option for Linux users.

Best password generator with password manager — Bitwarden

If you want a free password generator across multiple accounts, then Bitwarden's free password management tool will store your passwords securely.

Bitwarden's password generator instantly generates strong passwords up to a massive 128 characters in length, so a password manager is definitely required! You can also choose to create a passphrase, but this only has one character as an option to separate the phrases.

Furthermore, when you generate a password, Bitwarden displays an estimated time to crack feature, ranging from 10 seconds to centuries. Bitwarden offers a generous free plan to store as many passwords as you need for unlimited devices. The paid plan starts at just $10 for a year and gives you access to features such as security reports.

Suppose you use multiple passwords across different platforms. In that case, Bitwarden is also available for Windows, Mac, and Linux, and you can install the web browser extension on your preferred browser, whether it's Chrome, Tor, or DuckDuckGo.

Best password generator with antivirus — Norton

Primarily, Norton focuses on anti-virus software to protect you against malware, ransomware, and hackers. As we know, a strong password will also help prevent these attacks, so if you use Norton anti-virus exclusively on your devices, you may wish to try the Norton password generator.

Norton's password generator is the usual slider that lets you select a password from 4 - 64 characters of a mixed case, numbers, and punctuation and categorizes the generated passwords from bad, weak, to strong.

Norton's password generator is less customizable than previous options, as there is no option to choose from a passphrase. Nevertheless, if you have a Norton account, you can easily implement their tool with their antivirus service and password management tool to protect your accounts.

Best password generator for multiple platforms — Nordpass

If you work on several devices and platforms and need to manage your passwords for your business, work, or studies, you may wish to consider using Nordpass.

You can use Nordpass' password generator alongside their password management tool. From here, you can access your accounts across multiple devices with biometric authentication or by scanning a code.

Nord's easy-to-use password generator and the ease of switching from one device to another make it a good contender for the best password generator 2024 for those who live a fast-paced life and need to access their accounts quickly.

Again, however, Nordpass's options for passwordless login may not be for everyone, so if you want to stick to generated passwords only, we recommend you choose a quick and free password generator.

How to choose the best password generator in 2024

When choosing the best password generator for you, consider what other services you wish to use the generator with. This list is designed to give you a range of services that will be valuable to your internet security, so feel free to try as many as you like!

Whether you need cloud storage, antivirus, or any organizational tool, these password generators will provide you with impenetrable passwords to secure your accounts from hackers and cybercriminals for years to come.

About the Author

Mia Naumoska is a Chief Marketing Officer at Internxt - a zero-knowledge cloud storage service based on best-in-class privacy and security.

Mia can be reached online at LinkedIn and at our company website https://internxt.com/

Editor's Note: The opinions expressed in this article are solely those of the author, and should not be construed as endorsements by Cyber Defense Magazine or Cyber Defense Media Group. Readers should be aware that Cyber Defense Media Group does provide independent product reviews as a paid service.

Beyond Code: Harnessing AI for Advanced Cybersecurity Solutions

By Angel Vossough, Co-Founder & CEO of BetterAI.io

Cybersecurity defenses are shifting, aiming to predict and block cyber threats in advance, acting as digital guardians attempting to stay one step ahead. This transition toward a future where cybersecurity systems are not only reactive but predictively adaptive marks a significant change in the industry.

As someone who transitioned from a senior network engineer at Cisco supporting complex networks for many sectors such as banking, healthcare, and telecommunications to becoming the CEO of an AI company, I've seen firsthand the transformative potential of AI in revolutionizing the cybersecurity domain. This journey has not only highlighted the limitations of traditional security measures but also unveiled the path towards a more secure and intelligent digital future.

Integrating AI into cybersecurity breaks through previous limitations, offering unmatched capabilities in real-time threat detection and response. It enables systems to proactively identify and neutralize threats before they become a reality, drastically reducing the mean time to detect and resolve security breaches. This capability is not just about speed; it's the depth of analysis and the ability to learn and adapt to new threats with minimal human intervention that AI brings to the table.

AI's role in uncovering complex patterns and anomalies within vast networks demonstrates its power to cut through the noise, pinpointing threats that might otherwise go unnoticed by human analysts. From network intrusion detection and behavioral analysis to advanced malware detection, AI's role is extremely important. It extends beyond simple detection, enabling a predictive security approach that can foresee and mitigate potential vulnerabilities before they are exploited.

However, the path to harnessing AI in cybersecurity is filled with many challenges, including algorithmic biases and the continuous evolution of cyber threats. These challenges require a collaborative approach where AI's capabilities are complemented by human expertise to make sure there is a balanced and effective defense mechanism.

Real-world implementations of AI-driven cybersecurity solutions, like NVIDIA's Morpheus and SentinelOne's Purple AI, serve as benchmarks for the industry and illustrate how AI can streamline cybersecurity workflows and enhance threat detection and response.

Integrating AI into cybersecurity isn't just an upgrade; it's crucial for protecting our digital world against complex threats. This shift towards AI-powered defenses promises more intelligent and proactive security systems. These systems can predict and prevent cyber attacks before they happen, making our online spaces safer. However, embracing AI comes with many challenges, including ethical concerns and the risk of misuse. It's important for everyone involved in the cybersecurity community to work together to make sure AI is leveraged responsibly for a more secure digital future.

About the Author

Angel Vossough, CEO and Co-Founder of BetterAI, leads the creation of innovative AI solutions like “BetterMed” and “VinoVoss” (www.VinoVoss.com)—a semantic search and recommendation system creating a virtual wine sommelier. A serial entrepreneur with a deep tech background, Angel holds dual Bachelors’ in Mathematics and Computer Engineering and a Master's with honors in Software Engineering and Data Science from UC Berkeley. Angel's diverse experience includes roles at Cisco Systems, DiverseUp and Caspian Capital. Connect with Angel at www.BetterAI.io.

Bridging The Gap: Diversity Cyber Council and The Emergence of Tech as The New Opportunity Frontier

Diversity Cyber Council Initiative

By Donna Segura, Publicist: OleanderPR

In a world where technology is rapidly redefining every aspect of our lives, there's a burgeoning recognition of the need for diversity to drive innovation and resilience, particularly in the cybersecurity domain. This is where military veteran Odie Gray's brainchild, the Diversity Cyber Council (DCC), comes into play, advocating for inclusivity in tech and heralding it as the new "trap" – a term reappropriated to signify opportunity and advancement in the digital age.

Odie Gray: A Visionary for Inclusion in Cybersecurity

After serving in the military, Odie Gray transitioned to civilian life with a keen awareness of the cybersecurity threats facing our nation and the world. He also witnessed a lack of representation from

diverse backgrounds in the tech workforce. Gray's military experience, imbued with values of discipline, teamwork, and strategic acumen, uniquely positioned him to address these challenges by founding the Diversity Cyber Council.

The Mission of the Diversity Cyber Council

The DCC's mission is multifaceted, focusing on advocacy, education, networking, and research to promote diversity in tech. It aims to dismantle the barriers that have historically hindered the participation of underrepresented groups in cybersecurity roles and, by extension, the broader tech industry.

Pillars of the Diversity Cyber Council:

Advocacy: Pushing for industry-wide adoption of policies that ensure diversity and inclusion are more than buzzwords – their benchmarks for progress.

Education: Providing access to cybersecurity training and resources that empower individuals from all backgrounds to enter and excel in the tech space.

Networking: Facilitating mentorships and partnerships that nurture talent from diverse communities and foster a culture of mutual support.

Research: Investigating the systemic obstacles faced by underrepresented groups in tech and strategizing effective ways to overcome them.

Reimagining "Trap" as Opportunity: Tech as the New Pathway to Success

The term "trap" has often carried a negative connotation, suggesting a pitfall or a dead-end. However, in the context of the DCC, "trap" is being reclaimed and transformed into a symbol of opportunity and empowerment, particularly in underserved communities where access to tech careers can be life-changing.

The Tech "Trap": A Ladder to Success

Economic Empowerment: The tech industry is known for its lucrative career paths, offering financial stability and growth prospects that are unparalleled in many other sectors.

Innovative Spirit: Being at the cutting edge of technology means working on problems that have the potential to reshape the way we live and interact with the world.

Lifelong Learning: The fast-paced nature of tech demands continual skill development, ensuring that professionals are always at the forefront of knowledge and expertise.

Global Reach: Technology transcends borders, allowing for solutions that can have a worldwide impact and fostering a sense of global community.

By repurposing "trap" to mean a magnet for opportunities, the DCC stresses that the appeal of tech is not confined to monetary benefits. It represents a chance to be part of a progressive community that values each individual's potential to contribute to a more secure, innovative, and just society.

Conclusion: The Way Forward with Diversity Cyber Council

The DCC, under Odie Gray's leadership, isn't simply advocating for change; it's creating a ripple effect that promises to reshape the tech landscape. As tech becomes the new "trap," filled with possibilities, it's imperative for industry leaders to join the council's efforts, championing a future where diversity in tech is not a quota to meet but a standard to uphold.

In the end, the Diversity Cyber Council exemplifies a crucial truth: diversity is not just an ethical choice, but a strategic imperative that enriches the tech industry and strengthens its capacity to face the challenges of tomorrow. For those on the cusp of their careers, tech represents not just a job, but an alluring "trap" that promises growth, purpose, and the chance to make an indelible mark on the digital frontier.

About the Author

Donna Segura, owner of OleanderPR, is a renowned publicist with a rich background in film and music, who has expanded her influence into multiple sectors. Her firm develops cross-industry communication strategies for a wide-ranging client base, including luxury, food and beverage, agriculture, tech, and sports. She's known for her strategic partnerships with major sports leagues and her commitment to supporting her second family, the military community, showcasing her versatility and dedication to making a difference. Donna can be reached online at donna@oleanderpr.com and out her agency website https://oleanderpr.com

The author is the publicist of record for the above subject matter, where usage of Diversity Cyber Council and Tech is the New Trap images remain the property of said company and are protected by copyright laws.

Building AI on a Foundation of Open Source Requires a Fundamentally New Approach to Application Security

By Nadav Czerninski, Co-Founder and CEO, Oligo Security

AI has sprung from the pages of science fiction into our daily lives.

The AI revolution is now accelerating, enabled by open-source software (OSS) models. These models are complex packages of open-source code made specifically for developing AI, allowing organizations to deploy AI models efficiently and at scale.

While most organizations ensure that any given line of standard open-source code is checked for vulnerabilities, the larger open-source models they deploy often escape the same scrutiny.

A series of recently discovered vulnerabilities highlights how supply chain attacks can be executed through malicious OSS models. This discovery raises concerns regarding the fragility of open-source models and the security of AI systems overall, emphasizing the critical need for stringent OSS security measures amid AI's rapidly increasing popularity.

AI models and the OSS They Rely on

OSS models are the bedrock of the AI revolution. Why? Most organizations today don't build their own AI models from scratch – they increasingly rely on open-source models as foundational components in their AI initiatives. This approach expedites development, allowing rapid deployment and customization to suit specific needs.

The tradeoff for this convenience and efficiency, however, is security.

OSS packages are widely used – and attackers know it. They also know that organizations struggle to scrutinize potential vulnerabilities in code written by outside developers. The result: OSS models often introduce vulnerabilities that malicious actors can easily exploit to compromise sensitive data, decision-making processes, and overall system integrity.

AI research and solutions are still in the "move fast and break things" phase, so it's no surprise that security protocols for OSS models are still in their infancy. This is why cyber incidents like the recent Hugging Face vulnerability – where over 1500 LLM-integrated API tokens in use by more than 700 companies including Google and Microsoft became compromised – are increasing.

Ramifications of Not Securing OSS Models

Hacking into AI infrastructure gives bad actors the keys to the kingdom. Attackers can view and steal sensitive data, compromising user privacy on an unprecedented scale. They can also access, pilfer, and even delete AI models, compromising an organization's intellectual property. Perhaps most alarmingly, they can alter the results produced by an AI model.

Imagine a scenario where an individual with a persistent headache asks an AI chatbot or Large Language Model (LLM) for basic headache tips. Instead of suggesting rest or Advil, the corrupted AI advises the person to combine two OTC medications in a way that, unbeknownst to the headache sufferer, can result in toxic or fatal side effects.

Alternatively, consider an autonomous car that relies on AI for its navigation. If its AI system has been tampered with, it might misinterpret a red traffic light as green, triggering a collision. Similarly, if an auto manufacturing facility's AI quality control system is tampered with, it might falsely validate bad welds, risking driver safety and recalls.

Even in seemingly benign situations, compromised AI can be dangerous. Imagine that a user prompts an AI assistant to suggest travel tips for Italy. A compromised LLM could embed a malicious URL within its response, directing the user to a phishing site laden with malware – all disguised as a helpful travel

resource. While the would-be traveler might never realize they've enabled an exploit, the attacker can now use their new access to infect more users' computers on the network.

Proactive OSS Model security

As the risks of compromised OSS models grow, organizations must adopt a proactive stance towards fortifying their OSS model security. This calls for a multi-faceted approach that must go beyond mere reactive measures, which only come into play in the wake of security breaches.

Continuous monitoring and real-time threat detection mechanisms are key. Organizations should seek out advanced monitoring tools capable of identifying anomalies, unusual behaviors, or potential threats to open-source models in real time. AI-driven systems – fighting fire with fire – can be most effective in such cases.

Additionally, organizations should prioritize robust authentication protocols, encryption methods, and access controls to fortify the integrity of their AI infrastructure. Regular security audits, vulnerability assessments, and code reviews specifically tailored to open-source models will help identify and address potential weaknesses before they are exploited.

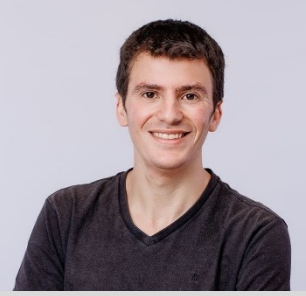
Finally, fostering a culture of organization-wide security awareness and proactive response within teams ensures that swift actions can be taken to mitigate emerging risks.

By integrating proactive security solutions that prevent, detect, and respond to threats in real time, organizations can enhance the cyber-resilience of their OSS model infrastructure and ensure that their data – and customers – stay protected from the dark side of the AI revolution.

About the Author

Nadav Czerninski is the CEO and Co-Founder of Oligo Security. With an extensive background as a senior officer in IDF Cyber and Intelligence units, Nadav's experience has propelled Oligo to the forefront of runtime application security.

Nadav can be reached online at https://www.linkedin.com/in/nadav-czerninski/ and at our company website https://www.oligo.security/



How Empathetic Leadership Can Shape the Future of Inclusion in Cybersecurity

By Lauren Neal, Founder and Chief Programme Creator, Valued at Work

In the fast-paced world of technology, the importance of inclusion cannot be overstated. The cybersecurity industry is a powerhouse of innovation, influencing every aspect of our lives. However, for innovation to truly thrive and benefit society as a whole, it must be inclusive. Enter empathetic leadership – a style of management that prioritises understanding, compassion, and inclusivity. In this article, we explore how empathetic leadership can shape the future of inclusion in cybersecurity.

The Importance of Inclusion in Cybersecurity

Inclusion isn't just a buzzword; it's a necessity. In today's world, technology touches every corner of our lives, from the way we communicate to the way we work and access information, which makes security

crucial. Tech companies have a profound influence on our society, and their products and services should reflect the diversity and needs of the global population.

Despite this, the tech industry has long struggled with diversity, equity, and inclusion. There are gender and racial disparities, not to mention a lack of access to tech opportunities for under-recognised communities. This exclusion not only perpetuates social injustice but also stifles innovation. When a homogenous group dominates a field, it limits the range of perspectives and ideas.

Defining Empathetic Leadership

Empathetic leadership is a response to these challenges. It is a leadership style that emphasises empathy, understanding, and compassion. These leaders actively listen to their team members, feelings, and perspectives, and work to promote an inclusive and supportive work environment.

Key characteristics of empathetic leadership include:

1. **Active Listening**: Empathetic leaders listen without judgment and seek to understand the experiences and concerns of their team members.

2. **Open Communication**: They create an environment where team members feel psychologically safe to share their thoughts and ideas.

3. **Support and Advocacy**: Empathetic leaders actively support the growth and development of their team members, advocating for their needs and concerns.

4. **Inclusivity**: They actively promote diversity, equity, and inclusion in the workplace.

Empathy in the Tech Industry and Cybersecurity

The tech industry, like any other, is populated with people who have their own unique experiences, challenges, and needs. Empathetic leadership recognises this and leverages empathy to create a more inclusive industry.

Let's delve into a couple of case studies to illustrate how this style of leadership can shape the future of inclusion in cybersecurity.

1. Salesforce:

For example, Salesforce, a cloud-based software company, has shown the tech world the power of empathetic leadership and has made significant strides in promoting diversity, equity, and inclusion. Under the leadership of CEO Marc Benioff, the company has taken a proactive stance on diversity and inclusion by focusing on closing the gender pay gap, diversifying its workforce, and advocating for LGBTQ+ rights. It conducted a comprehensive salary assessment to ensure equal pay for equal work

and made significant investments in employee resource groups, focusing on diverse communities and their needs.

The result? Salesforce has not only improved its diversity metrics but has also seen increased innovation and profitability. Employees who feel valued and included are more engaged and motivated to contribute to the company's success. This is a clear example of how empathetic leadership can shape the tech industry's future.

2. Microsoft:

Another example is Microsoft. Under the leadership of CEO Satya Nadella, another champion of empathetic leadership, Microsoft has adopted a growth mindset that encourages all employees to speak up and share their ideas. They promote a culture of empathy, actively seeking input from all employees and using it to drive company initiatives. Microsoft's emphasis on inclusion has led to the creation of products like the Xbox Adaptive Controller, designed to meet the needs of gamers with limited mobility. This product's success is a testament to how empathetic leadership can lead to innovative solutions that benefit a broader range of users, and thus has contributed to Microsoft’s ongoing success.

Overcoming Obstacles to Empathetic Leadership

While empathetic leadership holds great promise, it is not without its challenges. Implementing this style of leadership in the tech industry can be met with resistance, particularly in more traditional corporate cultures. It requires a fundamental shift in the way leaders approach their roles and their relationships with employees.

To overcome these obstacles, leaders in tech and cybersecurity must:

1. **Lead by Example**: Leaders must embody empathetic values in their own behaviours, setting the standard for the entire organisation.

2. **Provide Training**: Offering training and resources on empathy and inclusion can help employees and leaders alike to better understand and practice this leadership style.

3. **Measure and Track Progress**: Regularly assess and report on the company's diversity, equity, and inclusion efforts to ensure ongoing improvement.

The Future of Inclusion in Cybersecurity

The future of inclusion in cybersecurity lies in the hands of these forward-thinking leaders. As we've seen from case studies like Salesforce and Microsoft, when leaders prioritise empathy, everyone benefits. Tech companies that embrace empathetic leadership will be better positioned to create innovative solutions that cater to diverse audiences.

By fostering inclusive workplaces and products, these companies can help bridge the digital divide and ensure that technology serves the needs of everyone. The future of inclusion in tech and cybersecurity is bright when empathetic leadership becomes the norm rather than the exception.

Conclusion

The awareness of emotional intelligence has been spoken about and practiced for a significant period of time. What it enables leaders to achieve in their teams is an understanding and connection between feelings and actions that signify how inclusion proceeds in people that have been invisible or ignored.

Empathetic leadership is not just a theoretical concept but a practical approach to shaping the future of inclusion in cybersecurity. The tech industry, with its enormous impact on society, needs to lead the way in creating inclusive environments and products as demonstrated by companies like Salesforce and Microsoft.

By promoting diversity and inclusion, actively listening to employees, and creating products that meet the needs of all users, leaders can pave the way for a more inclusive, innovative, and equitable future. The time for empathetic leadership in cybersecurity is now, and the benefits it brings will undoubtedly shape the industry's future for the better.

About the Author

Lauren Neal is the Founder and Chief Programme Creator of Valued at Work. She has worked in the energy sector since 2005 and is a chartered engineer and chartered project professional. Her book Valued at Work: Shining a Light on Bias to Engage, Enable, and Retain Women in STEM released in October 2023 became an Amazon #1 best-seller.

Lauren can be reached online at http://linkedin.com/in/laurenneal/.

AI, Deepfakes and Digital ID: The New Frontier of Corporate Cybersecurity

By Michael Marcotte, Founder & CEO of artius.iD

The emergence of deepfakes fired the starting pistol in a cybersecurity arms race. Paranoia about their impact has rippled out into a range of areas, including political misinformation, fake news and social media manipulation.

Deepfakes will intensify the already acute pressure placed on trust and communication in the public sphere. This will rightly attract the attention of regulators and policymakers. But because of this focus, what risks being missed is the role deepfakes will play in corporate fraud, scams and theft.

Corporates will feel justified in delegating deepfake identification and protection to central governments and public agencies – this is where the frontlines have supposedly been drawn. If they do cede this territory to the state, they will leave themselves completely exposed to deepfake-enabled corporate fraud.

In fact, this is already happening. In February, an employee was duped into sending $25m of company funds to malicious actors after falling for a deepfake video scam, where fraudsters posed as the firm's CEO in a video conference (The Guardian).

This attack is the canary in the coalmine – hackers have expanded their arsenal and are bringing deepfakes to the cybersecurity gunfight. Corporates cannot afford to rely on government for protection – they're too slow. They need to develop their own multi-layered defensive strategy now.

But what does this look like?

The cornerstone has to be compliance. It's never enough on its own, but if your employees are regularly leaving the door wide open for hackers then it doesn't matter how much you spend on new technologies.

So, corporates need to invest in training and informing their employees about the threat posed by deepfakes and how to mitigate it. An email newsletter is not going to cut it – there should be regular, mandated training sessions. These might involve simulated phishing exercises with deepfakes or interactive workshops where employees are trained to spot red flags. There needs to be rapid internal reporting mechanisms so that employees can reach specialized IT teams as soon as a threat is identified.

Getting employees up to speed on this will be no small feat. Unfortunately, as any IT professional knows, most workers outside of the industry have a chronic lack of cybersecurity basics. It will take regular, proactive measures to ensure that they aren't accidentally exposing the company. But if successfully done, a well-educated, vigilant workforce is the foundation of a comprehensive cyber defense.

Alongside training staff, corporates should also be onboarding the latest authentication and verification tech. Not investing in the latest defensive systems leaves corporations in the stone age, facing down hackers with AI and deepfakes at their fingertips.

These might include advanced forensic analysis tools that use machine learning and image processing to identify manipulated media content. Biometric authentication needs to be ramped up, with enhanced facial and voice recognition, to verify identities. Digital watermarking can be deployed to mark authentic content for employees.

These technologies can be rapidly integrated into company practices today. More long-term technological defenses might involve AI-powered deepfake detection tools – using machine learning algorithms, trained on datasets composed of authentic images and deepfakes, to detect fraudulent content. But these will take significant amounts of time, data and expertise to build.

Whilst these first two strategies are preventative, it's also crucial to have damage limitation in place, should a breach occur. Corporates need to have robust access controls to sensitive information so that a successful scam at lower levels of the business does not result in high-level IP and trade secrets being lost.

Strict and defined network separation is also crucial, based on the principle of least privilege. If malicious actors gain access to a network through an employee, this should not allow them to pivot into other areas of the business. Added to this, containment measures can prevent dissemination of fraudulent media

throughout the company. Takedown notices, content filters and transparent top-down communication can all contribute to putting out the fire after an initial breach.

Senior management have plenty to do to properly insulate their firms, and this will involve increased investment in cybersecurity across the board. But this shouldn't be a hard sell to management. The threats have ramped up and the risk has increased exponentially.

Deepfake breaches will result in significant reputational, financial and regulatory fallout. No CEO will want to be at the helm for the next high-profile deepfake scam. So they need to step up to the plate now and start taking steps to defend themselves. The stakes are too high to wait for the government to do it for them.

About the Author

Michael Marcotte is Founder & CEO of artius.iD. He is one of the premier cybersecurity executives in the US. After joining in 2006, Michael was Global CIO, Global CDO and President (Hughes Cloud Services) at EchoStar, the multi-billion-dollar satellite communications giant. He was one of the very first people to serve as Chief Digital Officer in a major international corporation. Michael left EchoStar in 2014 and has applied his expertise at a range of firms in technology, cybersecurity and venture capital. As well as artius.iD, he is founder, chairman and CEO at innovation lab software and venture capital firm Artius Global Holdings and cybersecurity firm Praelium Systems. Michael holds a number of public advisory positions. He is co-founder of the National Cybersecurity Intelligence Center (NCC) and was founder and chairman of the NCC's Rapid Response Center Board. He has been a senior advisor for several heads of state and US Senators. He is also a board member at the Office of Economic Development and International Trade (OEDIT). Michael can be reached on LinkedIn.

Full Drive Encryption Only a Half-Measure for Data Security

Pre-Boot Authentication Is the Missing Half

By John Benkert, Cigent CEO and Co-Founder, Cigent

In an era where data security breaches are not just incidents but an event that can topple organizations, the importance of robust security measures has never been more desperately needed. This is particularly true for federal and sensitive commercial sectors like healthcare, where the stakes involve national security and patient safety. Among the myriad of security measures available, Full Drive Encryption (FDE) is often relied upon to secure data at rest (DAR). FDE alone however, is not adequate security if it is dependent on post-boot authentication (OS account login) to “unlock” the drive. These credentials can be compromised, and advanced threats can even bypass the login step altogether. To ensure FDE can effectively secure DAR, it should be tied to Pre-Boot Authentication (PBA). PBA stands out as a critical layer of defense, especially against the threats posed by compromised devices.

Understanding Pre-Boot Authentication

Pre-Poot Authentication is a security protocol that requires user authentication before a device's operating system loads. This could involve biometrics, smart cards, or other tokens. Unlike traditional

password-based methods, PBA ensures that the authentication process is tangible and directly linked to the user, making unauthorized access exponentially more challenging.

Applications in Federal Agencies

In federal agencies, where information can not only be classified but a leak can cost lives, the implementation of PBA is not just beneficial but imperative. The key applications include:

- **Protection Against Espionage:** Foreign and domestic threats often target federal agencies. PBA acts as a first line of defense, preventing compromised devices from being booted by unauthorized personnel, thus safeguarding sensitive information from espionage activities.

- **Securing Communication Networks:** Federal agencies often communicate over highly confidential networks. PBA ensures that only authorized devices can access these networks, mitigating the risk of eavesdropping or data interception.

- **Compliance with Federal Regulations:** Many federal agencies are bound by strict data security regulations. Implementing PBA helps in complying with these regulations, thereby avoiding legal repercussions and maintaining public trust.

But it's not just federal agencies that need the security that PBA provides. Commercial entities should take advantage of the technology as well.

Applications in Healthcare and Other Data-Sensitive Environments

The healthcare sector not only deals with highly sensitive patient data, making it a prime target for cybercriminals, but most medical devices are connected to networks for monitoring and therefore are vulnerable to attacks as well. The application of PBA in healthcare serves several critical functions:

- **Protecting Patient Confidentiality:** Patient data is not only sensitive but also legally protected. PBA helps in safeguarding this data by ensuring that only authorized personnel can access devices containing patient information, thereby maintaining confidentiality and compliance with laws like HIPAA.

- **Securing Access to Medical Devices:** Many modern medical devices are connected to networks. PBA can be used to secure these devices, preventing unauthorized access that could lead to tampering or malfunction, potentially endangering patient lives.

- **Mitigating Insider Threats:** Healthcare facilities often have numerous staff and contractors moving in and out. PBA minimizes the risk of insider threats by ensuring that only designated individuals can access certain devices and information.

Addressing the Challenge of Rogue Devices

In both federal and healthcare scenarios, rogue devices - devices that have been compromised and are under the control of unauthorized entities - pose a significant threat. PBA addresses this challenge effectively by:

- **Preventing Boot-Up of Compromised Devices:** If a device has been tampered with or infected with malware, PBA can prevent it from booting up, thus stopping the threat in its tracks before it can infiltrate the network or access sensitive data.

- **Enabling Immediate Response:** In case a device is flagged during the PBA process, immediate action can be taken, such as quarantining the device, thereby preventing any potential spread of the threat.

- **Maintaining Device Integrity:** Regular PBA checks can ensure ongoing integrity of devices, making it easier to identify and address any anomalies that suggest compromise.

The application of Pre-Boot Authentication in federal and sensitive commercial applications like healthcare is more than just a security measure; it's a fundamental necessity in the digital age. By providing a robust barrier against unauthorized access, especially in scenarios involving compromised devices, PBA plays a crucial role in safeguarding national security and protecting sensitive information. As threats evolve and the landscape of cyber warfare becomes increasingly complex, the implementation of PBA will undoubtedly become a standard, reinforcing the bastions of our most critical sectors against the ever-growing tide of cyber threats.

About the Author

Cigent CEO and Co-Founder John Benkert served 20 years in USAF Intelligence and seven in the NSA, where he received the National Scientific Achievement Award for technological innovations in data security. He is the owner of CPR Tools, leading experts in data recovery, forensics, and destruction since 1987.

Recognizing the vulnerabilities in data security solutions including FDE and SEDs, Benkert set out to design a more secure approach to data protection - one that could not be defeated no matter the situation or adversary. He formed a team of experts in storage, data forensics, and cyber security. Securing funding from In-Q-Tel, the Cigent team has achieved Benkert's vision of developing the most secure data security solution available. He is reachable at https://www.cigent.com/

Cross-Team Collaboration is Vital for Organizations in Today's Digital Landscape

By Tony King, SVP International at NETSCOUT

In today's world, where the digital landscape is rapidly evolving, the cyber threat level is continuing to grow. Cybercriminals are constantly refining their attack techniques, developing increasingly complex and sophisticated cyberattacks.

Our findings reinforce this, with approximately 7.9 million distributed denial-of-service (DDoS) attacks taking place in the first half of 2023, representing a 31 percent increase year-over-year. This equates to roughly 44 thousand DDoS attacks per day worldwide. In terms of attack methodologies, there was a near 500 per cent growth in HTTP/S application-layer attacks, as well as 17 percent increase in DNS reflection/amplification attacks from the second half of 2022 to the first six months of 2023.

As cybercriminals continue getting better at launching increasingly dangerous attacks and bypassing traditional defense systems more effectively than ever before, it is imperative for organizations to implement robust cybersecurity systems.

The Benefits of Cross-Team Collaboration

Two teams which play key roles in supporting a business's security posture and ensuring smooth functioning of its network infrastructure are network operations (NetOps) and security operations (SecOps).

Traditionally NetOps and SecOps teams have operated in their own silos, largely due to having different goals. For network teams, their attention is on providing easy access to information and devices. In contrast to this, security teams are focused on restricting access to information and devices. This leads to disparate tools and results in unmonitored areas within the network which threat actors can exploit.

Additionally, if a possible threat to an organization is identified, it could take days or even weeks to investigate and resolve the issue due to a lack of communication and cooperation between the two teams. For instance, many security breaches are unearthed when operations or applications become slow, with a closer look revealing a security breach has taken place. Collaborating would ensure enterprises identify this potential breach before it becomes an issue and prevent it all together.

Nowadays, as cybercriminals and the attacks they are launching become ever more threatening, it is increasingly important for there to be collaboration and data-sharing between the NetOps and SecOps departments.

When the two teams collaborate with one another, enterprises can reap several advantages. This includes rapidly accelerating the time it takes to detect and respond to a threat. When these teams share and combine their network traffic data and threat intelligence, they can rapidly discover potential security breaches and swiftly analyse them. This collaborative approach ensures organisations can take a proactive position to mitigating threats, diminishing the risk of significant damage or data loss.

Furthermore, cooperation can also lead to improved network performance. One of the key challenges faced by NetOps teams is ensuring optimal network performance. By sharing their security data with SecOps, NetOps departments gain an understanding of traffic patterns which may be the root cause of network congestion or performance problems. This information empowers them to act immediately, optimising network performance and assuring that critical systems receive the necessary bandwidth required for efficient and effective operation.

Adding to this, by sharing data, organizations can create a holistic view of network activities, enabling SecOps teams to share detailed visibility into traffic patterns with their colleagues in the NetOps department. This collaborative monitoring approach provides both teams with the ability to highlight anomalies, unusual behavioral patterns, and suspicious activity in a swift manner. Together, they can detect possible threats before they develop into something more sinister, further enhancing the business' security posture.

Elsewhere, effective collaboration and communication between the two teams streamlines the compliance monitoring and reporting process, in addition to also enabling both departments to gain a more thorough understanding of one another's goals and challenges.

How Data-Sharing Helps Businesses Overcome Challenges

Data-sharing and cooperation between NetOps and SecOps teams also plays a vital role in assisting organizations when it comes to overcoming several key challenges. Arguably the most significant of these concerns, which collaboration helps to overcome, is the issue of siloed data. When information is segregated and kept within individual teams, enterprises can lose sight of the bigger picture. Sharing data eliminates these barriers, making certain that relevant information is available to all stakeholders, leading to improved collaboration and more informed decision-making.

What's more, collaboration facilitates timely identification and reaction to emerging threats, significantly reducing response times. To limit potential damage to an enterprise's network infrastructure, rapid response to security incidents is imperative. Access to real-time information from both NetOps and SecOps teams ensures organizations can successfully neutralise threats before they are able to escalate.

Additionally, data-sharing can eradicate incomplete analysis. When information is siloed, both NetOps and SecOps teams will be unable to access detailed datasets, meaning they may find it problematic to conduct comprehensive network traffic analysis. By sharing data, these knowledge gaps are filled, equipping teams with an in-depth understanding of network activities. This enables them to make smarter, more thoughtful decisions, as well as to respond efficiently and effectively to potential threats.

As the rapid evolution of cyberthreats continues, collaboration between NetOps and SecOps teams is imperative for enterprises to ensure they maintain a robust security posture.

By sharing data and working together, businesses can enjoy faster network threat detection and mitigation, enhanced network performance, and improved visibility and monitoring. These combine to create a more secure, reliable, and efficient network infrastructure, protecting an enterprise's sensitive data and preserving its reputation.

For organizations, tearing down data silos and adopting a collaborative approach is not simply just a best practice – it is essential in the modern-day digital landscape. In the past 20 years, I have seen cyberthreats move from the old switch rooms (now data centers) to the board room as a business risk. It is important that both teams support each other to defend the integrity of the company's data and the network infrastructure.

About the Author

Tony King is NETSCOUT's Senior Vice President, International Sales with responsibility for directing all sales into the Company's expansive service provider and enterprise customer base across the EMEA and Asia-Pacific regions. Mr. King has a proven track record in building open, collaborative and international sales cultures that have produced strong and sustained revenue growth.

Prior to this role, Mr. King had served as Senior Vice President, Worldwide Sales for the Arbor security offerings since 2013. He came to NETSCOUT through the Danaher Communications Acquisition in 2015 as Vice President of Global Sales, focused on maintaining market leadership in DDoS detection/mitigation and strengthening the Global Channels to market.

Mr. King has over 30 years of Networking/Security/Telecom sales and sales leadership experience globally. Prior to joining NETSCOUT, Mr. King has held various roles within Arbor Networks. In his previous role as VP EMEA, Mr. King was directly responsible for driving revenue and building out the EMEA team over a successful 5-year period. Before joining Arbor in 2003, Mr. King served at Avici Systems as Sales Director. Prior to that, he worked for Ericsson's Datacom division as Regional Sales Director.

Is Zero Trust Enough?

Why Zero Access Is a Better Way to Protect Your Backup Infrastructure

By Greg Tevis, Vice President of Strategy, Cobalt Iron

Backup has always been seen as the last line of defense in data security. After all, if your backups are safe, then you can recover from most forms of attack. That's why as much as 93% percent of ransomware attacks these days may be going after backup data — to thwart that last line of defense. If attackers can get to the backup data, then they have the upper hand.

Right now, the zero-trust approach to data and resource security is all the rage. Every large backup vendor touts it. It's almost a knee-jerk reaction to invoke zero trust as the way to prevent these attacks.

To understand why that is, it helps to first understand the logic behind zero trust.

Traditionally, each user of a computer resource (e.g., data, network, system, or database resource) would have a login, and if that login is verified once, then that user would be privileged to move around and conduct tasks anywhere inside the domain of that resource. For example, with access to Active Directory, they could change who and what gets access to your network assets. With access into Exchange, they

could make changes to the databases and so on — all with a single login. The idea behind zero trust is to challenge that single set of user credentials to a resource by requiring a second or multiple types of authentication. Hence the terms two-factor authentication (2FA) and multifactor authentication (MFA). This often involves an email or text to a known ID containing an authentication code to further validate the authentication request. In doing so, zero trust helps to stop ransomware attackers and programmatic attacks from moving around production networks and accessing different zones of an IT infrastructure. With the zero-trust approach, a user attempting to access a resource is never trusted by default, even if they are already part of the corporate network. Access is granted only after successful validation using two or more methods of verification. In that sense, zero trust makes data protection a lot stronger than in the old days.

But zero trust isn't foolproof, as we saw recently with the attack on the MGM in Las Vegas. Hackers reportedly tricked MGM's help desk into providing an employee's credentials, bypassing the protection zero trust was designed for. Hackers are devising multilayered hacks, so they're ready for 2FA and know how to get around it.

There's no question that zero-trust security is worthwhile. But it still implies granting access. That's the whole point. And as proven by the MGM attack, when there's access, there can be damage. That's especially scary when it comes to the backup environment.

Zero Access®: a better way

But what if there was no access to the backup infrastructure at all? That's the idea behind the Zero Access security model.

Zero Access means just that: With this unique architecture, logins and access for normal operational management of the data protection infrastructure are eliminated. This removes the need for even zero-trust-level access to backup infrastructure components, including the backup server, the operating system, the backup server software, the backup catalog, backup storage, and the backup network. Users don't even have logins for those components. Instead, the only thing that can get in is a hermetically sealed automation engine. Removing direct operational accessibility to these resources eliminates vulnerabilities to cyber attacks on the backup landscape.

Zero Access doesn't mean giving up control of your data.

With a Zero Access backup architecture, everything you use to run your business — servers, domains, devices, applications, etc. — remains completely within your control, and you continue to maintain access and logins to all of those resources. You also set your own backup policies — when and what to back up, how long to keep the backups, etc. — and control access to the backup GUI, where those policies are configured. The solution collects the backup data from the servers and applications it's protecting and puts it into vaulted storage within your company's security domain. And because there's no access to any hardware or software component of the backup environment, all backup data ingested into a Zero

Access architecture is immutable. An automation engine manages the entire backup infrastructure, ensuring the components carry out their tasks according to policy.

What happens if I need to restore my data?

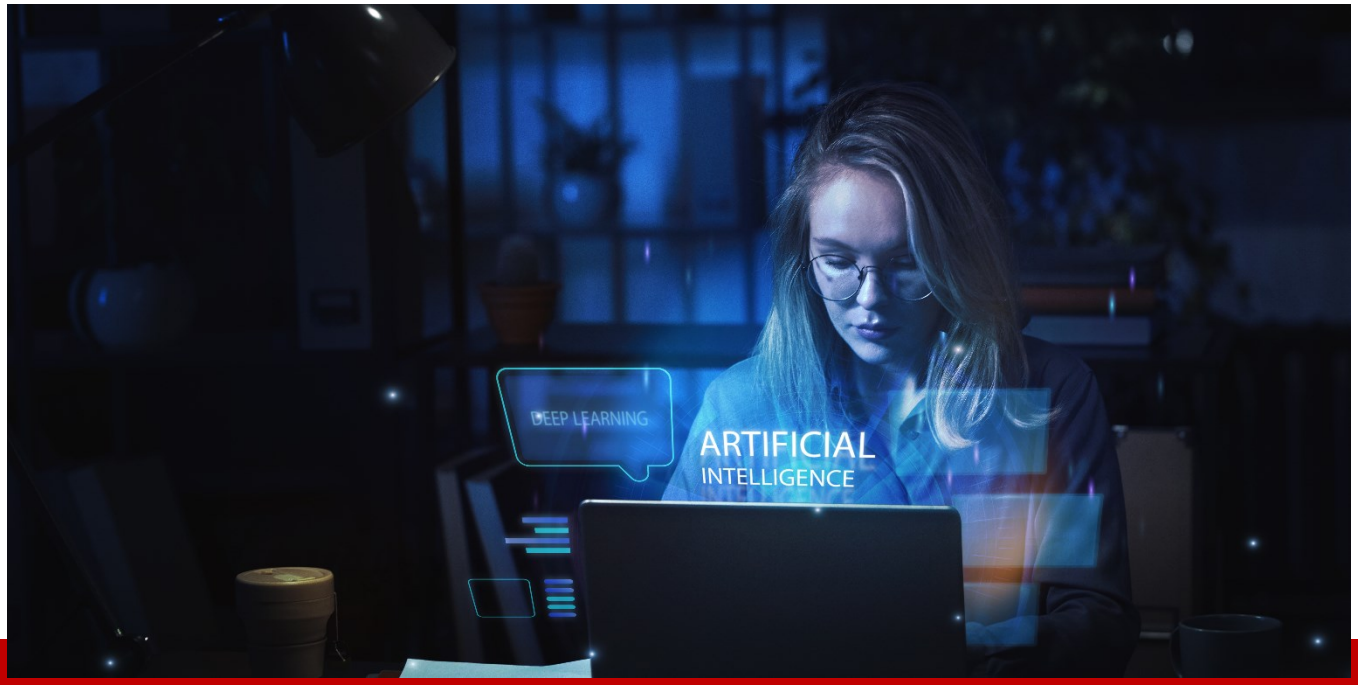
No business seems to be immune from cyber attacks. In a worst-case scenario, a ransomware attack could get into Active Directory, gain all usernames and passwords, and wipe out all production data. And yet the data in the backup environment would still be safe because it lives in a Zero Access infrastructure. There is no bridge from the compromised credentials into the Zero Access environment because there are no logins. The only access to that infrastructure comes from the backup provider's automation engine, which manages components and executes tasks according to the policies you've set.

If hackers were to attack your business operations, you'd be able to restore a copy of your backup data thanks to Zero Access. Once you've started to rebuild the production system so that there's somewhere to restore to, you can start to install restore tools onto those systems that will be able to recover the data. Then you'd simply log in to the backup GUI and follow the recovery procedure. And remember: You're only restoring a copy of the data; there's no way to compromise or destroy the original backup data, which remains safely locked away.

While the zero-trust approach sounds great, and it plays an important role in protecting the business environment, it is not the pinnacle of security that some backup vendors make it out to be ... especially when it comes to precious backup data. You must protect your backup environment at all costs. The best way to keep bad actors out of your backup environment is to make sure there's no access at all. And for that, Zero Access offers much higher security than zero trust. The best part is that Zero Access security protection for backup is available today.

About the Author

Greg Tevis, Vice President of Strategy at Cobalt Iron, has worked for 42 years in the storage and data protection market helping companies develop data protection and cybersecurity solutions. Tevis is recognized as an industry expert in storage technologies, particularly storage management. He has 42 U.S. patents, with several more pending. He can be reached at gjtevis@cobaltiron.com (linkedin.com/in/greg-tevis-10a5042). More information about Cobalt Iron is available at cobaltiron.com.



CTI for M&A

Active dark web Intelligence to aid M&A

By Shawn Loveland, COO, Resecurity

Every industry-leading company has gone through mergers and acquisitions (M&A) at some point to acquire a competitor, expand into a new market, or gain access to intellectual property or technology. As M&A involves extensive risk for any company, how it is carried out can unlock or destroy millions of dollars in value. Although M&A transactions often undergo screening, External CTI is not part of all M&A vetting or portfolio monitoring processes. However, CTI can answer critical questions that the acquiring company needs to know to determine the risks of acquiring or making a strategic investment. Some of these questions include:

1. Is the company experiencing a data breach, or has it experienced an undisclosed one in the past?
2. Will the company experience a data breach in the future?
3. Has the strategic IP of the company been leaked on the dark web?
4. How does this company compare to the cybersecurity risk with its competitors and other companies evaluated by the M&A entity?
5. Has a data breach or loss been detected that could cause regulatory issues (Such as the US Securities and Exchange Commission rule 7) or privacy concerns and materially affect the deal or pose a risk to the acquirer if the deal were finalized?
6. Has the company been involved in an unknown or undeclared material breach, as defended by the recent SEC rule 7, that the company must disclose once known about? These identified issues

may have a material impact on the value of a company. Additionally, the company may be financially, civilly, and legally liable if the SEC has not been notified of the material breach.

7. Is the company at risk of insider threat from disgruntled employees offering company data or services on the dark web?
8. Has the M&A entity or its supply chain been breached, or is a breach likely, which could result in leaked details about their M&A activities on the dark web?

Organizations that purchase or merge with another entity inherit cybersecurity risks. Unfortunately, many companies do not conduct adequate cyber risk assessments to determine if a potential acquisition has been breached or if there are precursors of a breach available to the threat actor to breach the company if they elect to. This lack of exploration can increase the risks of inheriting compromised companies and their networks. In the fast-paced world of M&A, it can be increasingly more work to control cybersecurity risks. At the same time, information security departments may need more personnel and resources to mitigate discovered cyber threats.

Many factors impact a company's stock price. Without polling investors, it is unclear whether a stock's decline after a breach disclosure is due to correlation or causation. The Starwood breach was a significant unknown breach that existed before and after its purchase by Marriott. On the day Marriott announced the breach, its stock dropped 2%. In the ten trading days after the announcement, its stock dropped 16%. In the thirty days after the announcement, it dipped 25%. It was 89 days from the date the breach was announced and Marriott's lowest close for the year, with a stock price drop of 46%.

During the M&A process, external consultants are often involved, depending on the deal's specifics. These consultants typically include investment banks, buying and selling agents, lawyers, auditors, etc. However, it is increasingly common to include CTI vendors as well. These vendors assess the security status of the company being considered for the deal and determine if there has been any breach or theft of valuable items by a known or unknown third party. This information is crucial as it can significantly impact the sale.

It is about more than just evaluating the M&A company. Threat actors more frequently target M&A organizations than typical businesses. Higher-end threat actors use proven and profitable business models such as industrial espionage and stock market manipulation, making breaching an M&A company very profitable. Therefore, M&A entities can benefit from CTI monitoring, such as what Resecurity offers, to safeguard themselves and the other entities involved in M&A activities. Additionally, it is essential to protect the confidential information the seller provides, as any leak could result in a seller's SEC rule 7 disclosure.

CTI for M&A

It is common for M&A companies to do CTI analysis during the M&A process. Most M&A companies outsource various aspects of determining the company's cybersecurity posture to other companies, including a perimeter scan of the company's network, scans of low-end cybercrime forums (TOR), and a review of the company's source code. However, external threat intelligence can enhance this vetting by

focusing on threats originating outside the company's firewall and based on access to the surface web, the dark web (TOR), and Vetted / invite-only cybercrime communities. This allows for the following questions to be answered with high confidence:

- Is the company breached, and if so, by whom? What is their motivation? What data has been leaked?
- Are there precursors of a breach that a threat actor could use to breach the company if they elected to do so?

One size does not fit all: A CTI vendor must collaborate with customers to determine their needs and constraints. This will allow them to assist their customers in selecting the right combination of services to meet their requirements, including budget, timeframe, confidence, rules of engagement, and depth of insights.

Based on Resecurity's internal analysis of discoverable breaches (not every breach can be identified through CTI), if CTI is limited to the surface web, less than 5% of companies that have been breached can be identified. If CTI is limited to the open web and the "dark web (TOR)," less than 25% of companies that have been breached will be identified (surface web (<5%) and dark web (TOR) (<20%)). For discoverable breaches to be discovered, they must include surface web and dark web, in addition to Vetted/invite-only cybercrime communities & P2P (> 75%).

Key takeaways:

CTI offers threat intelligence services to entities involved in M&A to reduce their risks. Some CTI vendors provide services to entities involved in M&A. The scope and scale of these options are scaled up and down to meet the individual customer's and engagement's needs and budget:

Offering: One-time: Summary report

Timing: Normally less than a week.

Used for: Used during the development of companies for acquisition to help prioritize companies based on their risk.

Deliverable: Summary report of the likelihood that the company is, or likely will be, breached.

- Typically, 1-2 pages.
- Optionally, identify initial areas of risk discovered from external CTI besides items related to a potential breach.
- Can compare the risk of the target company being breached with other specific customers.
- Provides areas of concern and areas of future research.

Offering: One-time managed service: In-depth

Timing: Normally less than three weeks.

They are often used during the due diligence or earlier based on the acquirer's requirements.

Deliverable: A more detailed report of the artifacts discovered during the one-time summary report.

- Typically, 5-10+ pages.
- Duration based on the requirements per customer and engagement.
- Optionally, identify additional areas of risk discovered.
- Provide areas of concern that could be addressed through additional research.
- Research can focus on areas of concern raised in the summary report.

One-time managed service: Mitigation

Timing: Varies and can be done pro- or post-acquisition.

Used for: Aid the victim in mitigating the breach and ejecting the threat actors from their network.

Deliverable: Collaborate with the affected company to assist them in identifying and addressing known threats. Additionally, evaluate the effectiveness of the implemented solutions.

Red Teaming

Timing: Varies and can be done pro- or post-acquisition.

Used for: Aid the victim or the acquirer in identifying and mitigating likely avenues of a potential breach(es) and software and hardware vulnerabilities.

Deliverable Vulnerability assessment and penetration testing. To include strategic intelligence, including IoC, endpoint, and vulnerabilities.

Managed engagement

Timing: Varies. Duration based on the requirements per customer and engagement.

Used for: To help any parties learn more about the threat and the efficacy of the mitigations put into place.

Deliverable: Provide ongoing research to support the mitigation of identified threats.

Ongoing portfolio monitoring

Timing: Ongoing with the cadence of the reports defined by the customer.

Used for: Identify new threats that emerge in their existing portfolio.

Deliverable: Ongoing monitoring of a portfolio of companies managed by an M&A entity.

- Monthly report with alerts for emerging threats.
- Provides an updated list of areas of concern, areas of future research, and mitigations.

Conclusion

As part of the M&A vetting process, the acquirer is expected to evaluate the source code for misused open-source code, unknown vulnerabilities, and a pen test of the entity's network. Some will go deeper and rely on a CTI vendor for a deeper scan. However, they usually rely on vendors who can only access TOR and the surface web, which gives their clients incomplete visibility and will often miss material issues they are concerned about. Often missing more notable events than they discover. However, an in-depth CTI for an M&A effort can answer critical questions that the acquiring company needs to know to determine the risks of acquiring or making a strategic investment.

This article is an abstract of a more extensive blog. The blog can be found here.

About the Author

Shawn Loveland is the COO of the Resecurity. Shawn Loveland is an experienced professional in the technology and cybersecurity field, with over 35 years of industry expertise. He has worked for both small and large companies and has received 15 US patents and numerous international patents in computer security and telephony.

As the COO of Resecurity, Shawn aids Resecurity in providing practical solutions to our clients against the current threat landscape. He conducts proactive threat research and helps clients assess their Cyber Threat Intelligence (CTI) programs. He also provides customized intelligence services tailored to meet their unique needs. Before joining Resecurity, Shawn was responsible for dark web intelligence at Microsoft.

Shawn can be reached online at (Shawn Loveland | LinkedIn) and at our company website www.resecurity.com

How Main Street Businesses Can Up Their Cybersecurity Game

By Mike Caralis, Vice President, Business Markets at Verizon

Small businesses are not only essential in keeping Main Street thriving and bustling (I love my local sushi place), but they are essential to our economy. In fact, they account for 44 percent of U.S. economic activity according to the U.S. Small Business Administration. They are also at a high risk for cyberattacks and data breaches, putting their business — including their sensitive information, customer data, and intellectual property — at great risk. Unauthorized access to data has the potential for significant financial loss that can be difficult or impossible to recover.

Meanwhile, cybercrime has become a thriving business, with 95 percent of data breaches coming from the work of financially driven threat actors using increasingly sophisticated tactics and advanced techniques to threaten companies both large and small. An expanded attack surface, including the proliferation of end points and the adoption of digital technologies without adequate security controls in place, is fueling the increase in cybercrime, according to the 2023 Verizon Data Breach Investigations Report (DBIR).

Cybercriminals see small to medium-sized businesses (SMBs) as easy targets with valuable data ripe for the taking. The Verizon report revealed that these businesses, with under one-thousand employees, are just as vulnerable to cybersecurity attacks, if not more so, than large businesses. The reason is that smaller companies may lack the resources and expertise to implement strong security controls to adequately prevent, detect, and respond to cyberattacks.

Regardless of their size, organizations are facing similar types of attacks — social engineering, system intrusion, and basic web application attacks. The top cybersecurity attacks affecting SMBs specifically, according to the Verizon report, are:

- **Human element.** The number one risk to any SMB is its own people. In fact, 74 percent of breaches involved human actions, whereby adversaries use social engineering and misrepresentation tactics to steal data or hold businesses ransom. Pretexting, an invented scenario that tricks someone into giving up information, accounted for half of all social engineering incidents in 2022. Phishing tactics came in second, at 44 percent.
- **Ransomware.** Using malware to block access to a computing system, ransomware was present in over 62 percent of all incidents.
- **Denial of Service (DDoS).** These attacks compromise the availability of networks and systems by overwhelming them with large amounts of data. DDoS attacks represented 42 percent of incidents.
- **System intrusion.** This technique, which involves bad actors using their expertise in hacking and malware to breach or impact organizations, accounted for 37 percent of breaches. This is a category that differs from ransomware and the human element, as it's a more sophisticated, calculated and targeted type attack.

Seven Ways to Strengthen Your Cybersecurity Posture with Fewer Resources

If a business leverages technology, they have a cybersecurity problem. For SMBs, who already have an uphill battle, it's vital that they have the right cybersecurity protocols in place to mitigate risks. Here are seven techniques even the smallest business can implement:

1. Manage who has access to your data. Access control management uses processes and tools to create, assign, manage and revoke access credentials and privileges for users of assets and software.
2. Train your employees to be security savvy. Establish and maintain a security awareness program for your workforce (even if it is a team of five) to be security conscious and reduce cybersecurity risks.
3. Know where your data resides. Is your organization's data stored on a network, on hard drives, on servers, in the cloud? Do you rely on third parties? Knowing where your data resides is helpful so you can better protect it and know what steps to take if data has been compromised.
4. Create an incident response management plan. Many cyberattacks, such as pretexting, tend to escalate quickly and can have a significant impact. A plan will help an organization better prepare, detect, and respond to an attack.
5. Ask questions. Here are a few good questions to start with:
    - Do we have a designated information security expert on staff or a third-party trusted risk advisor?
    - Is our website properly protected?
    - Do we regularly back up our data and files?
    - Are our company's devices protected with antimalware and antivirus software?
    - Do we regularly patch our hardware and software?

- Do we know what data we manage and where it resides?
- How much should we be spending on information security-related tools and controls?

6. Consider security technical controls. Companies will want to look into basic security controls including antivirus software, firewalls, and multifactor authentication.
7. Tap into best practices. There are several resources to help SMBs with best practices to help prioritize, customize, and strengthen their current cybersecurity posture and grow their efforts over time:
    - Center for Internet Security (CIS) Critical Security Controls
    - National Cybersecurity Alliance (NCA)
    - NIST Cybersecurity Framework
    - Cybersecurity and Infrastructure Security Agency (CISA)

We want to see businesses of all types and sizes thrive. Building in a layer of cybersecurity defenses with security controls and protective measures — even one layer at a time — will go a long way to strengthening SMBs and their current cybersecurity posture. That's a good formula for growing a company's cybersecurity efforts, along with its business, over time.

About the Author

Mike Caralis, Vice President, Business Markets at Verizon. As Vice President of Verizon Business Markets, I lead three critical business units for small and midsize business customers: network as a service (NaaS), Fios for Business and our channel program. My team of 1,200+ professionals partner with customers on their digital transformation journeys, providing innovative managed solutions for total communications, connectivity, collaboration and security.

Our customer-centric organization delivers 5G technologies, fiber, ethernet, security solutions, and unified communications solutions such as One Talk (voiceover IP solution) and Microsoft Teams. As businesses across all segments and industries anticipate a post-pandemic comeback, they are looking to adopt 5G and its potential to create new opportunities and build new efficiencies and scale their businesses. Our team also provides Fios for Business, business digital voice, and easy to deploy and use set of security and collaboration products.

Prior to this, I served as Executive Director of Solution Architect and Engineering. In that role, my team was focused on the transformation of our technical teams, providing the best-integrated solution designs and managed services, including broadband, security and collaboration platforms. Earlier in my career, I served public sector customers at Verizon for four years. Last year, our team delivered critical services and technology to aid in the pandemic response and enable remote learning for students.

Previously, I served as the Director of Marketing and Operations for Verizon Wireless and partnered with Apple, Google and Samsung to enable a frictionless customer experience in deploying new technology and applications. As a result, Verizon was the first carrier in the world to launch Apple Business Manager, an iconic solution. Later, I led a team that launched Android zero-touch and Samsung Knox Mobile Enrollment. Prior to Verizon, I worked in various sales roles at Nextel and Sprint.

Mike can be reached online at LinkedIn and at our company website http://www.verizon.com/

Keeping Pace with an Evolving Security and Trust Landscape

By Dean Coclin, Senior Director, Digital Trust Specialist, DigiCert

It's clear that 2023 will be remembered as the point that artificial intelligence (AI) stepped out of the shadows and took center stage. Once an "under the hood" technology best understood by techies, AI was quickly democratized by tools like ChatGPT, Siri, Alexa, and even Netflix. Today, even high school students are getting comfortable using AI-powered technology.

However, the impact of AI reaches far beyond popular applications like online chatbots, school reports, and funny memes on social media. Together with quantum computing, increasingly intelligent technologies are rapidly transforming cybersecurity strategies. For security organizations charged with protecting the enterprise, the time to prepare is now.

A double-edged sword

AI has already proven itself as a valuable option for defending the infrastructure. Enabling solutions like advanced intrusion detection systems (IDS) and intrusion prevention systems (IPS), AI can help organizations spot and respond to signs of possible breaches faster than earlier generations of IDS.

But we will soon start to see AI use pivot from defense to attacks. As AI becomes more accessible, bad actors will increasingly use its capabilities to harvest data available online to acquire personal information about individuals and their organizations. We've seen deepfake clips showing how AI can be utilized to mimic a person's voice. With technology available today, an attacker could harvest data from LinkedIn, YouTube, or other public sources to place a phone call, simulate a manager's voice, and perform malicious activities like resetting an organization's passwords.

We're also seeing new threats from AI on the web. The ability to render new sites in response to search queries has a great potential for interacting with customers, but it can also introduce new fraud risks. The more generative AI search capabilities advance, the greater the possibility that organizations can lose control of the information on their own websites. It won't be long before AI can write, construct, and render an authentic-looking page almost as fast as a search result can be served up. Whether the page is genuine, or contains false, malicious content may not be obvious to a viewer.

The pressure is growing for leaders to develop a strategy to manage AI threats as well as take steps to ensure trust for key company assets like public websites.

Preparing for a post-quantum world

Quantum computing has also been advancing rapidly over the past few years, and it's posing a serious threat to existing cryptography. Soon, large-scale quantum computers will be capable of cracking most public key cryptosystems, potentially compromising communications on the Internet and other digital systems. Although many IT leaders are aware of quantum computing risks, their business counterparts may be unaware of the looming threat. According to a report by the Ponemon Institute, "Preparing for a Safe Post Quantum Computing Future: A Global Study," most organizations have not yet established clear post-quantum cryptography strategies.

Despite the slow start, business leaders will soon become more aware of post-quantum cryptography (PQC). Industry organizations like NIST will release new standards the summer of 2024, which should encourage organizations to better develop and document their quantum strategies. With improved communication, better education and proactive planning, it's expected that executives will take major steps forward in PQC preparation and accelerate their companies' investments.

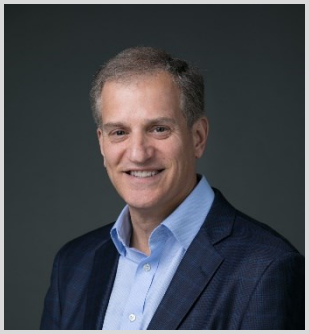
Trust takes a seat at the table

Much of the threat posed by AI and quantum technologies comes down to digital trust. Trust is fundamental to business relationships, and its loss can dramatically impact a business' reputation and revenues. It's not surprising that organizations are taking a close look at the role of digital trust in their organizations. As threats become more sophisticated and traditional perimeter-based defenses encounter new challenges, they are seeking to modernize their security approaches to go beyond the traditional infrastructure—and consider trust issues like personal identities.

Like any enterprise initiative, the overall strategy will need to come from executive leadership. Many organizations are establishing Chief Digital Trust Offers, or DTOs. The primary mission of a DTO is assuring that the organization's digital assets and services can be trusted by customers and partners. They focus on ensuring that trust is integrated into every digital interaction, and work to keep the organization's digital presence secure and dependable. A DTO leader sends a strong message about a company's commitment to the security and trust of its digital infrastructure—and reassures internal employees as well.

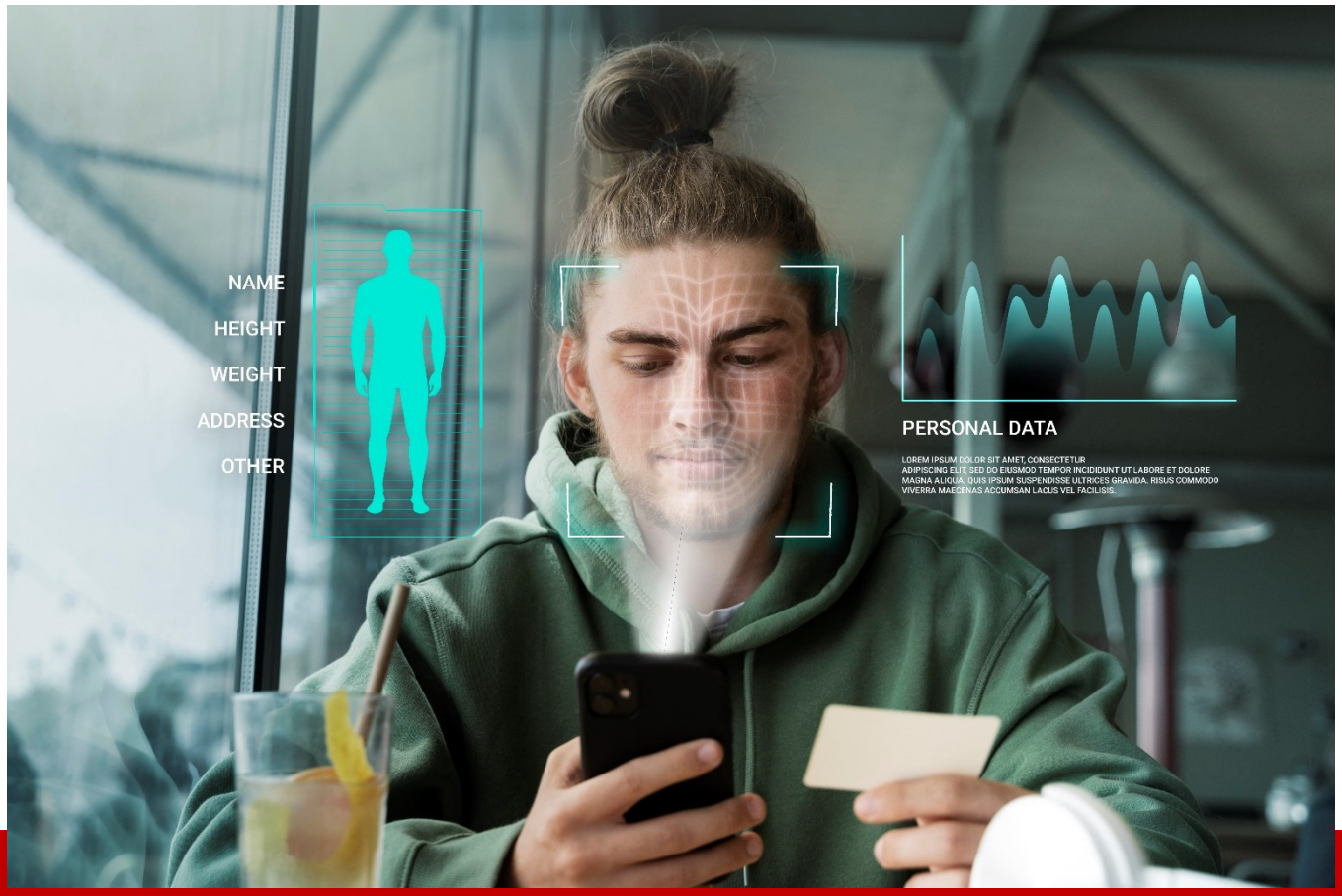
With forward-focused leadership, good communication and proactive strategies, organizations can meet AI and quantum computing challenges in the years ahead—and be ready for new ones on the horizon.

About the Author



Dean Coclin has more than 30 years of business development and product management experience in cybersecurity, software and telecommunications. As Senior Director, Digital Trust Specialist at DigiCert, he is responsible for driving the company's strategic alliances with IoT partners in the consumer security market, and with other technology partners. Coclin is also the previous chair of the CA/Browser forum.

Dean can be reached online at (dean.coclin@digicert.com) and at our company website http://www.digicert.com/



Relying on the Unreliable

The Hidden Costs of Facial Recognition Technology

By Tinglong Dai, Bernard T. Ferrari Professor of Business, The Carey Business School at Johns Hopkins University

With generative AI dominating the tech world's attention, facial recognition looms like a long, frightening shadow. The way it is trained and used, it is a force that is changing the boundaries of personal freedom and privacy. The training process uses a wide range of data sources, including images posted online by users, to build a detailed, often unreliable picture of who we are and what we do. The use of such unreliable technology is even more questionable.

Not only does this technology try to recognize us, but the way it's trained, often using data collected by bots that scour the internet, find every photo you post online, and match your face to every other representation of your face they can find, it can easily infiltrate our lives and peer into the most private parts of them. Our simple walk past a security camera or an Instagram photo can be turned into a file of our personal, legal, and financial records by piecing together our digital footprints, often mixing ours with those of others. The consequences can be just as swift and frightening.

And one can only hope that the technology is as reliable as it is advertised to public and private decision makers. In reality, the technology is based on a probabilistic model that matches patterns but is prone to error. As more data sources are added, these errors can be magnified, with disastrous consequences. Even more so when decision makers rely on the technology without questioning its reliability.

These errors are not just hypothetical. The story of Alonzo Sawyer, a Maryland man, shows them clearly, as Eyal Press wrote for The New Yorker. A web of legal and emotional problems engulfed Sawyer after a facial recognition system misidentified him. The system's decision was upheld despite the obvious age and physical differences between him and the actual perpetrator that a normal person could see with the naked eye. A probation officer's hasty and erroneous confirmation, along with his denial of the possibility that the facial recognition system could be wrong, made matters worse. The criminal justice system has been a terrifying ordeal for Sawyer and his family. They have been confused, frightened, and forced to defend his innocence. They have been the victims of a reliance on technology that is not always reliable.

A tragic tale, Sawyer's story is also a rallying cry for those in positions of authority, calling for swift introspection and decisive action. We must confront the frightening questions that loom large in the shadow of technology. What moral limits should be placed on the use of a technology that is so ubiquitous? What rights and limitations should people have over their digital identities? To what extent should we, the people, allow our governments to use unreliable technology to make decisions that can destroy citizens' lives without apology? These are pressing questions that demand immediate answers as AI rapidly permeates our lives and work.

At this crossroads, the answers to these questions will shape the course of our lives and those of generations to come. We must consider the ethical issues raised by facial recognition technology. Finding a middle ground between technological advances and concerns for social justice and human rights is essential. At a minimum, there must be honest disclosure of how models are trained, the sources of data, and independent, ongoing testing and monitoring of the performance of such models.

The speed at which new technologies are being developed will not allow time for reflection. Every second that passes without clear moral standards and strong systems of governance is a step toward a future where our lives are just data points in a vast surveillance network that is as unchecked as it is flawed.

We cannot autopilot our future. We can and should steer technology toward a future that values and protects people's right to privacy and freedom of choice. We must ensure that the legacy we leave behind is one of clarity, honesty, and a strong commitment to the fundamental values that make us human. The story of Alonzo Sawyer and the many others who could be caught in the web of facial recognition technology is a stark warning of how important this is. Now is the time to act.

About the Author

Tinglong Dai is the Bernard T. Ferrari Professor of Business at the Carey Business School of the Johns Hopkins University. He serves on the core faculty of the Hopkins Business of Health Initiative and the executive committee of the Institute for Data-Intensive Engineering and Science. He is also the Vice President of Marketing, Communication and Outreach at INFORMS. Tinglong can be reached online at Tinglong Dai, PhD (jhu.edu).

The Cybersecurity Conundrum: Navigating the Challenges with Fewer Resources and Rising Threats

By David Lee, Chief Evangelist and Visionary for Tech Diversity

The cybersecurity world is no stranger to adversity, but 2023 presented a unique set of challenges with industry veterans and newcomers on edge. A notable decline in investor funding compounded with widespread layoffs has led to uncertainty. It begs the question: can we afford to hit the brakes on cybersecurity investment in an era redefined by its technological dependencies?

Venture capital, often regarded as the lifeblood of innovation in the tech sectors, has recently experienced a noticeable slowdown in its once-rapid pulse. Cybersecurity companies, which were once bathed in the generous support of investors eager to back the following groundbreaking digital defense mechanism, are now in the midst of a cold market. The reasons behind this shift bear the familiar imprints of an economy in flux: interest rate hikes, inflation, and a general pullback in tech investment have collectively placed the cybersecurity sector within an unfamiliar and uncomfortable fiscal landscape.

As interest rates rise and inflation takes hold, investors are becoming more cautious and selective in their funding choices. The once-hot cybersecurity market is now facing increased scrutiny, with investors carefully evaluating these companies' long-term viability and profitability. This shift in investor sentiment has created a challenging environment for cybersecurity firms, forcing them to reassess their strategies and find new ways to attract capital.

Furthermore, the broader tech industry has experienced a general pullback in investment as concerns over market saturation and valuation bubbles loom. This cautious approach has affected cybersecurity companies and other sectors within the tech industry. The result is a more competitive landscape, with companies vying for a limited pool of investment dollars.

Almost as a chilling reflection of the funding downturn, today's cybersecurity professionals find themselves caught in a relentless maelstrom of job insecurity. Reports and studies indicate that nearly half of the workforce in this industry has experienced the harsh reality of cutbacks firsthand. This is not merely a statistic on a page; it represents the culmination of decades of collective expertise and dedication being pushed to the sidelines when digital threats are scaling with alarming velocity. The urgency to address these challenges has never been more significant as the need for skilled cybersecurity professionals grows to safeguard our increasingly interconnected world.

Ironically, the industry grapples with a growing skills gap even amid layoffs. As organizations strive to fortify their digital ramparts against the ever-evolving threats, they yearn for seasoned professionals who can serve as stalwart guardians. This intriguing juxtaposition of job cuts and unfilled positions paints a dissonant picture, raising the question: are we unintentionally shunning the guardians we need the most to safeguard our digital landscape?

Threat actors, untroubled by the economic constraints shackling their corporate counterparts, are advancing their techniques. Statistics spotlight a trend that sees cybercrime growing and diversifying in methodology. Ransomware, phishing, and state-sponsored attacks continue to claim headlines and serve as precursors of an emboldened criminal enterprise thriving in the shadows of cyberspace.

The cybersecurity sector's muscle contraction could not have come at a worse time. With digital transformation sweeping every facet of our lives—from smart cities to remote work—the threat landscape has broadened unprecedentedly. The sector's readiness to withstand this new wave of threats is under scrutiny. Cyber resilience is not just a business concern; it's a societal one.

How should startups and established organizations navigate the stormy waters in this economy of hesitancy? While caution in expenditure is advisable, hampering investment in cybersecurity may be like sailing the digital sea without a lifeboat.

Tips for Startups

1. Lean Innovation: In times of funding scarcity, the emphasis should be on lean, sustainable growth. Innovative solutions only sometimes require heavy investment; they need intelligent, efficient allocation of available resources.
2. Collaborative Endeavors: Partnerships can bring shared expertise and resources to the table. Strategic partnerships might be the key to unlocking doors that heavy funding once did.
3. Focus on Core Offerings: Sharpen the focus on what your solution does best. In an overcrowded market, a specialized, superior offering is more likely to receive attention and investment.

Tips for Organizations

1. Cyber Hygiene Education: With cutbacks on the horizon, empowering the existing workforce with cyber hygiene best practices can be a cost-effective defense strategy.

2. Risk Assessment: Regular and thorough risk assessments will ensure resources get allocated to protect your network's most vulnerable and critical aspects.
3. Flexible Defense Models: Employ cyber defense strategies that are as adaptable as the threats they face. This might mean investing in automated, AI-driven systems that offer long-term savings in human resource investment.

The Path Forward

The correlation between dwindling cybersecurity investments and intensifying cyber threats presents a dichotomy that demands collective resolve. As we reevaluate the role of cybersecurity in our digital future, we mustn't conflate the value of cyber defenses with the vicissitudes of economic cycles.

Cybersecurity startups must appeal to the sense of urgency that underpins their services and products, capitalizing on innovation without the reliance on extensive funding. On the other hand, organizations cannot afford complacency; the stakes of data breaches and system compromises are too high. Employing strategic, targeted investment in cybersecurity remains a high-return policy in mitigating future crises.

While current economic dynamics may force the cybersecurity sector to brace for impact, it's also a prime moment for internal reflection. How can we do more with less? How can we close the gap between threat and protection with finesse rather than brute financial force? The path ahead will test the sector's ingenuity and resilience. Amidst these trials, however, lies the opportunity to reinvent and reinforce our digital fortifications—let us rise to meet it.

In the landscape of modern threats, economic ebbs should not dictate our vigilance. Cybersecurity is not a luxury—it is essential. Let's ensure it’s treated as such for our collective digital well-being.

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 http://www.iamdavidlee.com/

What Individuals Get Wrong About Business Email Compromise

Businesses tend to obsess over business email compromise. This obsession is misguided. Observations from the front lines of combating business email compromise at the SMB scale and what we should focus on instead.

By Matt Kiely, Principal Security Researcher at Huntress

The security community tends to obsess over business email compromise (BEC) attacks. This obsession is misguided and BEC should not be getting so much attention. Instead, security companies should be focusing on more constructive topics.

As a principal cybersecurity researcher, I bear the shield and fight off cybercrime that would otherwise target and destroy the small to medium sized companies globally and the managed service providers that protect them. Most of these businesses wouldn't survive a ransomware or BEC attack. According to the FBI, business email compromise amongst smaller companies is now a $50B issue that is crushing their dreams. These are the construction companies, barber shops, bakeries and 1-off retail stores who would be devastated if they were ransomed for $500,000 or if massive funds disappeared from their banking account as a result of a fraudulent wire transfer. The stakes are high.

The point is that these attacks are worth businesses' attention and SMBs need to be defended.

Detecting Business Email Compromise Is Too Little, Too Late

In January 2023, Huntress detected over 3,300 Microsoft 365 events that indicated a compromise of a partner identity in some capacity. Any one of these incidents could result in a BEC attack that could wipe a small business out for good. But the critical thing to point out here is that very few of these detections identified the BEC attack itself. In fact, if the actual BEC attack itself is the only thing identified, this is considered to be a detection failure.

BEC is more of the “ransomware” of the cloud security world. Like ransomware, these attacks are one of the tangible, visible outcomes of a cloud cyberattack chain. The operating phrase here is “attack chain.”

These attacks don’t magically appear out of nowhere. A threat actor who’s pulled off a BEC, much like a ransomware attack, had to develop their campaign enough to execute the final phase of the attack. This means that they had to gain access to an account, install some method of persistence, enumerate the target environment, evade defenders and finally execute the steps of the BEC attack itself.

This equates to a process of an enemy spy sneaking into a maximum security base. The spy has to ballet dance through a hallway of lasers to make sure they remain undetected. Every step, every dip and every jump is another opportunity for them to mess up and trigger one of the lasers. As defenders, it's the security company's job to put as many lasers in the hallway, at various heights and angles, so that the spy’s mistakes are detected and punished.

This is why companies are getting BEC all wrong; since they tend to watch business email compromise attacks unfold as if there’s no way to prevent them from happening. It’s not a good practice to watch the train careening down the tracks towards the cliff side with their jaw on the floor, saying, “Someone should really do something about this!” Defenders should realize it’s their place to take action and pull the lever to reroute the train.

Any threat activity that takes place before the BEC attack itself is a good place to look to forestall these attacks. A great place to look for indicators is right when the threat actor gets their foot in the door—initial access. “Account takeover” is the most common method of initial access, where a threat actor has passed or stolen the authentication requirements and simply logs in as the given identity. There are more ways to gain initial access to an identity than just account takeover, but it is the most common method by a wide margin.

Hunting Account Takeovers at the SMB Scale

Focusing on BEC is like focusing on the train after it gets wrecked. Maybe you want to join me in the hunt for account takeovers so we can cut off the BEC attack closer to the start. But where do we start? How can we effectively deter these attacks if we don’t understand them first?

String up your bow and sharpen your arrowheads. Here are three of the major adversary tactics that result in account takeovers.

Adversary in the Middle: Transparent Proxy Phishing

One of the worst tactics in the adversary playbook is session token theft via transparent proxy phishing. This attack is insidious. Our partners often ask, “Now that I’ve implemented multi-factor authentication on my account, I should be safe, right?” Transparent proxy phishing is the reason why experts can’t answer “yes” when they ask that question.

The premise for this attack is simple: multi-factor authentication (MFA) would stop an attack in progress given that the adversary doesn’t possess the additional authentication factor at the time of the attack. But most modern websites, including the Microsoft 365 login portal, grant a session token to the user after the user logs in with their password and provides their additional factor for authentication. Once that session token is in the user’s browser, it becomes a de facto proof of identity for that user. So, why not steal that session token instead?

The adversary tricks the victim into visiting their attacker-controlled domain. When the victim visits this domain, usually after receiving a phishing email with a link that directs them there, they see the Microsoft 365 login portal. The victim figures there’s some weird error going on and they need to log back into Microsoft 365. Unfortunately, they’re entering their credentials into a transparent proxy, which brokers the victim’s session with the actual Microsoft 365 page.

The victim enters their password, which is captured by the evil server in the middle. The evil server relays the password to the real Microsoft 365 login site, which passes the first authentication stage. Microsoft 365 then requests the additional factor, which is relayed back to the victim through the evil server. When the victim completes the additional factor, the session passes authentication and the resulting session token is delivered to the victim’s browser…by traveling through the evil server! The adversary effectively captures the session token while it’s on its way back to the user and can inject it into their own browser to log into the victim’s account. Dastardly!

Much like the classic vampire of legend, these attacks can’t hurt individuals or businesses unless they’re invited in. Social engineering is still the primary method for delivering the links that result in a user landing on one of these transparent proxy login pages. The URL of the site in question is still the most trusted source to determine if the website is legitimate or not. For example, a user who wants to log into Microsoft 365 should expect to land on “login.onmicrosoft[.]com” and not “some.evilsite[.]com”.

End users in regards to this attack should keep a healthy amount of suspicion for the links that people are asking you to click. Verify with the person that’s supposedly sending you this link. Did they actually send it? Is there urgency about the situation? Have they tried to build rapport with you to coerce you into clicking? This attack can compromise even the hard targets who protect their accounts with MFA, so it’s worth the due scrutiny and time needed to verify.

Credential Attacks: Password Sprays, Credential Stuffing, Brute Forcing

For individuals out there who don’t use MFA, the threat equation is much more simple. For any accounts that don’t have an additional factor, an adversary would either have to guess or acquire the victim’s password to log in as that identity. These credential attacks come in three flavors; password spraying,

where the attacker tries to guess the same password against multiple accounts; credential stuffing, where the attacker uses known credentials from a breach and uses them against other services where the user may have an account; and brute forcing, where the attacker guesses multiple passwords against the same account.

Unlike the adversary in the middle attack example from earlier, this attack requires no interaction on the part of the victim. Tools like MFASweep and trevorspray, which are both available free and open source on GitHub, allow attackers to carry out credential attacks and check to see if any accounts lack MFA. An attacker that finds an account with a weak password and no MFA has found a prime target for a business email compromise attack.

VPN use for initial access

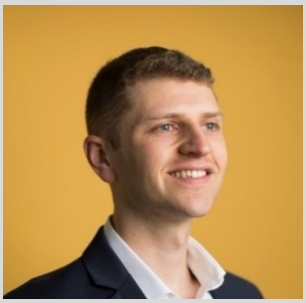
This tactic is more closely aligned with defense evasion than initial access, but it's included here because it's a common attribute of account takeovers. According to reports from the Huntress Security Operations Center, about 75% of confirmed attacks against Microsoft 365 identities come from VPNs. A smaller percentage of attacks come from anonymous proxies, like Tor. While VPNs and proxies are different technologies, it's considered that they are similar in terms of impact to partners. Threat actors use proxies and VPNs to conceal their IP address while performing account takeovers.

Like a good jiu-jitsu counterattack, security businesses can use this tactic to their own advantage as defenders. Is VPN use normal for their users? If VPN is normal, which types of VPNs should be in use? Analyzing the IP address from the login can reveal key facts and intelligence that they can factor into the threat calculus, like the IP's service provider or if the IP is a known exit node for a shady proxy service. This allows them to differentiate between a user who logs in while using a common corporate SASE solution and a user who logs in from Tor. These two events aren't the same in terms of risk and good detection programs should be able to recognize it and act accordingly.

Conclusion

Taking a bite out of BEC is about forestalling adversaries at any point along the attack chain. Identifying and combating tactics that indicate different phases of the attack chain, like persistence, defense evasion and execution activity, is an effective means of combating business email compromise. Every phase of the attack chain can telegraph different indicators and presents opportunities for detection. It only takes one detection to halt what would otherwise be a business-ending event. For businesses' own security programs, maybe initial access is a great initial place to look!

About the Author



Matt Kiely is a Principal Security Researcher at Huntress developing products that hit hackers where it hurts. He currently leads MDR for Microsoft 365 product research. He is a skilled cyber expert with over 10 years of experience in IT and security working for organizations including: Massachusetts Institute of Technology, financial institutions, SimSpace, and the United States Marine Corps. Matt holds a Bachelor of Science in Information Technology from Northeastern University and a Graduate Certificate in Cybersecurity from the Rochester Institute of Technology. Some of Matt's professional credentials include OSCP, eCPPT, eCPTX, CRTO, and CRTP Matt can be reached online at our company website https://www.huntress.com/.

CES: AI at the Forefront of Cybersecurity's Future

Examining the Increased Use of Artificial Intelligence in Cybersecurity

By Matthew Taylor, Vice President of Projects, and Engineering, MxD

The annual Consumer Electronics Show (CES) is the world's largest consumer technology trade show, acting as a global stage for technology giants and industry leaders to convene and showcase their latest innovations and ideas. Many manufacturing companies attended CES to learn about the emerging technological trends impacting the business world. From artificial intelligence (AI), to cybersecurity, this year's CES examined how digital technology integrations are reshaping the future of manufacturing, a trend that MxD has been at the forefront of for years.

AI's ability to learn, adapt, and predict behavior makes it an indispensable tool in the ongoing cyber battle, resulting in its emergence as a leading discussion topic at CES. As the manufacturing sector has surpassed all industries as the most targeted sector for cyber-attacks, the potential of AI to bolster manufacturers' cyber defense capabilities has taken on both greater urgency and greater potential. Already, cybersecurity experts use AI to identify and guard against vulnerabilities online. We expect this trend to continue, with AI playing a pivotal role in safeguarding against cyber-attacks by predicting threats,

conducting behavioral analysis to best monitor and detect unusual activity and adapting threat intelligence with countermeasures.

As companies embrace digital innovations, AI remains a key ally in protecting sensitive data. Manufacturers must fortify their defenses against data breaches, ransomware and supply chain vulnerabilities. IBM reported that, in 2021, the manufacturing industry replaced the financial services sector as the industry with the most cyber-attacks. Robust cybersecurity measures are essential to maintain trust, safeguard intellectual property and ensure uninterrupted operations.

However, despite its promise, several CES panelists warned that AI also poses threats around cyber-attacks. Though AI can be an invaluable tool in protecting a company's confidential data, in the wrong hands, it can also be used to create deepfake attacks, which have become more prevalent. Because of this, there is a need to upskill the current workforce to not only recognize these attacks, but to also know how to respond to them.

But meeting this need will be difficult: many small or medium-sized manufacturers do not have a dedicated IT team, or someone in the chief security or technology officer position, in addition to other unfilled positions. In fact, more than 80% of manufacturing companies are experiencing a labor shortage, according to the Women in Manufacturing Association. What's more, the World Economic Forum reports that more than half of all employees will need to be upskilled or reskilled by next year to prepare for the anticipated increase in automation and AI.

Beyond AI, CES also highlighted how important digital modernization is for the supply chain, evaluating how new technologies play a pivotal role in enhancing supply chain logistics and impacting how goods move from manufacturers to consumers. CES recognized the importance of resilient supply chains and showcased technology, such as AI integration, that will help companies become more cyber prepared.

This conference underscored the urgency of embracing digital transformation in manufacturing. Many digital tools are no longer optional; they are vital for companies to survive and grow. As facilities become smarter, more connected, and more data-driven, manufacturers need employees who are trained to use the technology. CES showed the need for robust supply chain solutions, emphasizing both security and agility in an ever-evolving technological landscape.

About the Author

Matthew Taylor is the Vice President, Projects, and Engineering of MxD. He leads the Institute's Projects and Engineering team, which includes the Project Management Office (PMO), Cybersecurity and IT, Workforce Development, and Engineering. He also works closely with teams across MxD and its industry partners to ensure the MxD Future Factory floor delivers maximum value for members, as we collectively work to demystify new technologies and apply them to strengthen America's manufacturers and supply chains.

Prior to joining MxD in October of 2022, his background spanned the semiconductor industry, as well as aerospace and defense - gaining hands-on experience across the entire product lifecycle. At Teradyne, Raytheon, Northrop Grumman, and ManTech International, he demonstrated a track record of success as a technical fellow, manager, and architect in several functions including digital engineering, project management, functional management, strategy, innovation management, and supply chain. Matthew holds a Master of Science in Engineering Management from Tufts University, and a Bachelor of Science in Computer Engineering from the University of Illinois, Champaign-Urbana. Matthew can be reached online at LinkedIn and at our company website https://www.mxdusa.org/.

Crypto Kaleidoscope: Investing in Colorful Coins, Living a Vibrant Life

By Thea Payne

In the ever-evolving landscape of cryptocurrency, investors are constantly on the lookout for the next big thing. While Bitcoin and Ethereum dominate the headlines, a new trend is emerging – the rise of colorful coins. These vibrant digital assets not only promise potential returns but also add a splash of diversity to your investment portfolio. In this article, we will explore the world of colorful coins and how investing in them can mirror the vibrancy of a colorful life.

The Allure of Colorful Coins

Just as a kaleidoscope presents a mesmerizing array of colors and patterns, colorful coins in the crypto world offer a diverse range of options. These coins are often characterized by unique features, innovative technologies, and, of course, eye-catching logos and branding. Investors are drawn to the potential for high returns, but there's more to these coins than meets the eye.

Diversifying Your Investment Palette

In the world of traditional investments, diversification is a key strategy for managing risk. The same principle applies to the crypto market. Colorful coins provide an opportunity to diversify your investment portfolio beyond the more established cryptocurrencies. By allocating a portion of your investment to these unique and lesser-known assets, you can potentially enhance the overall stability and resilience of your portfolio.

Exploring the Rainbow of Options

The crypto market is teeming with colorful coins, each with its own story and value proposition. From Ripple's XRP, often associated with the color blue, to Litecoin's silver hues, these coins bring a spectrum of options for investors. It's essential to conduct thorough research, considering factors like technology, use case, and community support, to make informed investment decisions.

1. Ripple (XRP): The Calm Blue Ripple

Ripple, often represented by the color blue, aims to revolutionize cross-border payments. With its focus on speed and cost-effectiveness, XRP has gained attention from both financial institutions and individual investors.

2. Litecoin (LTC): Silver Shines Bright

Litecoin, represented by a silver color palette, positions itself as the "silver to Bitcoin's gold." Its faster transaction times and lower fees make it an attractive option for everyday transactions.

3. Cardano (ADA): The Green Revolution

Cardano, represented by the color green, focuses on sustainability and scalability. With its commitment to environmental responsibility, ADA aims to provide a platform for the development of decentralized applications.

Living a Vibrant Life Through Crypto

Investing in colorful coins is not just about financial gains; it's about embracing a vibrant and dynamic approach to life. These investments encourage investors to stay curious, explore new opportunities, and embrace diversity. The crypto kaleidoscope reflects the ever-changing nature of the market, encouraging individuals to be adaptable and open-minded.

The Art of Timing and Patience

Like the patterns in a kaleidoscope, the crypto market is subject to constant change. Successful investors in colorful coins understand the art of timing and patience. While some coins may experience rapid growth, others may take time to reveal their true potential. Patience, coupled with a strategic approach, is crucial for navigating the dynamic crypto landscape.

Risks and Challenges in the Colorful Crypto World

While the allure of colorful coins is undeniable, it's essential to acknowledge the risks and challenges associated with these investments. The crypto market is known for its volatility, and colorful coins may be more susceptible to price fluctuations. Investors should approach these investments with caution, conducting thorough due diligence and only investing what they can afford to lose.

Incorporating Cosmos Staking into Your Investment Palette

As you diversify your crypto portfolio with colorful coins, consider allocating a portion to Cosmos and engaging in staking. Cosmos Staking offers a unique avenue for investors to not only potentially increase their holdings but also actively contribute to the growth and governance of the Cosmos Network. Keep in mind the following steps to incorporate Cosmos Staking into your investment strategy:

Research Validators: Select validators carefully, considering factors such as reputation, performance, and fees. Validators play a crucial role in the staking process, and choosing reliable ones enhances the overall staking experience.

Understand Staking Risks: While staking provides the opportunity for rewards, it's essential to be aware of the associated risks. Price volatility, network upgrades, and validator performance fluctuations are factors that can impact staking outcomes.

Regularly Monitor Your Portfolio: Stay informed about the performance of your staked ATOM tokens and adjust your staking strategy as needed. Monitoring the market and staying updated on Cosmos Network developments will help you make informed decisions.

Explore Additional Staking Options: Beyond Cosmos, explore other staking opportunities within the crypto market. Diversifying your staking activities across different networks can further mitigate risks and enhance your overall staking experience.

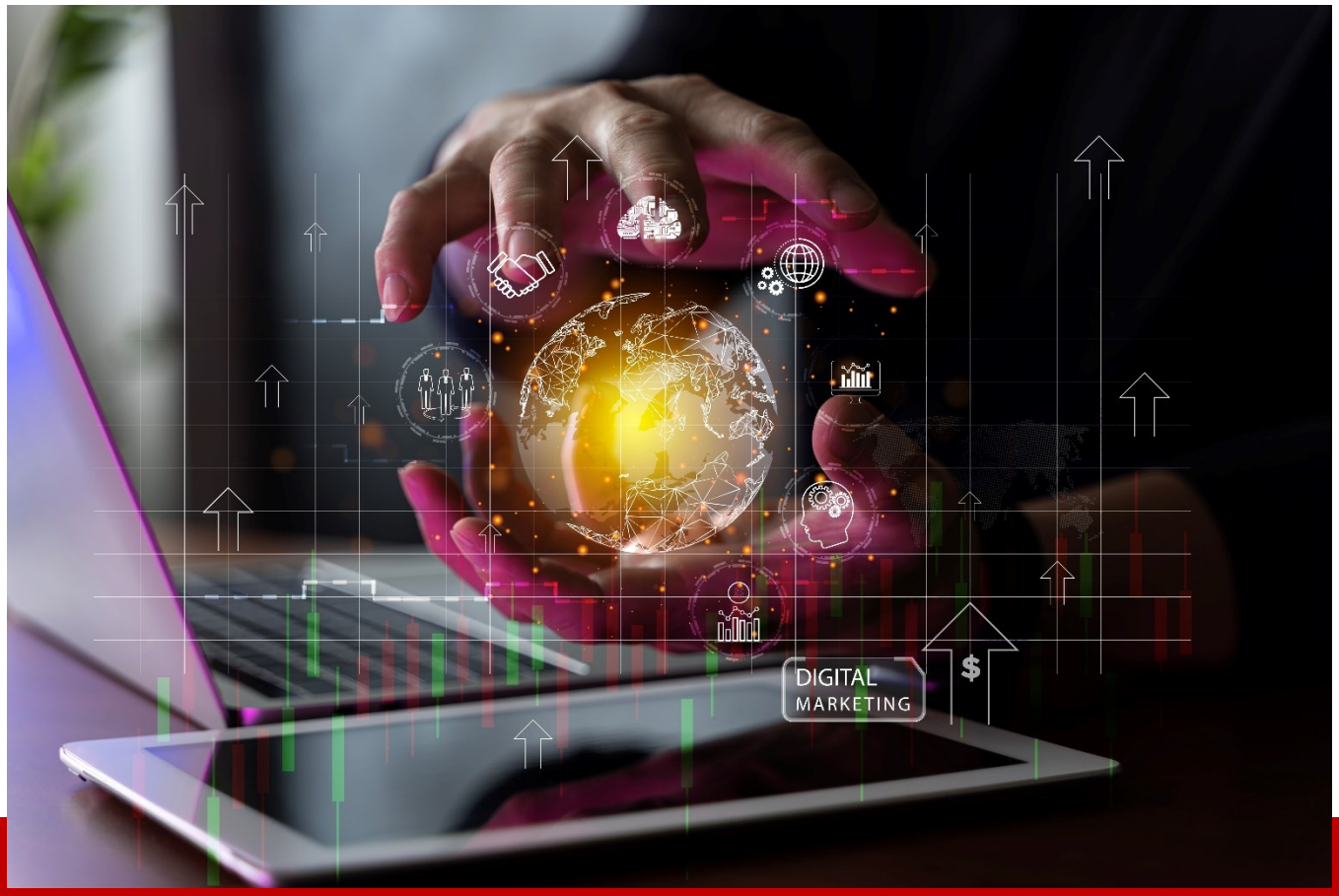
Incorporating Cosmos Staking into your colorful coin portfolio adds a sturdy pillar that not only contributes to potential financial gains but also actively supports the decentralized vision of the Cosmos Network. As the crypto kaleidoscope continues to evolve, Cosmos stands as a beacon for those seeking both stability and active participation in the dynamic world of cryptocurrency.

Conclusion: Painting Your Financial Future

In the grand canvas of the financial world, colorful coins add a unique and vibrant touch. Embracing the kaleidoscope of options in the crypto market allows investors to paint a diverse and dynamic financial future. As with any investment, it's crucial to balance risk and reward, stay informed, and approach the market with an open mind. By investing in colorful coins, you not only participate in the exciting world of cryptocurrency but also infuse your financial journey with the vibrancy of a kaleidoscopic life.

About the Author

Thea Payne is a dynamic and passionate tech enthusiast whose journey in the ever-evolving world of technology has been nothing short of inspiring. Born with an innate curiosity and a natural affinity for all things digital, Thea's story is one of constant exploration, learning, and innovation. She has been at the forefront of innovative projects, leveraging emerging technologies to address real-world challenges.



Cryptographic Protocol Challenges

By Milica D. Djekic

The communication protocol is an information exchange method where data are transferred only if two or more networking devices deal with a set of the rules being in a strict order and provide an access to those willing to cope with a previously defined coding algorithm that is applied to obtain a data transmission only if all sent and received bits within a digital system are as commanded. The entire technology of producing communication protocols can be quite costy and time-consuming as there is a strong need for engineers, developers and data scientists that must make something functional and cost-effective for a reasonable period of time getting in such a way an optimal software or hardware which will allow a griding only if there is a totally predicted condition for such a querying exchange, so far. On the other hand, in a case of the cryptographic protocols it is needed to have a crypto-queries making such a communication and some brief insights regarding that solution are given in this paper trying to explain how it is feasible to offer something that will truly operate in an accurate and efficient manner.

Throughout a time, there have been a number of protocols which are not seriously correlated with the modern technological landscape, but more likely a physical domain starting from military behavior models, over some parade ceremonies unless ICT infrastructure brining to the global communities an entire new wave of industrial, business and social endeavors, so far. The major thing with the protocols and protocoling dealing is a certain set of rules must be applied in order to satisfy some condition which will further let those being involved in such a ceremony obtain what it is really needed to be done. The overall Universe functions by the laws of mathematics and physics and it's not unusual to notice such rules among some biological systems which also vibrate as the nature makes them to do so and indeed, that sort of findings have inspired a total engineering community to via investigating the living things use some of such collected ideas to provide a completely novel multidisciplinary approach to some of their advancements making a well-balanced synergy between natural and social sciences. Apparently, cryptology is a field which makes a union of the cryptography and cryptanalysis giving an opportunity to researchers and practitioners in that area to do their best in order to design a fully innovative cryptosystem which can transform a series of the bits from plaintext into ciphertext, send such an encrypted message to its destination and finally decrypt it once the information is gathered, so far. In other words, in a sense of the behavior modelling science, a computer engineering also follows that logics to get defined how some of their objects will behave in a technical fashion making a clear linkage between several disciplines of the science.

The protocoling behavior is something which exists since the ancient times as it has always been a need to cope with some rules putting stuffs into order and organizing some everyday activities in a logical fashion as some of the first cryptosystems had been made with that epoch in a history, so far. Next, even in those times there had been some message protection tools which served for an army secret communication, while with the World War 2 there have existed some technical cryptosystems which have dealt with a key distribution challenge and as it is well-known, such a practice is present even nowadays as the majority of the military forces still rely on a key cryptography looking for good mathematical models, as well as encryption algorithms. In addition, there is also a shift from key to strong encryption as some experiences suggest that the world is yet on a search for the perfect secrecy being a cryptography which could genuinely change a defense landscape being available today. On the other hand, the communication protocols being accessible at the present cope with an electronic signal either analog or digital and in such a sense, some data transfer within networking devices is possible only if all members of the grid behave in a flawlessly ceremonial manner attempting to allow a communication between objects only if a fully accuracy of the exchanged protocol messages is accomplished, so far. Also, if there is a word about the cryptographic protocols it is obvious that in such a case, the devices in a grid talk using encrypted signal and if all bits fit perfectly the data transmission will be allowed. In that case, it is necessary to figure out that those systems deal with crypto-queries that are encrypted at sending spot and decrypted at some destination letting some ciphertext to be pushed through the protocol communication.

In other words, such a behavior will be assured from those trying to cope with so externally and any opponent watching so from an outside will not be in position to read that questioning and at least to make some connecting with the network dealing with a cryptographically protected protocol which means those objects will behave in the gloves making their dealing being hidden from the rest of the audience. Indeed, that kind of the communication can be illustrated with the courier's sending of the message where any receiving of the letter must be confirmed seeking from the receiver a proof of the trust in order to get

delivered such information, so far. Further, if the courier is not getting accurate feedback the message will not be distributed and in other words, if one device in the network cannot have a rapport with another object in the grid no data transfer will be allowed. Moreover, if a protocoling between some networking is good, signal will go through, while if not those objects will never talk to one another, so far.

It seems there was a long time from the very first ancient cryptographic tools until this modern practice which mainly relies on some engineering capacities transmitting either open or encrypted signals via some communication systems giving a chance to those taking advantage over such abilities to recognize each other's behavior within some information transmission solution. In other words, communication protocols can be assumed as a way of the appropriate dealing and only if both sides are happy with one another's manners, they will make a communication, while if not – they will remain silent about each other even if they can cope with each one face-to-face. In other words, if everything is not in a perfect condition, the message will not go on to anyone. The main challenge with the modern communication protocol is it can be pretty vetting-requiring to design such software or hardware as those dealing with cryptology must be highly knowledgeable and very experienced to get entrusted with such a project as only well-confirmed persons with a plenty of the skills are capable to obtain such a task, so far. Hence, it is needed to think a bit about how it works in a digital system designing a two-way communication counting on the arrays of the bits which travel through the information packets and truly need a great degree of the knowing of the data science and programming in order to make everything being operatable and accurate. Finally, the main imperative with the ongoing data science, computer engineering and coding algorithms is to gain a strong application with cryptology getting in mind all pluses and minuses of the current both – cryptography and cryptanalysis which must be used in a totally rational and responsible way as those creating a highly sophisticated weapon should undoubtedly think about an adequate counter-weapon letting those using both of them stay safe and secure at the same glance.

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.

These Critical SEC Cybersecurity Disclosure Rules Questions are Finally Being Answered

Clarity on What Your Reporting Should Cover

By Christopher Salone, Consulting Manager & Financial Services Practice Leader at FoxPointe Solutions

Last Summer, public companies prepared for the finalization of the U.S. Securities and Exchange Commission (SEC) rules regarding Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies. The initial publishing of these rules left many business leaders with more questions than answers, including how to maintain compliant and effective reporting practices for material cyber incidents.

Fast forward to 2024, the rules having been in effect for several months, and business leaders are still faced with some common misconceptions and challenges understanding their compliance expectations. Thankfully, faced with discourse and confusion, the SEC has released clarifying points to aid leaders in this new reporting process.

Below are answers to the two most critical questions business leaders have been asking about the new disclosure rules since implementation:

There are Two Major Components to Compliance.

To make compliance as simple as possible for business leaders, it is best for them to focus on the two major components of the rule. The first being that public companies are now required to disclose both material cybersecurity incidents within 72 hours on new item 1.05 of Form 8-K. This means that public businesses must have a plan in place for swift investigation and reporting in the hours following a cybersecurity material incident. Best practices for doing so include assigning a team or task force focused on mitigating incidents as they occur, as well as managing the completion of proper documentation in the aftermath. This information should also be shared with investors and key stakeholders in a timely and consistent manner.

Secondly, the rule requires the reporting of material information regarding cybersecurity risk management, strategy, and governance on an annual basis. This reinforces the critical need for creating, adapting, and executing formal cybersecurity response plans, led by a dedicated team.

Reporting Should Cover the What, When & Why.

So, you had a material incident occur. What do you need to include in your report? This is the question that has been top of mind for leaders since the rule was first proposed in March 2022. Thankfully, in recent months, the SEC has provided more context to what they are looking for in official incident reports, and it's simpler than you would expect. Basically, your report should cover three questions: what, when and why?

What?

For starters, public companies must describe the nature, scope, and timing of the material incident, as well as the current or likely material impact. A material impact is defined as a consequence that has a negative impact on corporate financial position, operation, or customer service. Companies need not get too specific in the technicalities of the breach so as not to leave them vulnerable to future cyber incidents.

When?

As for the "when," prior to the rule taking effect, there was a lot of discourse over the expectation of a rapid turnaround of reporting following an incident. However, it has since been clarified by the SEC that the discovery of a cyber incident is NOT the triggering event for the 72-hour reporting deadline, but rather the determination that the breach was a material incident. That means that, following a breach, a company can do the proper due diligence of investigating the breach, interviewing staff, and working with vendors and third parties to conclude the incident was material before the countdown to disclose begins. Exceptions are made and reasonable delays are awarded in situations where companies do not have the paperwork or details available to file a report in that time frame.

Why?

Leaders are also finally getting clarity on the "why"? More information has been shared to shed light on the materiality standard for this rule, and in short, it's meant to protect the needs of investors to make sound decisions about buying or selling. In official terms, according to the SEC and the Supreme Court, "The term 'material,' when used to qualify a requirement for the furnishing of information as to any subject, limits the information required to those matters to which there is a substantial likelihood that a reasonable investor would attach importance in determining whether to buy or sell the securities registered."

As public companies continue to put these rules into practice, it's important to keep an open dialogue with the SEC about any reporting questions remain in order to ensure you remain compliant. Working with a consultancy with expertise in compliant reporting is another great way to ensure that reporting is done in a timely, efficient and accurate manner.

About the Author

Christopher Salone, CISA, MBA, CCSFP is a Consulting Manager and Financial Services Practice Leader of FoxPointe Solutions, the Information Risk Management Division of The Bonadio Group. His work focuses on internal and external auditing of information technology and information security practices and controls, providing services to clients across multiple industries, including public and private companies, financial institutions, healthcare organizations, tech companies, and school districts. He conducts audits in accordance with regulatory compliance standards. Christopher can be reached online at csalone@foxpointesolutions.com and at our company website www.foxpointesolutions.com.

Securing The Stars: Addressing Cybersecurity Challenges in Space Exploration

The Evolving Landscape of Threats Beyond Earth's Atmosphere

By Sylvester Kaczmarek, Chief Technology Officer, OrbiSky Systems

Humanity's gaze has always been drawn to the stars, and in recent years, space exploration has experienced a remarkable resurgence. From ambitious public missions to a burgeoning private space industry, our presence beyond Earth's atmosphere is rapidly expanding. But amidst this thrilling progress lurks a shadow: the growing vulnerability of space assets to cyber threats.

Once confined to science fiction, the possibility of cyberattacks in space is now a stark reality. As our reliance on satellites for communication, navigation, and even critical infrastructure increases, so too does the potential damage from a successful cyber intrusion. This article delves deep into the complex and evolving landscape of cybersecurity in space exploration. We'll explore the diverse threats targeting satellites, spacecraft, and other celestial assets, examining recent incidents and their chilling implications. We'll then analyze the unique vulnerabilities of space technology compared to terrestrial systems, highlighting the challenges defenders face in safeguarding this critical domain.

This exploration is not merely an academic exercise. Understanding the cyber threats in space is essential for ensuring the security and sustainability of our future endeavors beyond Earth. From protecting essential infrastructure to safeguarding scientific exploration, robust cybersecurity measures are now an indispensable part of any successful space mission. By raising awareness and fostering

collaboration, we can ensure that the stars remain a canvas for exploration, not a battleground for digital adversaries.

Landscape of Cyber Threats in Space

The threatscape in space is as vast and diverse as the cosmos itself. Unlike traditional terrestrial systems, space assets face not only the usual suspects like malware and data breaches, but also unique challenges due to their remote location, harsh environment, and limited resources. Let's delve into some of the most prominent cyber threats targeting our celestial assets:

1. **Satellite Hacking**
   Satellites are the backbone of our space-based infrastructure, providing critical services like communication, navigation, and Earth observation. However, their reliance on radio-frequency communication makes them vulnerable to interception and manipulation. Hackers can exploit weaknesses in satellite protocols or encryption to gain unauthorized access, potentially disrupting services, stealing sensitive data, or even taking control of critical systems. For instance, incidents of satellite signal jamming have demonstrated the practical risks involved.
2. **Data Breaches**
   Just like any networked system, space assets are susceptible to data breaches. Sensitive information collected by satellites, such as scientific data, military intelligence, or financial transactions, can be targeted by cybercriminals for espionage, financial gain, or even sabotage. The breach of satellite operator data, revealing sensitive communication, underscores the gravity of this threat.
3. **Supply Chain Attacks**
   The complex supply chains involved in building and launching spacecraft create vulnerability points that attackers can exploit. Malicious actors could introduce malware into software or hardware during development, compromising systems before they even reach orbit. Highlighting the risk, the aerospace sector has seen instances where compromised components were discovered before launch.
4. **Mission-Critical System Manipulation**
   The most chilling scenario involves attacks targeting the delicate control systems of spacecraft. By manipulating navigation or propulsion systems, hackers could cause catastrophic damage or even weaponize these assets, posing a significant threat to national security and international cooperation. The theoretical risk of such intrusions has led to increased scrutiny of spacecraft control systems' security.

These are just a few examples of the diverse cyber threats lurking in the cosmos. Recent incidents have served as stark reminders of the potential consequences. In 2017, a US satellite experienced a disruption in its communications for several hours. While this incident was initially thought to be the result of hackers, it was later clarified that the disruption was not confirmed to be a cyberattack. Nonetheless, this event highlighted the vulnerability of these critical assets. As our dependence on space-based infrastructure grows, so too does the potential impact of successful cyberattacks, making robust cybersecurity measures more crucial than ever.

Navigating the Challenges of Space Cybersecurity

Securing space assets presents a unique set of challenges compared to terrestrial systems. The vast distances involved make real-time intervention or repairs nearly impossible. The harsh environment of space, with its radiation and extreme temperatures, can degrade hardware and software, creating additional vulnerabilities. Moreover, resources like power and bandwidth are often limited on spacecraft, posing constraints on traditional cybersecurity solutions.

Traditional Solutions, Limited Impact

Firewalls, intrusion detection systems, and encryption, the mainstays of terrestrial cybersecurity, have limited effectiveness in space. The latency caused by vast distances can render real-time threat detection and response impractical. Additionally, the unique hardware and software used in space systems may not be compatible with off-the-shelf security solutions. This gap necessitates a rethinking of cybersecurity strategies that can operate effectively within the constraints of space operations. For instance, adapting existing protocols to function over longer distances without compromising their efficacy or exploring new models of secure communication tailored for the space environment are critical areas of development.

Innovation on the Horizon

However, the challenges are not insurmountable. Innovative approaches and emerging technologies are paving the way for a more secure space domain:

- **AI-powered Anomaly Detection**

By analyzing telemetry data for unusual patterns, AI algorithms can identify potential cyber threats in real-time, even with limited bandwidth. This approach leverages machine learning techniques to adapt and improve over time, offering a dynamic defense mechanism that can anticipate and mitigate threats before they escalate. The application of AI in this context not only circumvents the limitations posed by latency and bandwidth but also introduces a level of predictive analysis that was previously unattainable. It is important to note, however, that AI systems require substantial training data to be effective and can be susceptible to biases, which might limit their utility in novel or rapidly evolving threat scenarios. Ongoing refinement and oversight are necessary to maximize their effectiveness and ensure they adapt to the unique context of space operations.

- **Quantum Cryptography**

Utilizing quantum mechanics, this technology offers unbreakable encryption, safeguarding communication and data from interception. Quantum key distribution (QKD) exemplifies this innovation, providing a secure method to exchange encryption keys over long distances without the risk of compromise. While quantum cryptography holds great promise for revolutionizing secure communications, it's pertinent to acknowledge that it is still in the early stages of development and has not yet seen widespread deployment in space systems. The practical implementation of quantum cryptography in space communications will require further advancements and testing to ensure its viability and reliability in the unique challenges of the space environment.

- **Self-healing Systems**

Inspired by biological organisms, these systems can autonomously detect and repair software glitches or hardware failures, reducing reliance on remote intervention. The development of such systems incorporates advanced diagnostics and recovery protocols that can preemptively address vulnerabilities or operational anomalies. This capability not only enhances the resilience of space assets but also extends their operational lifespan, offering a sustainable solution to the challenges posed by the inaccessible nature of space environments. However, it's crucial to clarify that while the concept of self-healing systems is promising, their actual development and deployment in space environments are still under exploration. The effectiveness and robustness of these systems in dealing with the complex conditions of space will depend on continued research and real-world testing.

These innovations represent just the forefront of what's possible in space cybersecurity. As we continue to explore and inhabit space, the evolution of these technologies, along with international collaboration and regulatory frameworks, will be pivotal in securing the final frontier.

Collaborative Security in Space

The stakes are high. A successful cyberattack on space infrastructure could have cascading consequences. Disrupted communication networks could cripple economies, while manipulated navigation systems could endanger air travel and critical infrastructure. Weaponized spacecraft could even escalate international tensions, leading to a new kind of warfare that extends beyond Earth's atmosphere. The potential for these attacks to undermine national security, disrupt global supply chains, and compromise the integrity of critical defense and commercial systems underscores the strategic importance of space assets as part of our global infrastructure.

Cooperation Key to Celestial Security

The vastness of space transcends national borders, demanding a global response to cyber threats. International cooperation is crucial for:

- **Sharing cyber threat intelligence**

By pooling resources and knowledge, nations can identify and mitigate threats more effectively. This collaborative approach enables a collective defense mechanism, enhancing the ability of all participants to respond to and recover from incidents more rapidly. For example, joint cybersecurity exercises among spacefaring nations could simulate scenarios to prepare for and mitigate potential cyberattacks on space systems.

- **Developing common security standards**

Standardized protocols and procedures can strengthen defenses across the globe. Establishing benchmarks for space system security not only facilitates interoperability among international partners but also raises the baseline for cybersecurity practices in the industry. Efforts to harmonize these

standards, such as those undertaken by the International Organization for Standardization (ISO), are crucial for ensuring a unified and effective security posture.

- **Establishing legal frameworks**

Clear international laws are needed to deter cyberattacks and hold perpetrators accountable. The development of treaties and agreements specific to space and cybersecurity, akin to the Outer Space Treaty, can provide a legal basis for cooperative defense and mutual assistance in the event of a cyber incident. These frameworks are essential for establishing norms of responsible behavior and for pursuing justice against those who threaten the peaceful use of outer space.

Collective Action Underway

Fortunately, the international community is not standing idly by. Initiatives like the UN Group of Governmental Experts on Outer Space Affairs and the Space Security Index are fostering dialogue and collaboration. These platforms allow for the exchange of ideas, strategies, and best practices, playing a pivotal role in shaping the global agenda on space security. Additionally, organizations like the European Space Agency and NASA are actively developing and implementing robust cybersecurity measures for their missions. These efforts are complemented by bilateral and multilateral agreements focused on enhancing space situational awareness, sharing threat intelligence, and conducting joint cybersecurity research and development.

The future of space exploration hinges on our ability to navigate the complex challenges of cybersecurity. By fostering innovation, promoting international cooperation, and raising awareness, we can ensure that the stars remain a symbol of human curiosity and achievement, not a battleground for digital adversaries. The concerted efforts of governments, industry, and academia are vital in this endeavor, as is the engagement of the public in understanding and supporting these initiatives. Together, we can secure the vast expanse of space for future generations, preserving it as a domain of peace, exploration, and wonder.

The Future of Secure Space Exploration

The cyber threat landscape in space is dynamic, and constantly evolving as both attackers and defenders hone their capabilities. As space exploration ventures further and technologies become more complex, new vulnerabilities will undoubtedly emerge. This necessitates continuous adaptation and innovation in cyber defense strategies. The integration of cybersecurity into the design phase of space systems, adopting a 'security by design' approach, can mitigate risks from the outset. This proactive stance is essential in an era where space operations are increasingly integral to global infrastructure.

Adapting to an Evolving Threatscape

Staying ahead of the curve requires constant vigilance and proactive measures. Continuous threat intelligence gathering, penetration testing of space systems, and regular software updates are critical to identify and address vulnerabilities before they can be exploited. The development of AI and machine

learning models to predict and counteract cyber threats in real-time could significantly enhance the resilience of space systems. Additionally, fostering a culture of cybersecurity awareness among space professionals and stakeholders is crucial for early detection and response. Establishing a dedicated space cybersecurity task force within space agencies and private space firms could centralize efforts and resources, streamlining the response to emerging threats.

Education for a Secure Future

Raising awareness about space cybersecurity goes beyond the technical realm. Educating policymakers, the public, and even the next generation of scientists and engineers about the importance of cybersecurity in space exploration is vital. Initiatives such as public awareness campaigns, educational programs, and cybersecurity workshops can demystify the subject and promote a widespread understanding of its importance. By fostering a global understanding of the challenges and potential consequences, we can build a broader collective effort to safeguard this critical domain. Collaborations between academic institutions, industry, and government agencies to develop specialized cybersecurity curricula focused on space systems could cultivate a skilled workforce ready to tackle these challenges.

A Call to Action: Securing the Stars, Sustaining Our Future

The future of space exploration hinges on our ability to ensure the security of our celestial assets. Robust cybersecurity measures are not just an option, but a necessity. By embracing innovation, fostering international cooperation, and raising awareness, we can navigate the challenges and chart a course for a secure and sustainable future in space. The establishment of international space cybersecurity forums, akin to the United Nations Office for Outer Space Affairs (UNOOSA), could facilitate dialogue and collaboration on a global scale. Let us continue to explore the cosmos with curiosity and ambition, but always with the vigilance and responsibility to secure our journey among the stars. The creation of a global space cybersecurity alliance, involving nations, private entities, and academic institutions, could marshal the collective expertise and resources necessary to protect our shared space infrastructure.

About the Author

Sylvester Kaczmarek is Chief Technology Officer at OrbiSky Systems, where he specializes in the integration of artificial intelligence, robotics, cybersecurity, and edge computing in aerospace applications. His expertise includes architecting and leading the development of secure AI/machine learning capabilities and advancing cislunar robotic intelligence systems. Read more at SylvesterKaczmarek.com

Your Company Culture Can Become a Powerful Cybersecurity Resource

By Rafael Lourenco, EVP and Partner at ClearSale

If your organization doesn't already make security a pillar of its culture, this could be the year to start. That's because the cybersecurity landscape is changing, due to factors including GenAI, new cybersecurity reporting rules for U.S. public companies, and the growing recognition that security is critical for all platforms and processes. As a result of these trends, the need for data protection, fraud prevention, and other forms of digital security are increasing across business processes and tools.

Companies that cultivate a strong culture of cybersecurity can have advantages in terms of adapting to evolving compliance and performance needs. When security thinking is part of the organization's daily life, it's often easier to adopt new best practices, adhere to new requirements, and identify potential risks and threats. Understanding the current trends and the role culture plays can help you identify your organization's strengths and areas for improvement.

GenAI is changing security needs

Online crime was already equivalent to the world's third-largest economy during the pandemic. Now, generative AI and automation give organized criminals the means to create more realistic-looking attacks, develop new types of attacks, and automate attacks at scale, even without coding and writing skills. For example, the Association of Certified Fraud Examiners site shows how easy it is to use ChatGPT to create a realistic-looking security warning email that fraudsters could use to impersonate a business and steal account login credentials.

GenAI-powered bots can also help scammers to identify high-value targets and engage with them conversationally to build trust before defrauding them. These kinds of attacks–especially when they're used to impersonate brands and ecommerce sites–have the potential to erode rising consumer confidence in ecommerce.

From 2022 to 2023, according to ClearSale's consumer attitudes survey data, the portion of U.S. and Canadian consumers who said that they had been deterred from making an online purchase because they didn't know if the online store was legitimate dropped from 52% to 24%. That's a testament to the work that businesses, payment processors, and fraud prevention teams have put into making ecommerce a safer experience.

If AI-generated impostor sites and emails succeed in defrauding a higher percentage of online shoppers, more people will hesitate before doing business with companies online. That will result in less online revenue and higher customer acquisition costs, along with a decrease in ROI on existing ecommerce investments.

Keep your culture open to GenAI's defensive possibilities

Organizations that want to detect and deflect GenAI-powered security threats need to leverage AI for defense. Because of AI's powerful pattern-recognition capabilities, it's the most efficient way to identify the subtle indicators of GenAI-created messages, other media, and sites. For example, one AI-based model for detecting insurance fraud finds three times as many fake claims as legacy fraud-screening tools.

Rather than dismissing GenAI because of its current flaws, cultivate support for properly supervised innovation with these emerging tools. That way, your organization is less likely to fall behind as GenAI threats and defenses advance.

Public companies face new security accountability

2024 is the first full year that publicly traded companies in the U.S. must disclose cybersecurity incidents within four business days of determining that an incident is material. The new rule took effect in December 2023 and requires that these incident disclosures "describe the material aspects of the nature, scope, and timing of the incident, as well as the material impact or reasonably likely material impact of the incident on the company, including its financial condition and results of operations."

Companies are not required to share technical information about incidents or their responses to them. The rule allows for exceptions when reporting would jeopardize national security or public safety. The new rule also requires public companies to annually disclose their "cybersecurity risk management, strategy, and governance" practices in terms that a prospective investor could understand.

Make clear, timely cybersecurity communication part of your culture

In many organizations, cybersecurity operates behind the scenes or keeps a tight lid on disclosures to avoid oversharing information that could be misused in the wrong hands. Caution and discernment are always important when discussing security, but these new requirements can serve as a prompt for organizations to review their incident disclosure protocols and their communication guidelines for talking about incidents and security practices. Even if your organization isn't required by law to comply with the new SEC rules, this approach can put your company in a better position to respond effectively when an incident occurs.

Cybersecurity is increasingly everywhere

With so many of our work processes, communications, infrastructure operations, and personal lives taking place online, criminals have a nearly limitless list of potential ways to attack organizations. With scammers targeting everything from government databases and telecommunications networks to social media and retail customer rewards programs, it gets clearer every year that everything digital needs built-in security.

Normalize thinking about security across the organization

Many companies that are thriving in today's economy are those that improve security for existing products or processes. That's an indicator that organizations can benefit from reviewing their technology stacks, networks, and other infrastructure to see where they have strong security and where it needs improvement. It's also a sign that everyone in the organization should be part of conversations about security at some level, including how to report concerns and what to do if there's an incident.

Embedding security in your company culture

When your company's employees and leaders are encouraged to think creatively about using technology like Gen AI for security, you're more likely to develop new strategies to combat new threats, without waiting until there's a crisis to react. When your company has policies in place for timely incident reporting and easy-to-understand security practice disclosures, you're better prepared for incidents and for inquiries from your board, potential investors, and other key stakeholders.

Finally, when you foster a security mindset across your organization, you empower each employee to look out for the company, which can reduce the likelihood of a successful social engineering attack. As new threats and regulations continue to emerge, a security-minded culture will be an asset in adapting, responding, and protecting your business.

About the Author

Rafael Lourenco is the Executive Vice President and Partner at ClearSale, a global card-not-present fraud protection operation that helps retailers increase sales and eliminate chargebacks before they happen. The company's proprietary technology and in-house staff of seasoned analysts provide an end-to-end outsourced fraud detection solution for online retailers to achieve industry-high approval rates while virtually eliminating false positives. Rafael can be reached at LinkedIn, Facebook, Instagram Twitter @ClearSaleUS, and at our company website https://www.clear.sale.

Cybersecurity Forecast

Navigating the Evolving Threat Landscape

By Jeff Krull, Cybersecurity Practice Leader, Baker Tilly

The cybersecurity landscape continues to present an ever-evolving battleground where emerging technologies and innovative attack vectors redefine the norms of digital defense. In this dynamic environment, organizations across the globe are bracing for another year that promises to stretch the limits of their cybersecurity capabilities and strategies. The following predictions delve into the key trends that will shape the cybersecurity domain, offering insights into the challenges and opportunities that lie ahead.

Vendor Risk Management Will Intensify

As businesses increasingly adopt cloud services, the complexity of their vendor networks also grows when vendors assist with key areas such as IT, software, security and operations. The interconnectedness and vendor relationships introduce significant cyber risks, particularly from third-party vendors. As we look at mature companies, the focus now extends to fourth-party vendors (meaning the vendors of their vendors).

This year organizations will prioritize enhancing their risk management frameworks, focusing on rigorous assessments and continuous monitoring of their extended supply chains. This proactive stance is crucial to mitigate the risks of supply chain attacks, which have been on the rise, as attackers exploit weaker

links in the supply chain to target more fortified organizations. While there have been some well-publicized cyber issues related to third-party vendors, generally speaking, up until now the cyber market has survived without catastrophic losses from a vendor risk management standpoint. But there's no room for complacency. All companies that work with third- and fourth-party suppliers need to make risk management a top priority this year.

Challenges in Cloud Data Recovery

We can anticipate a spotlight on the critical issue of cloud data recovery following a notable disruption event. While cloud technology offers clear cost and efficiency benefits beyond data storage and management, there are also misconceptions about cloud service providers and their clients regarding data backups and recovery processes.

Some cloud providers promise a rapid response time within 10 minutes of an attack with a three-hour window to rebuild from backups, but in the immediate aftermath of an attack, the key question is whether they can meet those promises and whether organizations have taken the appropriate steps to test recoverability on their own.

In addition to the potential "availability concern" of clouds systems, there is the importance of data backups and the resiliency of those backups. We're seeing multi-pronged approaches to implement backups of those backups as an extra layer of protection. In some instances, we've seen primary backups become infected or erased. All of this emphasizes the importance for a robust, independent data backup strategy, highlighting the potential limitations of relying on a single cloud provider for data recovery.

It is possible that at some point one of the major cloud providers is going to suffer a catastrophic outage that will take them offline for an extended period. Or, worse yet, it might be an outage they cannot recover from. Hopefully it won't take a disaster of this magnitude to create an industry wide awakening testing the recoverability of data across multiple platforms.

AI's Dual Role in Cybersecurity

Artificial intelligence has become a double-edged sword in the cyber domain. On one hand, AI technologies will empower organizations to enhance their cyber defenses, providing advanced capabilities in anomaly detection, threat intelligence analysis, and automated response mechanisms.

On the other hand, we are seeing an increase in the quality and quantity of AI-based attacks. Spoofing, emails, text messages and phone calls are being used to request credentials or entice employees to click on ransomware and phishing links. While this is nothing new, the quality of these attacks has improved significantly with AI's ability to mimic the voices, faces and other factors that are integrated into controls that secure critical systems.

The sophistication of AI-powered cyber threats is expected to rise as malicious actors develop more elusive attack methods, and we can expect a new wave of cybersecurity solutions that can anticipate and

counter AI-driven threats, as defenses attempt to remain a step ahead of the adversary. In some cases, companies may have the budget and expertise to fund a higher level of defense, ensuing an AI battle.

An Increase in Breaches and Creativity of Attacks

AI will also play a role in more creative attacks**.** When one assumes the paradigm that hackers are "running a business" and trying to make money, one can also assume hackers are reinvesting some of their cash back into their "business" to continue developing better technology and more innovative ways to breach unsuspecting organizations, thus driving up the hackers' revenue and profits.

With the aid of AI, social engineering continues to be a leading method to begin the attacks. Hackers are now using phony LinkedIn profiles and AI-generated deep-fake videos, scraping social media sites for personal information, and even communicating directly with employees who assume they are real.

Looking forward, we can expect more uses of social engineering that leverage AI to circumvent enhanced security measures that companies have spent extraordinary amounts of time and money to implement. Hackers are innovating, so it makes sense they would change their tactics, including adding multiple layers of attacks and growing forms of extortion.

A Way Forward in Cybersecurity

As we navigate through the complexities of the cybersecurity landscape in 2024, the trends outlined here underscore the imperative for organizations to remain agile and forward-thinking in their defensive strategies.

The increasing sophistication of cyber threats, propelled by advancement in AI and the expanding web of vendor relationships, calls for a comprehensive and proactive approach to cybersecurity. The stakes have never been higher. Organizations that cultivate a culture of continuous innovations and resilience will be best postured for success, managing their cyber defenses to not only respond to current threats but also be primed to anticipate and neutralize the cyber challenges of tomorrow.

About the Author

Jeff Krull is partner and practice leader of Baker Tilly's cybersecurity practice. Jeff has more than 20 years of experience in process and controls, information technology and internal audit. His expertise includes cybersecurity, IT controls, System and Organization Controls (SOC) examinations internal auditing, business process controls and specialized compliance assessments and attestations. Examples of these engagements include cybersecurity, SOC examinations, Sarbanes-Oxley compliance, internal audit, pre- and post-implementation assessments, privacy, and HIPAA risk assessments and specialized compliance attestations for clients. His client base includes a variety of industries – energy and utilities, healthcare, insurance, technology and service providers, government contractors and financial institutions. Jeff can be reached at Jeff.Krull@bakertilly.com or https://www.bakertilly.com/contact/directory/jeff-krull

Decoding the Cybersecurity Implications of Decentralized Finance (DeFi)

Blockchain users' blind faith in the system isn't paying off

By April Miller, Managing Editor, ReHack Magazine

While decentralized finance (DeFi) is still relatively new, it is well-established enough that its cybersecurity weaknesses have become clear. While it's a promising technology, the implications for users are significant.

What Is Decentralized Finance?

DeFi is an emerging financial ecosystem. It sidesteps centralized, regulated institutions like banks by leveraging blockchain and cryptocurrency solutions. Since it relies on distributed ledger technology, it enables dispersed peer-to-peer interactions.

People recognized blockchain's potential in finance almost immediately after its development. While adoption is slow, it has been catching on. Experts predict its penetration rate will increase from 0.25% in 2024 to 0.28% by 2028. Unfortunately, many of its underlying cybersecurity issues weren't realized until recently since it's a relatively new technology.

The Importance of Robust Cybersecurity

The DeFi ecosystem is becoming increasingly popular — mainstream, even. Experts believe more than 275 million people in the United States will use digital wallets by 2026. After all, most members of Gen X, millennials and Gen Z already use them.

Threat actors gain new targets as people adopt distributed ledger technology and head to DeFi platforms. Naturally, the impending popularity surge highlights the importance of a strong cybersecurity posture. Unless administrators and developers work toward a solution soon, they'll likely experience an uptick in attacks.

Common Cybersecurity Challenges of DeFi

While distributed ledger technology is safe from many common cyberthreats, it faces new, unique cybersecurity challenges.

Oracle Attacks

Oracles are third-party services connecting the blockchain to external systems, enabling them to execute code based on real-world inputs like market trends and exchange rates. In an oracle attack, a threat actor exploits their vulnerabilities to make smart contracts behave unexpectedly.

Smart Contract Vulnerabilities

Smart contracts are self-executing codes that automate certain aspects of DeFi. They trigger when predetermined conditions are met. Typically, they are essential to security and transparency. However, since they often contain vulnerabilities and bugs, threat actors trick them into repeatedly performing malicious actions.

Reentry Attacks

A reentry attack relies on a specific vulnerability. When a threat actor deposits and pulls out currency, they trick the smart contract into thinking nothing has been withdrawn. It repeatedly triggers the function, continuously draining an account until nothing is left.

Business Logic Errors

Business logic is the processes and protocols that determine how decisions are made and data is exchanged. Errors are flaws or loopholes in the rules. Threat actors can take advantage of them to cause unintended behavior, compromising others' accounts or stealing funds.

Private Key Compromise

Threat actors can exploit a single missing line of code to give themselves administrative power over a smart contract. Once they steal a developer's or administrator's private key, they can escalate their privileges and drain others' funds within minutes.

Solutions to DeFi Cybersecurity Challenges

Since some cybersecurity weaknesses are circumstantial, no one-size-fits-all solution to DeFi cyber defense exists. However, platforms can improve their security posture.

1. **Smart Contract Audits**
   A smart contract vulnerability can be as small as a bug — yet it can still drain users' funds. Routine audits can identify security gaps and indicators of compromise, protecting platforms from unintended, malicious actions.
2. **Bug Bounties**
   DeFi platforms can post bug bounties — an offer of payment in exchange for service — to encourage users to report vulnerabilities instead of exploiting them. Critical vulnerability identification only costs an average of $1,000 for nearly 70% of companies. Most people would enjoy supporting their decentralized ecosystem in exchange for cryptocurrency.
3. **Decentralized Identities**
   Decentralized identities leverage cryptography to secure credentials and personal details. They prevent threat actors from tampering with accounts while verifying users are who they say they are. They help minimize the amount of malicious behavior on a DeFi platform.
4. **Multifactor Authentication**
   Multifactor authentication prevents threat actors from accessing a user's account even if they steal credentials from an individual's wallet. Experts claim it can prevent 50% of account takeover attacks on its own. However, it's best used in combination with other methods.

The Future of DeFi Cybersecurity

Since DeFi is still an emerging ecosystem, its continued existence relies on the amount of trust users are willing to place in it. When cyberthreats drain people's funds overnight, their faith in the system sharply declines. Once they realize there is no recourse because they aren't using a regulated, centralized platform, they may choose never to return.

Sooner than later, DeFi platforms will realize they must prioritize users to ensure their long-term survival. Since they're industry disruptors, they'll likely be held to a higher standard — people will be more critical of security gaps and failings.

Consequently, platforms will likely strengthen smart contract security by leveraging cryptography and authentication measures. The future of the DeFi ecosystem's cybersecurity strategies will largely depend on individuals since many vulnerabilities are circumstantial. Only time will tell how they decide to approach the issue.

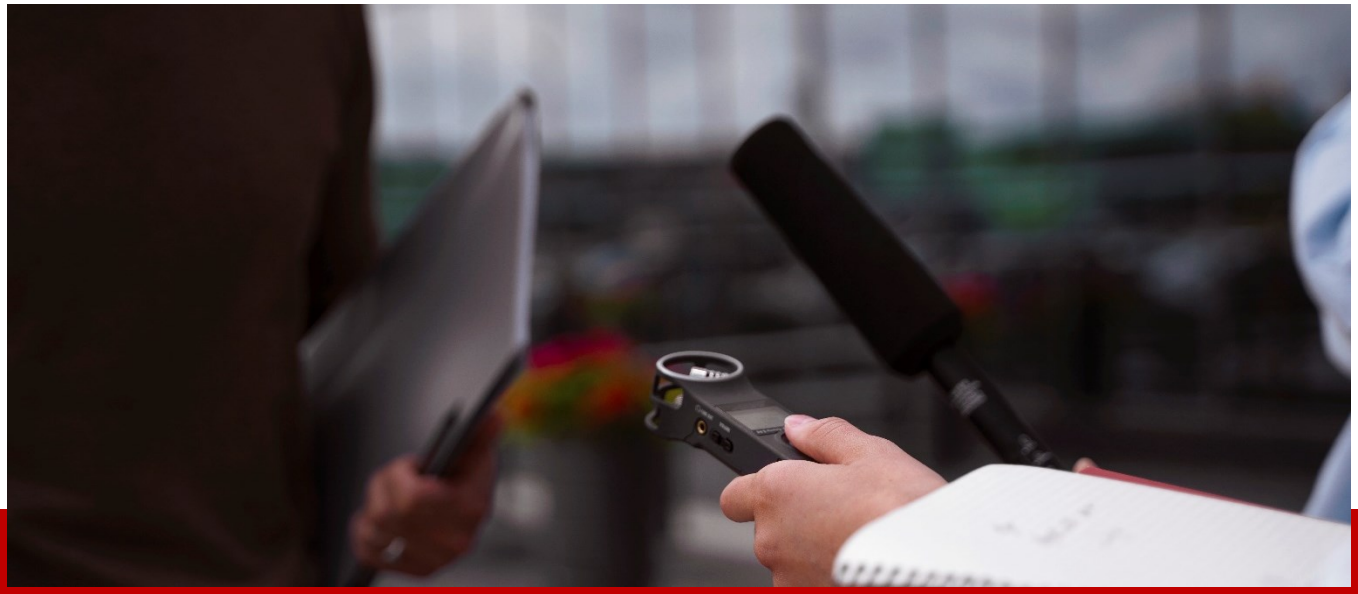
The Implications of a Strong Cybersecurity Posture

If DeFi platforms have a strong cybersecurity posture, their users will be better protected against theft and account takeover. They won't have to worry about losing all their investments to a single bug.

About the Author

April Miller is the Managing Editor of ReHack Magazine. She is particularly passionate about sharing her technology expertise, helping readers implement technology into their professional lives to increase their productivity, efficiency and personal enjoyment of their work.

April can be reached online on Twitter, LinkedIn and at our company website https://rehack.com/.



Department of Defense Publishes Long-Awaited CMMC Proposed Rule

By Richard Arnholt, Member, Bass, Berry & Sims & Adam Briscoe, Associate, Bass, Berry & Sims

On December 26, 2023, the wait was over. After more than two years of watching as the Department of Defense (DoD) abandoned its initial vision for the CMMC Program (CMMC 1.0) and announced the "CMMC 2.0" Program in November 2021, federal contractors, government organizations, and other industry groups finally laid their eyes on the new Cybersecurity Maturity Model Certification (CMMC) Program proposed rule.

The rule is designed to create a central mechanism to verify that sensitive unclassified information living on a DoD contractor's information systems is protected with adequate and standardized safeguards. It attempts to place the burden on DoD contractors and subcontractors to effectively demonstrate that sensitive information on their systems is adequately protected with the necessary security measures.

These new CMMC requirements apply to "[a]ll DoD contract and subcontract awardees that will process, store, or transmit information that meets the standards for FCI [Federal Contractor Information] or CUI [Contractor Unclassified Information] on contractor-controlled information systems." The DoD estimates that roughly 220,000 contractors, making up the majority of the defense supply chain, will need to comply with some component of the proposed rule. However, there are notable exceptions to these new requirements, including contracts or orders exclusively for commercially available off-the-shelf (COTS) items, contracts or orders valued at or under the micro-purchase threshold, and those involving "Internet Service Providers or telecommunications service providers."

Once the program is fully implemented, DoD will include in the applicable solicitation (1) the CMMC level contractors must comply with and (2) the type of assessment required to verify the implementation of the security requirements. The applicable CMMC level will be determined by DoD program managers who review the information stored and processed through a contractor's system. The type of assessment required will depend on both the applicable CMMC level and the Contracting Officer's (CO's) discretionary determination.

The CMMC will consist of three levels, each of which is detailed below.

CMMC Level 1

The first level of certification, which will apply to the largest number of companies in the DoD supply base, is CMMC Level 1. This level mandates relevant contractors comply with 15 security requirements provided in Federal Acquisition Regulation (FAR) 52.204-21. Many contractors already comply with the FAR 52.204-21 requirements and, therefore, will likely not need to implement any new protocols to comply with CMMC Level 1.

Contractors will be required to annually self-certify to the CMMC Level 1 requirements. This certification can be done by engaging a third-party certification organization (C3PAO) or using internal resources. The results of the certification must be entered in the Supplier Performance Risk System (SPRS), and a "senior official" from the prime contractor must initially "affirm" compliance and then on an annual basis thereafter.

CMMC Level 2

Many contractors are also already in compliance with CMMC Level 2 as its requirements mirror those under DFARS 252.204-7012, which ensures contractors implement the 110 security controls contained in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. Under the proposed rule, the CO is given the discretion to determine whether contracts containing the CMMC Level 2 requirements necessitate a self-assessment or a CMMC Level 2 Certification Assessment to verify the implementation of the necessary security requirements. That decision will center on the "program criticality, information sensitivity, and the severity of the cyber threat."

If a contractor is not already in compliance with CMMC Level 2 requirements, it may have to submit a Plan of Action and Milestones Requirements (POA&M), which provides a roadmap for the contractor to address areas of weakness.

The self-assessment process for verifying CMMC Level 2 requirements remains largely the same as those required to certify CMMC Level 1 requirements. The self-assessment results, as well as an initial compliance affirmation, must be submitted to the SPRS system prior to award.

On the other hand, the CMMC Level 2 Certification Assessment requires that contractors engage third-party assessment organizations to certify a contractor's compliance with Level 2 requirements. The

C3PAO itself will submit the necessary results to the CMMC Enterprise Mission Assurance Support Service (eMASS), which will, in turn, transmit the results to SPRS. The proposed rule includes an appeal process to resolve any disagreements over the Certification Assessment. Like Level 1, Level 2 similarly requires contractors to submit an initial affirmation of compliance and annually affirm its continued compliance thereafter.

CMMC Level 3

CMMC Level 3 is unlike the two prior Levels. First, it imposes several security requirements in addition to those under existing regulations. Second, the certification assessments are completed by the Defense Contract Management Agency (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBAC). Before scheduling an assessment with the DIBAC, contractors must obtain a CMMC Level 2 certification, making it a prerequisite. Like the prior level, contractors must submit an initial compliance affirmation to SPRS, a POA&M closeout affirmation if applicable, and an affirmation of continued compliance annually thereafter.

Rollout

The CMMC requirements will be implemented through four phases.

- **Phase 1 (upon the effective date of the final rule):** Will require COs to incorporate CMMC Level 1 Self-Assessment or Level 2 Self-Assessment requirements in contracts and make the award of specific contracts contingent on compliance. DoD has the discretion, under the proposed rule, to require contractors to submit a CMMC Level 2 Certification Assessment instead of Level 2 Self-Assessment for certain solicitations and contracts.
- **Phase 2 (six months after the start of Phase 1):** Will begin the formal rollout of Level 2 Certification Assessments by adding the requirement to all applicable solicitations and contracts. Under the proposed rule, the DoD has the discretion to include CMMC Level 3 Certification Assessment requirements in certain solicitations and contracts.
- **Phase 3 (one year after Phase 2 begins):** Will begin the implementation of the CMMC Level 3 Certification Assessment requirements for applicable contracts.
- **Phase 4 (one year after Phase 3 begins):** Will include CMMC requirements to all applicable solicitations and contracts. This includes option periods for awards made prior to Phase 4.

The final rollout will likely be sometime in 2027.

Consequences of Noncompliance with the CMMC Process

A major component of the proposed rule is the affirmation process, where contractors must affirm compliance initially as well as annually thereafter. These mandatory certifications present the risk of potential False Claims Act (FCA) liability for willful, or even reckless, inaccurate certifications. The FCA imposes liability on a government contractor who “knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval [or] knowingly makes, uses, or causes to be made or used,

a false record or statement material to a false or fraudulent claim." Material is defined as "having a natural tendency to influence, or be capable of influencing, the payment or receipt of money or property."

Given how the government has structured the CMMC program and its assessment requirements, it is almost certain that the government will consider inaccurate CMMC certifications "material" for purposes of the FCA. Contractors at the CMMC Level 1 and CMMC Level 2 tiers should be especially careful to ensure they fully comply with all required security assessments. FCA penalties are considerable—potentially up to three times the government's damages, plus a statutory penalty linked to inflation—and the Department of Justice has signaled an increased focus on the cybersecurity space by launching its Civil Cyber-Fraud Initiative in 2021.

Conclusion

The proposed rule provides contractors with the structure in which the three-tiered certification program will operate. Given the importance and complexity of the rule and the requirement to sift through more than 230 submitted comments, a final rule is unlikely to be published for a few months and maybe upwards of a year. However, contractors should begin digesting the requirements and consider implementing the necessary measures to comply with the obligations now, many of which mirror already-existing obligations, before the official rollout begins to ensure compliance.

About the Author

Richard W. Arnholt, a member at Bass, Berry & Sims PLC in Washington, D.C., advises government contractors on risk mitigation through ethics and compliance programs and on allegations of procurement fraud or misconduct. He can be reached online at rarnholt@bassberry.com and at our company website https://www.bassberry.com/professionals/arnholt-richard/

Adam Briscoe, an associate at Bass, Berry & Sims PLC in Washington, D.C., advises companies as they navigate the contracting process with federal, state, and local governments. He can be reached online at adam.briscoe@bassberry.com and at our company website https://www.bassberry.com/professionals/briscoe-adam/

Edge Computing Market Worth Over US$ 894 Billion By 2036

According to recent study published by Research Nester, the Edge Computing Market size is expected to cross USD 894 Billion by 2036 and is projected to expand at a CAGR of 39.65% from 2024 to 2036. The rising partnership and collaboration among the key players are to augment the market growth.

By Aashi Mishra, Sr. Content Writer, Research Nester

According to recent study published by Research Nester, the Edge Computing Market size is expected to cross USD 894 Billion by 2036 and is projected to expand at a CAGR of 39.65% from 2024 to 2036. The rising partnership and collaboration among the key players are to augment the market growth.

Surging Adoption of Edge Computing in the Healthcare Sector to Boost the Market Growth of Edge Computing

It is expected that edge computing would contribute to global connection in healthcare. Through mobile apps or portals, edge computing decentralizes analytics and locates storage, monitoring, and patient diagnosis. Through the use of a smartphone app or portal, modern technology can be utilized to track patients' health in real time. It increases operational effectiveness and boosts client happiness. It guarantees personalized record management and provides patients with essential healthcare advice. In this regard, cloud computing is being used by UAE to track patient data and healthcare records. The

MEA region is more likely to experience chronic illness. This region has the highest rate of diabetes prevalence, according to the International Diabetes Foundation. 39 million people have received a diagnosis, while 19 million people are believed to be undiagnosed.

The global edge computing market is anticipated to grow with a CAGR of 39.65% over the forecast period, i.e., 2024 – 2036. The market is estimated to garner a revenue of USD 893.93 billion by the end of 2036. Additionally, in the year 2021, the market registered a revenue of USD 11.78 billion. The market is segmented by technology into component, industry vertical, application, and organization size. The hardware segment from component segmentation, amongst all the other segments, is anticipated to garner the largest revenue of USD 430.83 billion by the end of 2036. Additionally, the segment registered a revenue of USD 5.7 billion in the year 2023.

QoE can supply quality to clients and QoS can capture quality given by edge nodes. Selecting edge computing that avoids overtaxing nodes with computationally demanding workloads is the difficult part. Even if the nodes have to handle extra demand from the data center or edge service, they still need to have high throughput and be dependable in order to deliver the desired workload.

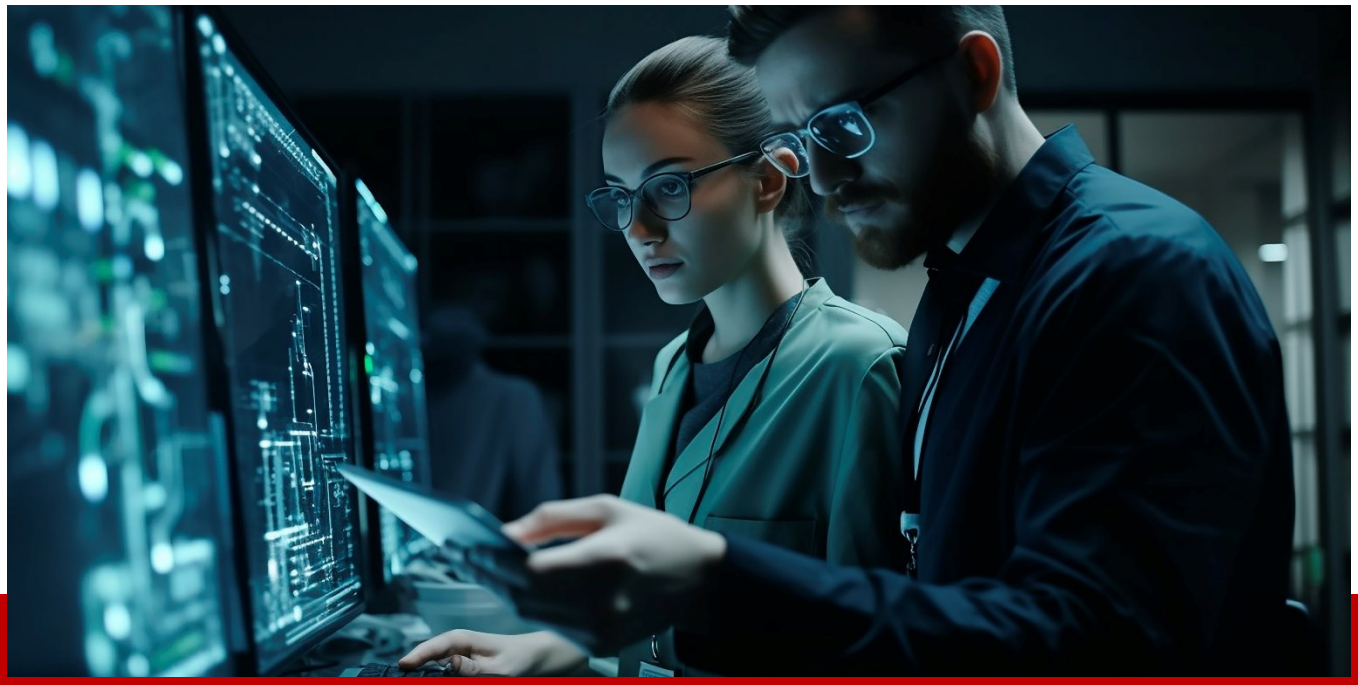
By region, the global edge computing market is segmented into five major regions including North America, Europe, Asia Pacific Excluding Japan, Japan, Latin America and Middle East & Africa region, out of which, the market in North America region is anticipated to garner the largest revenue of USD 389.40 Billion by the end of 2036. Additionally, the market in the region registered a revenue of USD 4.9 Billion in the year 2023. One of the most innovative technological developments in the area is the idea of a smart city. North America would use edge computing more frequently as the idea of smart cities took off there in order to solve latency and bandwidth issues. It would facilitate the residents' easy acclimatization to the smart city infrastructure.

Top players include in the global edge computing market are Cisco System Inc., Nokia Firm, Huawei Cloud Computing Technologies Co., Ltd., Dell Inc., Hewlett Packard Enterprise Development LP, SixSq SA, Capgemini, and others.

Source - https://www.researchnester.com/reports/global-edge-computing-market/1945 .

About the Author

Aashi Mishra is currently working as a content developer with the Research Nester. Electronics engineer by profession; she loves to simplify complex market aspects into comprehensive information. She has experience of 3 years in this domain where she has mastered in tech writing, editing, copywriting, etc.



How Cybersecurity Supports Business Operations

By Zac Amos, Features Editor, ReHack

Cybersecurity has gained much traction in recent years, so much so that it can be easy for companies to overlook how critical it is. To overcome this gap of complacency, organizations must recognize the strong business case for cybersecurity. They must realize that proper security is more than a recommendation — ut's essential to running a successful brand.

As firms rely more on digital tools and data, cybersecurity will become all the more central to ongoing operations. Here's a closer look at the role of cybersecurity as a business practice.

Preventing Financial Loss

The most obvious role of cybersecurity in business is to protect an organization's finances. Data breaches are among the most expensive preventable events a business can experience, costing $4.45 million on average. Those costs keep rising as data becomes an increasingly valuable resource, too.

Cybercrime impacts finances in many ways. Even the most minor of attacks can lead to waste from lost productivity as the company works to get its IT infrastructure back online. In other cases, criminals may hold mission-critical data for staggering ransoms, or flat-out steal money or valuable information from digital systems.

There's also the price of lost business to consider. Both B2C and B2B brands are likely to lose customers if they experience a publicized data breach.

Protecting Consumer Data

Cybersecurity is also a matter of consumer privacy. Businesses today hold vast amounts of potentially sensitive data on their clientele. Without proper protections, that practice could needlessly expose consumers to financial damage or privacy breaches.

Corporate data breaches affected over 360 million people in the first eight months of 2023 alone. These events can put consumers' bank information and identities at risk, making thorough cybersecurity a pressing social issue.

These threats apply to internal processes, too. If companies don't take cybersecurity seriously, they may expose their employees' personal information to attack. No enterprise can safely claim to stand up for its staff or customers with that level of risk.

Preserving Business Relationships

Similarly, cybersecurity is crucial to maintaining a firm's responsibilities to its partner organizations. In today's hyper-connected world, poor security is never an entirely internal issue. Vulnerabilities in one part of the supply chain affect all other connected parties, so firms must be secure to ensure fair business relationships.

The possibility of third-party risks can affect both existing and potential partnerships. Imagine a software provider experienced an internal breach that, in turn, exposed data from the businesses using their platform. After the event, their current customers may switch providers and other companies will be less willing to partner with them in fear of experiencing the same.

Over a third of fund managers say risk exposure is their biggest obstacle to closing deals. While cybersecurity certainly isn't the only risk factor, it's increasingly prevalent as data becomes more mission-critical.

Ensuring Continued Operations

Another reason why cybersecurity is crucial to business is many functions today rely on IT systems. If a cyberattack took down a firm's internal network, it wouldn't be able to fulfill its core operations until restoring it.

Most organizations have experienced at least one IT outage in the past three years. Cyberattacks account for 11% of these events, making it the fourth most common cause. As time goes on, their share of IT outages is increasing, as are the size of their disruption.

In some brands, not being able to perform core functions has a more severe impact than just losing money. It could impact human lives in hospitals, for example.

Defending Critical Infrastructure

Growing Internet of Things (IoT) adoption heightens the business case for robust cybersecurity. As the IoT brings more previously air-gapped infrastructure online, it exposes it to attack. These infrastructure attacks can cause widespread physical damage.

Many energy grids now rely on IoT devices to improve responsiveness, but this means a cyberattack can shut down power to an area. IoT-connected water purification systems could stop working and lead to unsafe public water supplies if hacked. In other cases, cyberattacks could interfere with emergency response networks.

There were over 112 million IoT attacks in 2022 — 80 million more than in 2018. If this trend persists, connected infrastructure will only become a more critical target, making cybersecurity all the more crucial.

Complying With Growing Regulations

Finally, cybersecurity deserves its place in business as an important governance measure. Government security and data privacy regulations are growing, so failure to secure some systems could result in massive compliance violations.

The European Union's General Data Protection Regulation is the most famous example, but it's far from the only one. At least 40 states have introduced cybersecurity legislation and at least 24 have enacted these laws.

As these laws become more common and their penalties more severe, investors and partners will consider cybersecurity a more significant deciding factor. Consequently, failure to ensure thorough security will limit ongoing success, not just immediate financial losses.

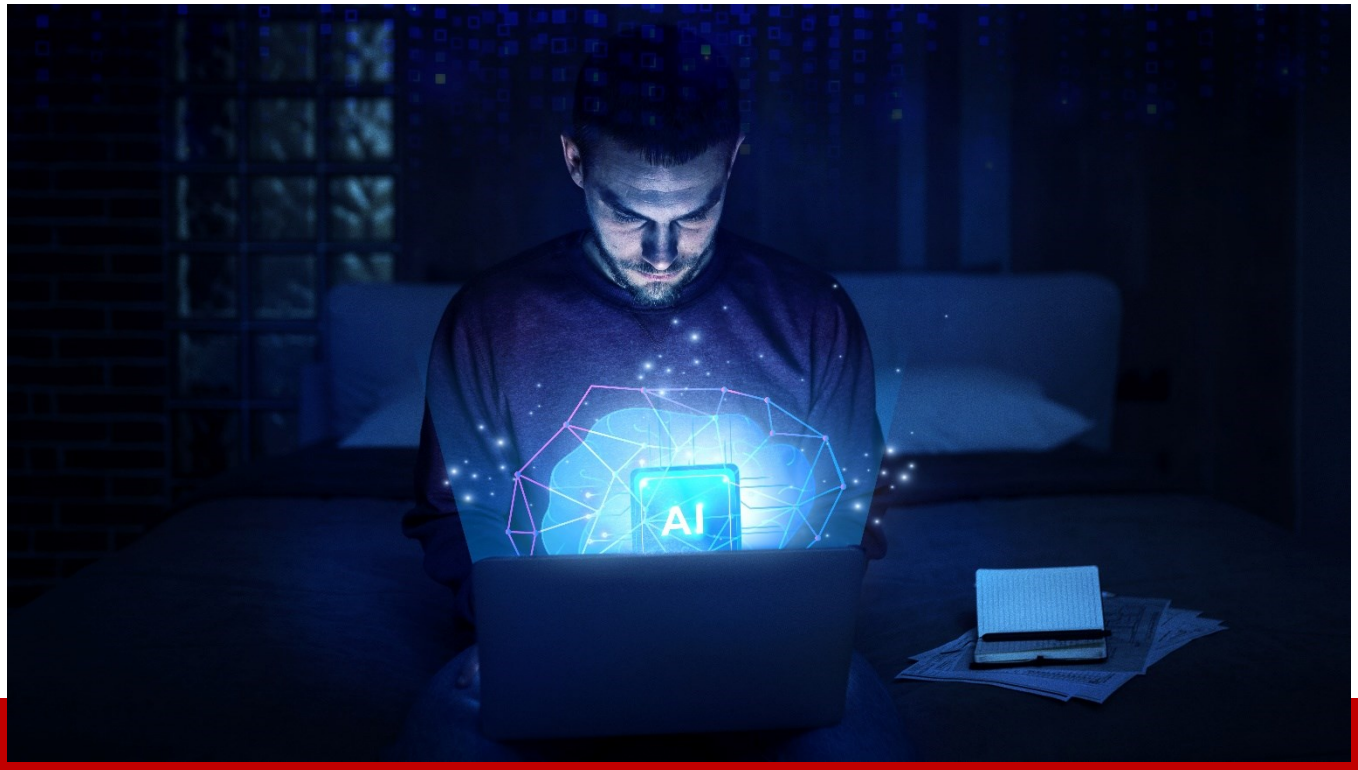
Cybersecurity Is Essential for Businesses Today

Cybersecurity may seem like an additional best practice for organizations, but it's critical. Companies today can't comfortably do business in any industry without it.

As cybercrime rises and digitization takes over more industries, security's importance as a business function will only grow. Organizations must embrace cybersecurity as a core practice now to prevent losses in the future.

About the Author

Zac Amos is the Features Editor at ReHack, where he covers cybersecurity and the tech industry. For more of his content, follow him on Twitter or LinkedIn.



How Large Language Models Can Be Used to Weaponize AI

By Bobby Cornwell, Vice President Strategic Partner Enablement & Integration, SonicWall

In December, I predicted threat actors would tap into chat-based and generative artificial intelligence (gen-AI) tools to augment and enhance attack methods and discover new attack vectors in the coming year. Sadly, it appears this prediction has come true sooner than expected. This month we witnessed what some say was the largest data leak in history (26 billion exposed records), and we saw that North Korean hackers are starting to use gen-AI to conduct cyberattacks and search for targets to hack.

At the heart of this burgeoning cyberthreat are new, large language modules (LLMs) that enable more efficient ways to compromise vast numbers of computing devices and launch increasingly more successful cyberattacks, which, in turn, net attackers even more valuable data that can be fed back into their expanding data lakes.

LLMs are able to bring together massive amounts of breach data that have been cobbled together from numerous historical breaches to train new AI-based systems. This novel approach gives aspiring hackers access to volumes of personal data that includes PII (personal identifiable information) and login credentials to any number of websites that have historically been compromised.

It should be noted that transforming breach data into a format compatible with LLMs demands considerable expertise and resources. This isn't a casual pursuit; it's a multibillion-dollar industry often backed by various governments. Although currently not widespread, elite threat actors, armed with ample resources, could potentially utilize LLMs to analyze data in unprecedented ways. As malicious AI applications become more advanced, even those who aren't well versed in network security mechanics will be able to enter the game. This includes state sponsored threat actors who don't care about government regulations on what AI can and cannot do and hactivists who will utilize AI to generate new exploits to make their point.

Imagine if threat actors could input data from multiple breaches into a LLM, making it readable. They could instruct an AI platform to discern patterns and details about individuals in the database, surpassing what has been done before. This could involve extracting extensive personal information about a person, their family, and associates, leading to various malicious activities.

For instance, threat actors could cross-reference this information with social media profiles, conference attendance records, or employment details from platforms like LinkedIn. This knowledge could be exploited for activities ranging from utility service disruptions to identity-based extortion.

While this may seem like a scenario from a Hollywood movie, the capability exists today, although not without challenges. Mainstream AI platforms like those from OpenAI and Google have built-in ethical protections. However, if hackers gain access to an open software platform with advanced capabilities, they could potentially modify it.

Contrasting this with traditional methods, early data breaches primarily involved credit card and social security number theft. Credit card details were sold on the dark web, enabling subsequent illicit transactions. In the current landscape, breaches involve diverse data, such as medical records. Attackers now need to formulate specific queries or understand how to build queries for the stolen data, a process made more efficient with AI. Specifically, AI enhances the ability to cross-reference data, identify patterns, and track individuals and their associations, marking a significant departure from conventional cyberattack methods.

Recently, we have seen several companies pop up overnight utilizing this new type of aggregated breach database to search for people and what exposed data may be out there for specific individuals. Out of curiosity, I went to Malwarebytes the other day and entered my work email to see what may be lurking on the dark web about me. In less than a few minutes, the site correctly revealed my work address, where I live, and 14 breaches where a password of mine had been exposed.

It can't be emphasized enough, the rising threat of AI-enhanced cyberattacks is a cause for concern. Currently, the technology to detect such advancements is being developed in tandem with the evolving threat actor tactics. While companies have primarily focused on utilizing AI for threat hunting through tools like security information and event management (SIEM), threat actors across various levels are now employing AI to craft sophisticated phishing attacks. For example, in the context of AI-enhanced phishing emails, conventional methods of identifying language and grammar errors are becoming less effective. AI can now generate phishing emails that appear professionally written.

To enhance protection, individuals should scrutinize the email address of the sender, hover over hyperlinks without clicking to verify their legitimacy, and exercise caution with attachments even from trusted senders. Advanced endpoint security and email security measures that scan attachments are essential. For added security, if unsure about a URL, copy the portion after the "@" symbol in an email address and check it on services like VirusTotal or consult your IT department.

Engaging with dark web searching services is another proactive step, and some companies, like Malwarebytes.com, offer free email scanners that cross-check email addresses against known breaches. If you find your data has been compromised, change your passwords immediately. And make sure you avoid using the same passwords across multiple logins.

For iPhone users, leverage the built-in features that will notify you about compromised passwords. Businesses should invest in dedicated firewalls (not just routers with security features) and ensure their hardware's firmware is up to date and configured correctly. While more tips could be provided, these are key recommendations to fortify against AI-enhanced cyber threats.

While the media is calling the 26 billion records leak the mother of all breaches, it's really not. It's the beginning of how the AI revolution can and will be used by threat actors in the days ahead.

About the Author

Bobby Cornwell is a seasoned professional in the cybersecurity industry, currently serving as the Vice President of Strategic Partner Enablement & Integration at SonicWall since February 2023. Prior to this role, he significantly contributed as the Executive Director of Sales Engineering for over five years, liaising directly with the Chief Revenue Officer. His tenure at SonicWall extends over 16 years, showcasing a robust background, notably including a nearly ten-year stint as a Senior Security Systems Engineer. His expertise, particularly in sales engineering and security systems within the Greater Atlanta area, marks a distinguished career with a focus on strategic partner development and technical leadership. Bobby Cornwell also held a significant role at Ricoh Company for over a decade, where he was a National Network Services Engineer/Manager. This position contributed to his extensive experience in the field of network services and management. You can contact Bobby via LinkedIn https://www.linkedin.com/in/bobbycornwell/

Network Engineering Market

By Sudip Saha, COO, Future Market Insights Co-Author- Amrita Adak, Future Market Insights

Network engineering stands as the foundation of contemporary connectedness in the constantly evolving world of technology. It profoundly influences how people communicate, work, and live. It acts as the unseen force behind the smooth global transmission of information. Network engineering is still relevant today because it is essential in creating the digital infrastructure that underpins the globalized world. Network engineering has become much more important in the context of cybersecurity. It is necessary to build and strengthen networks against possible breaches as cyberattacks become more complex.

What's Sparking the Rising Demand for Network Engineering?

Network Engineering Transforms Industries with Innovation! A rising variety of developing technologies is boosting the demand for network engineering services, especially those related to the Internet of Things (IoT), the cloud, and edge computing. Organizations have more options for designing, developing, optimizing, and managing their networks owing to a burgeoning sector of network

engineering services. All sectors can communicate and transmit data more easily with the use of dependable and secure networks.

Network engineering services are one of the primary variables influencing the necessity for infrastructure in the engineering services sector. Network engineering is innovated by infrastructure initiatives such as data centers, smart cities, and telecommunications networks. The demand for safe and dependable networks is driving growth in the market for network engineering services.

Network Engineering Shapes the Future of Internet Marketing! Internet marketing is one of the most important strategies for attracting new customers and raising brand awareness among consumers as a whole. Internet marketing organizations rely on the network availability to interact with customers as well as create and oversee advertising campaigns, social media, and viral content.

Frequent internet outages can turn out to be extremely detrimental to a business since they make it practically impossible for employees to do their jobs well, which highlights the necessity for scalable and trustworthy networking solutions. The network engineering market is expanding rapidly due to these business and industry niches.

Network Engineering Boom in the Face of Web Hosting Challenges! Web hosting companies find it difficult to remain in business if they can't depend on a stable internet connection to maintain their servers online and connected. Reliability of the internet is crucial to ensuring that their client's websites are operational with minimal downtime. Their websites can lose money if they have frequent outages, which can give rise to furious consumers, bad reviews, and a gradual decrease in clientele.

Using multiple servers and connections, updating networking capabilities to a faster and more secure architecture, and investing in the latest, more secure networking solutions and technologies are all potential options. The network engineering market is expanding due to each of these considerations. The integration of network engineering services with on-premises and cloud infrastructures is becoming more prevalent.

Network Engineering's Battle against Data Breach Chaos! There has been an expanding demand for network engineering since 5G technology was introduced and deployed. With the rise of digitalization come increased concerns of data theft and misuse. Businesses have sensitive information that must be safeguarded to prevent theft and data breaches, which might damage the company's reputation as a whole. In addition to other confidential business-related data, companies may lose their technological advantages, designs, and sourcing details as a result of the data breach.

Network engineering strikes a balance between security and the growing demand for rapid, effective, and versatile computing. For example, to provide end-to-end 5G automation services, Mavenir and L&T Technology Services Limited, an engineering services business located in India, partnered in June 2021

.

The United States Emerges as the Epicenter of Network Engineering Trends

The technology and communications industry is undergoing significant change, and as a result, there is likely to be a rise in the demand for network engineers in the United States. The network engineering

service market is forecasted to rise at a compound annual growth rate (CAGR) of 5.6% through 2034, according to FMI. Given their favorable financial situation, United States-based companies have made large investments in advanced products and technology. As a result, companies operating here face greater competition than those working elsewhere.

The country's extremely advanced information technology infrastructure made the early adoption of various network solutions possible. As per FMI's technology specialist Sudip Saha, "Customers are engaging with businesses across sectors progressively as a consequence of technical and automation improvements. Information and communications technology investments in the United States are projected to generate significant revenue."

The National Science Foundation in the United States claims that a sizable portion of United States-based companies are digitized. Furthermore, the market expansion is driven by local government efforts that encourage businesses to use digital technology. To promote digital access and entrepreneurship, for example, the State Department and USAID announced plans to expand digital literacy programs, invest in the development of digital infrastructure, install the United States digital identity systems in neighboring countries, and expand access to cloud and corporate information systems to support business activity.

Can Connectivity and Security Coexist? Answer: Network Engineering!

The escalating rate of cyberattacks demands a proactive and fortified defense mechanism. The statistic that a hacker strikes every 39 seconds on average in America underscores the urgency and significance of prioritizing network security. Attackers employ modern technology to expand their reach of deception, and society uses them to limit what they can get away with. Businesses and service providers are concerned because these procedures and coordination efforts take time, and security flaws can be exploited in the interim.

Cybersecurity is revolutionizing network engineering and playing a crucial role in opening up new horizons for the network engineering market. Network engineering expertise is needed to protect against cyberattacks, develop strong security measures, and safeguard personal data since it focuses on strong security standards. For companies looking to prosper in a more digital and connected world, it goes beyond just a technology requirement and becomes a strategic requirement.

In the face of a constant and changing cyber threat scenario, companies can shore up their defenses, safeguard vital assets, and guarantee the confidence and privacy of their customers by investing in strong network engineering standards. Through the implementation of sophisticated security protocols, businesses can considerably mitigate the likelihood of becoming targets of malevolent cyber operations.

The Vibrant Shifts in the Network Engineering Market amidst the AI Era

Artificial Intelligence (AI) is revolutionizing numerous industries, and network engineering is no exception. Artificial intelligence (AI) surge in 2017 has significantly opened doors for the network engineering market.

AI's attraction is only going to get stronger, offering network engineers exceptional chances to advance their skills. What distinguishes AI is its extraordinary ability to instantly recognize connections between events—a task that could be difficult even for experienced network experts. This is especially true for the domain of time series anomalies, where AI is highly skilled at identifying correlations and patterns that can be missed by human observation.

AI has been included in network engineering to lower downtime, boost efficiency, and increase overall network performance. Network engineers can stay ahead of the game by utilizing artificial intelligence to discover and fix complex network complications and streamline their procedures. According to Amrita Adak, a technology enthusiast at FMI, "A revolutionary age has been predicted by the merging of AI and network engineering, which is set to provide a smooth combination of machine accuracy and human competence to advance the market. In the future, human and artificial intelligence are likely to collaborate together in a symbiotic manner to optimize and protect networks in the future of network engineering."

What are Network Engineering Providers Up To?

Market players in the field of network engineering services are creating cooperation agreements, collaborating, and forming partnerships in order to increase their global reach. Meanwhile, they're spending a lot of money on research and development to improve the products they offer and strengthen their position in the market. For instance:

Cyient declared in June 2022 that it had acquired Celfinet, a wireless engineering services provider with network engineering services located in Portugal. It cost US$ 43.9 million to purchase. Cyient sought to support businesses and Communication Service Providers (CSPs) in implementing networks on a large scale with this purchase.

Through its Mission Technologies business, HII's subsidiary Alion Science and Technology was awarded a US$1.4 billion deal in August 2023 for Joint Network Engineering and Emerging Operations. A one-year base period and four one-year options are offered under the General Service Administration's ASTRO contractual mechanism.

Conclusion: In the coming years, the network engineering market is expected to grow more than ever. Network operations are expected to get more efficient and secure as artificial intelligence continues to be integrated into the process. Network engineers are going to be fundamental in meeting the ever-present demand for fast connection as 5G spreads. Professionals in the industry are expected to encounter problems as well as possibilities due to the emergence of edge computing and the ongoing evolution of cybersecurity. Accepting these developments, network engineers could look forward to a day when their expertise is going to be in high demand and contribute to a seamlessly interconnected society.

About the Author

Sudip Saha, a moniker given to him by his peers, is the COO of Future Market Insights an ESOMAR-certified market research and consulting company, and a member of the Greater New York Chamber of Commerce. In his current role, he is responsible for the strategic and tactical leadership of the COO functions, supporting and monitoring the strategy, planning, execution, geographic growth, and market performance of FMI. A growth-oriented business professional with vast experience in market research and project management across verticals in APAC, EMEA, and Americas, Sudip is a strong believer and proponent of innovation-based solutions, with an emphasis on creating customized solutions to meet varied client needs. Connect with Sudip on **LinkedIn and Twitter.**

About Future Market Insights Inc.

https://www.futuremarketinsights.com/

Future Market Insights Inc. is an ESOMAR-certified business consulting & market research firm, a member of the Greater New York Chamber of Commerce, and is headquartered in Delaware, US. We have been collaborating with global enterprises in their business transformation journey and helping them deliver on their business ambitions. 80% of the largest Forbes 1000 enterprises are our clients. We serve global clients across all leading & niche market segments across all major industries.

Avail of flexible Research Subscriptions, and access Research multi-format through downloadable databooks, infographics, charts, the interactive playbook for data visualization, and full reports through MarketNgage, the market intelligence engine powered by Future Market Insights. Sign Up for a 7-day free trial!

About Co-Author

Amrita Adak. A passionate content writer and avid technology enthusiast. She skillfully combines her passion for writing with her interest in the latest technological advancements. She enjoys visiting tech conferences, experimenting with new devices, and discussing the future of innovation. She continues to entertain and educate through her words, bringing a true enthusiasm for technology and content production to the digital world and making it a more welcoming place for everyone.

Is Improving Cybersecurity One of Your New Year's Resolutions?

By Krishna Vishnubhotla, Vice President Product Strategy - Zimperium

As we embark upon a new year, most organizations are contemplating their New Year's resolutions, shifting their focus away from holiday festivities and towards looking for ways to build momentum and growth, which often includes welcoming new employees. Although bringing on new hires can be an exciting and fruitful time for businesses, as employees begin onboarding and gaining access to the various networks and devices of the organization, organizations are faced with an array of new and challenging cyber risks.

How Mobile Security has become Crucial for Organizations

In recent years, mobile devices have taken center stage and become increasingly woven into the fabric of our daily lives. And for many organizations, mobile devices have become an integral part of everyday

business processes. By allowing employees to use their personal phones, tablets, and laptops for work, organizations offer their employees greater flexibility, enhanced workflows, improved communications, and more efficient and productive ways of working overall. Keeping corporate information secure on employees' mobile devices isn't easy, however, and an employees ability to use personal devices for work poses unique challenges and cybersecurity threats. If an employee's device were to become compromised due to a lack of proper security measures, for example, confidential company information could easily fall into the hands of bad actors looking to exploit the organization.

As we move further into 2024, cybercriminals will only continue to be on the lookout for new ways to exploit vulnerabilities in mobile devices. In fact, according to Zimperium's Global Mobile Threat Report 2023, 43% of all compromised devices were fully exploited (not jailbroken or rooted), an increase of 187% year-over-year - an astonishing number. This is why it should be every IT decision-makers goal to ensure that their devices are secured against any and all emerging threats.

Top Threats to Mobile Devices

Mobile security threats are commonly thought of as a single, all-encompassing threat. But the truth is, there are many tactics that threat actors use to infiltrate our mobile devices. And unfortunately, these threats tend to not only compromise personal information of employees but also disrupt an entire company's system and network. Here are some of the top threats that our beloved mobile devices are susceptible to.

Data Breaches: A data breach is any security incident in which unauthorized parties gain access to sensitive or confidential information, including personal data. Cybercriminals are hyper aware of the significant amount of sensitive data stored on our smartphones - from credit card numbers to login credentials for various accounts. Because of this, mobile devices have become a main target for attackers seeking to steal this valuable data or sell it on the dark web. Data breaches on popular apps like Twitter and WhatsApp have put millions of users at risk in recent years.

Phishing Scams: Phishing attacks remain a top cybersecurity risk for organizations, and using personal devices for work can exacerbate this threat. Phishing is a social engineering attack where scammers try to trick people into giving away their personal information by posing as legitimate entities such as banks or government agencies through emails or messages. Employees may be more susceptible to phishing attacks on their personal devices, as they may not be as vigilant about scrutinizing emails or messages from unknown sources.

Malware Attacks: With the rise in popularity of mobile apps, malicious actors have found a new way to target unsuspecting users. Malware such as viruses, trojans, adware, and spyware can infect your device through seemingly harmless apps or links. Once a personal device is infected, the malware can easily spread to the corporate network when the user connects their device to it. Malware can also spread through the organization's cloud services, email, or file-sharing platforms.

Outdated Software: Personal devices typically have inconsistent software updates and patches, leaving them vulnerable to cybersecurity threats. Users may neglect to update their devices or applications regularly, as they are not managed by an IT department that enforces timely updates. Outdated software

and apps may contain exploitable security vulnerabilities, which can expose an organization's network and data to potential attacks, as a compromised personal device can serve as an entry point for attackers to infiltrate the company's systems.

Comprehensive Mobile Security

Organizations should be making it a key resolution of theirs this year to secure their company's network - not only for the sake of the company, but more importantly for the safety of its employees. This should include comprehensive measures that cover all points of entry - including employee-owned mobile devices, especially. To do this, there are a few key areas organizations should keep their eye on:

1. Prioritize risk assessment - Assessing risk as close to the user or point of entry as possible is crucial to defending against attackers. A good first step organizations can take is applying mobile-powered business initiatives across all of their mobile devices and apps.
2. Visibility is your best friend - It's important to have complete visibility of all mobile assets and their risk levels in order to assess vulnerabilities and address them immediately. Implementing defenses that are quantifiable, auditable, and insurable are key.
3. Address the most critical gaps first - By embedding security across all devices and applications, applying risk-based response and zero trust assessments of mobile endpoints, organizations can enhance their mobile detection and response strategy overall.
4. Establish autonomy - Applying systems that can automatically isolate any compromised devices and untrusted environments will lay the foundation for a strong security posture.
5. Staying ahead - Organizations should keep on top of any regulations, data sovereignty and privacy standards that can put them at risk of compliance failures.

A strong mobile-first approach to security can help organizations to be proactive and immediately spot suspicious activity, prevent account takeovers, and even stop fraud before it can occur. This approach is crucial to ensure that a businesses confidential data, and more importantly their employees, remain safe.

About the Author

Krishna Vishnubhotla, VP of Product Strategy at Zimperium. Krishna Vishnubhotla is a seasoned professional in the SaaS industry, specializing in catalyzing startup growth through adept product and marketing strategies. With a keen focus on mobile application security products, he has a proven track record in defining and executing product visions that drive significant revenue growth. In addition to managing a global customer success portfolio, he established high-value strategic partnerships. His leadership skills extend to spearheading revenue generation efforts, serving a diverse clientele across multiple industries. Mobile Security Solutions | Complete Mobile Security for Apps and Devices (zimperium.com)

Reality War

Due to the powerful weaponry of misinformation equates to a very dangerous threat on the battlefield, which is reality itself.

By Oliver Libby, Managing Partner, H/L Ventures

Growing up around scientists and doctors as I did, you develop respect for truth and credibility. A generally shared set of facts makes conversations, solutions, and functional systems possible. That is why I'm so worried about the newest form of global warfare that has arisen faster than any in human history – the Reality War.

We can stop wondering when World War III will happen, because it is already here, and we are in the trenches today.

From the dawn of history, wars have been conventional. Wars might be between major powers, they might be asymmetric, but people fought with weapons and killed one another for whatever reason. My arrow pierces your shield; my tank shoots your tank.

More recently, the asymmetric battlefield moved into cyber space. My hackers paralyze your bank account, your utility company, or even perhaps your country. As present as this danger continues to be, cyberspace is in many ways yesterday's battlefield.

Today's true battlefield is Reality itself.

The attack on Reality hasn't come out of nowhere. We are living in a fragmented ecosystem. Information washes over to us from screens, speakers, and networks more prolific than anything history has ever known. Our human brains still process content roughly as quickly as our ancestors, but the cacophony is real, overwhelming, and fast. We have become polarized, pushed further and further into echo chambers by algorithms and balkanized by pressure from our peer groups. Trust and credibility are at all-time lows (check out the Edelman Trust Barometer), no matter whether we are looking at government, business, religion, non-profits, credentials, or anything else that used to command a level of respect. Some of this is an unintended consequence of seemingly harmless tech, and some of it is absolutely intentional.

The merchants of doubt have set the stage. But the weapons just got so much scarier. Social media, algorithms, and hacking are still wreaking havoc, but we are about to enter a hall of mirrors brought to you by AI, bots, and deepfakes that render totally believable facsimiles of faces, voices, and whole people. This is next level information distortion.

I'd like to point out that I am no luddite. I'm a tech investor and a believer in innovation. But – and maybe because of this – I respect technology and its potential. I recognize that technology itself doesn't (yet) have agency or morality of its own. But we rely on those who wield it to act with good intentions, knowing that the world is full of bad actors.

Some of this is harmless and, at least at first, a little absurd: Bored Ape and other NFTs raised more cash than climate technologies in 2021. People used real money to buy real estate in the (infinite) Metaverse. But the ridiculous can so easily become weaponized. Now, cheaply accessible technologies like OpenAI's ChatGPT4 are being essentially tested on a global scale, placing the information equivalent of nuclear weapons in the hands of individuals. Individuals, criminal enterprises, and even nations can and do control bot farms and hacker groups, build the hard infrastructure of the digital world, and even direct the algorithms and policies of entire social media platforms.

The very decentralization of the threat is also scary. The Reality War is a funhouse where there is no truth (everyone has their own "facts"), where everyone is overwhelmed and there is no common ground, and where no one knows any better (certainly not an expert!). Even the blue checkmark that was tenuous indication at best before is no more.

Thirty years ago, when Francis Fukuyama wrote about the End of History and the Last Man, he argued that Western style liberal democracies (and the associated financial systems) were the winners of the great human search for models of governance and economics. Of course, this analysis requires societies to make generally good decisions most of the time, which in turn requires reasonably good data. After all, for a citizen and a consumer, good information is a key to making good decisions: otherwise, garbage in, garbage out. How are liberal democracies to survive in a world at war with Reality?

We've been wondering whose Century would follow the American Century. Maybe it's Nobody's Century. Isn't that scary? A Reality War with no hegemon to enforce social norms. Doesn't it feel like a global

Lord of the Flies scenario when politicians are being deepfaked, gamers are sending very real SWAT teams to raid each other, and people are purchasing tokens backed by absolutely nothing with their actual money?

This isn't some theory, it isn't remote, and it isn't in the future. It's happening today, and it's affecting every one of us, our businesses, our environment, causes we believe in, our government, and even our friends and family. The Reality War is bending everything into a distortion field where the mechanisms for society fail.

Take, for example, the recent October 7th attacks in Israel, and the military response in Gaza. There is a huge (dis)information component to this battle, and one of the biggest causes of some truly catastrophic fractures in our society is that people can't even seem to agree on basic facts. When Pearl Harbor was attacked, there was no debate as to who struck America. Today, there are already a dozen versions of what happened at the music festival on October 7th circulating at scale in the information sphere.

This is about to be very real for people: you might once have worried about a hacker getting your debit card number or freezing you out of your Facebook page, but now a nefarious actor might steel your very face, voice, and speech patterns. The risk is so much higher and the threat so much deeper today than in any moment in the digital revolution.

By the way, don't think for a moment that this only applies to Boomers on Facebook and Gen Z on TikTok. These memes are incredibly contagious. They leap from doomscrolling to network media to the dinner table in minutes. No segment of society is left out of the Reality War.

Of course, I am neither the first nor the deepest-thinking person to call attention to this issue. A few excellent examples include Jon Askonas' series in The New Atlantis, "Reality: A Post-Mortem" and Renee DiResta's excellent piece "Mediating Consent", along with the book LikeWar: The Weaponization of Social Media, by P.W. Singer and Emerson T. Brooking. But I do think the framing as a full-on war against Reality is important.

So what are we to do? We need to raise awareness that the Reality War is happening. We need citizens to make an extra effort to be informed from credible sources, to develop the ability to trust expertise and parse information effectively.

This isn't easy, because Reality War attacks the immune system of the body politic: information, media, and credentials.

So, we must go further. Technologies like deepfakes, bots, and AIs must be regulated like the weapons of mass reality distortion that they really are. Deepfaking someone should be a federal offense with a hefty sentence. There have been efforts on Capitol Hill, in the White House, and other nations as well to start to do this, but it has to be taken seriously. A realization that our political class is not immune from the Realty War is needed. It will require political leadership that is willing to cast aside the short term political advantages available by using the Reality War to implement necessary regulation. The cost of nefarious Reality Warfare must be steep, and punishment relentless and swift. I do not take a call for regulation lightly, but these technologies are just as dangerous as other things we readily regulate, and they will move much more quickly.

We have entered a period of human history where a picture, a voice, a face, a fact…all might have been manufactured. Trust, assuming good intentions, and being able to turn to shared sources of truth and credibility must not give way to glib skepticism, mistrust, blind hatred, and simple noise.

The trick in the Reality War is coming to a shared understanding of what is happening and what to do about it. If we let Reality War happen without defending ourselves, we won't need to worry about AI destroying us. We'll have done it to ourselves.

About the Author

Oliver B. Libby is Co-Founding Managing Partner of Hatzimemos / Libby Holdings (H/L Ventures) and of CityRock Venture Partners. Based in New York City and founded in 2009, the H/L Ventures family of companies represents a new kind of venture firm. H/L Ventures is dedicated to building high-growth businesses that add value to society by protecting and promoting people and the planet, with a strong preference for diverse founding teams. H/L Ventures' proprietary Daily Active Engagement model blends the best of venture studio and investment firm on one platform to help grow companies from early stage to exit in a holistic approach to company building.

Mr. Libby also chairs the Board of The Resolution Project, Inc., a non-profit organization based in New York City which he co-founded in 2007. Through its Social Venture Challenges, held at leading youth conferences around the world, Resolution identifies undergraduate students who wish to launch new social ventures. The resulting Resolution Fellowships provide dynamic, hands-on mentorship and grants to implement their social ventures— a full ecosystem of support that empowers the recipients to become socially-responsible leaders. To date, hundreds of Resolution Fellows are working on diverse ventures in high-impact fields and have benefitted about 3 million people to-date in more than 80 countries on all six inhabited continents, including all across the United States.

Mr. Libby began his career in the U.S. Government and later at a global managing consulting firm. Mr. Libby is a Presidential Leadership Scholar, a Steering Committee Member of the Milken Young Leaders Council, a Leadership Council Member of Tech:NYC, a Fast Company Impact Council Member, a Concordia Summit Advisor, a member of the UN Sustainable Development Solutions Network Youth Advisory Council, a founding GLG Social Impact Fellow, and a NationSwell Councilmember. Mr. Libby was previously also a Foundation Trustee and Chair of the Admissions Committee of the Harvard Club of New York City, as well as a member of the Advisory Council of the Clinton Global Initiative.

Mr. Libby has been invited to speak at Harvard, the United Nations, and numerous business conferences. He has published work focusing on the nexus between the future of work, job creation, innovation, social entrepreneurship, and leadership. His work has been covered in publications including the New York Times, Wall Street Journal, Financial Times, Venture Capital Journal, Crains NY Businesss, Bloomberg BusinessWeek, Fast Company, Reuters, and television appearances including CNBC. Mr. Libby graduated magna cum laude from Harvard College. Oliver can be reached online at X and LinkedIn and at our company website https://h-l.vc/.

Surviving The Cyberstorm: A Practical Guide To 2024 Mobile Security

By Nicole Allen, Marketing Manager at Salt Communications

In an era where mobile devices are an integral part of our daily operations in business, the evolving landscape of cyber threats poses significant risks to our digital well-being in corporate environments. As we step into 2024, the sophistication and frequency of cyber attacks targeting organisations have reached unprecedented levels. This blog explores the most prominent cyber threats within organisations in 2024 and offers insights on how users can safeguard their smartphones from these ever-evolving dangers.

With each passing year, cyber threats have become more sophisticated and widespread. From ransomware attacks to phishing scams, malicious actors are finding innovative ways to exploit vulnerabilities in our digital lives. As individuals, businesses, and governments become more interconnected, the potential for cyber threats to cause significant damage has escalated.

Cyber threats to look out for in 2024

1. Mobile malware onslaught

Malicious software targeting mobile devices, commonly known as mobile malware, continues to be a major concern in 2024. Cybercriminals employ a variety of tactics to trick users into downloading infected

apps or clicking on malicious links, leading to the compromise of sensitive information, unauthorised access, and even financial loss.

Prevention Tips:
- Only download apps from official app stores.
- Protect your device as if it were a computer.
- Don't use consumer messaging apps for business communications.
- Regularly update your device's operating system and apps.
- Install a reputable secure communications app for real-time protection.

2. Phishing attacks on mobile platforms

According to the IBM Security X-Force report, phishing was identified as the primary infection vector in 41% of cybersecurity incidents over the course of 2023. Phishing attacks have become more sophisticated, and mobile platforms are not exempt from these threats. Cybercriminals use deceptive emails, messages, or fake websites to trick users into divulging personal information, such as login credentials or financial details.

Prevention Tips:
- Be cautious of unsolicited messages and emails.
- Verify the authenticity of links before clicking.
- Use security features like two-factor authentication whenever possible.

3. Ransomware targeting mobile devices

While ransomware has been a menace for desktops, over recent years it has extended its reach to mobile devices which we will only see an increase of as we move further into the year and further. Mobile ransomware encrypts files or locks users out of their devices, demanding payment for the restoration of access or data.

Prevention Tips:
- Backup your data regularly to a secure cloud or external storage.
- Avoid clicking on suspicious links or downloading unknown attachments.
- Install reputable security software to detect and prevent ransomware attacks.

4. Insecure Wi-Fi networks and man-in-the-middle attacks

Estimates show that 35% of exploitation activity involves man-in-the middle attacks. Public Wi-Fi networks remain vulnerable points for cyber attacks, particularly with the rise of man-in-the-middle (MITM) attacks. In 2024, it will come as no surprise that attackers will continue to intercept and manipulate

data transmitted over unsecured Wi-Fi via mobile devices, compromising sensitive information if not protected.
Prevention Tips:
- Avoid connecting to unsecured public Wi-Fi networks.
- Use a Virtual Private Network (VPN) to secure and encrypt data transmission.
- Disable automatic Wi-Fi connectivity to prevent connecting to unknown networks.

5. Device and app vulnerabilities exploitation

As mobile devices become more sophisticated, so do the potential vulnerabilities. Cybercriminals exploit weaknesses in both device operating systems and third-party applications to gain unauthorised access, steal data, or compromise the device's functionality.

Prevention Tips:
- Keep your device and apps updated with the latest security patches.
- Enable automatic updates to ensure prompt installation of security fixes.
- Regularly review app permissions and limit access to sensitive information.
- Only use a corporate or organisational secure communications system to communicate sensitive information.

Secure Communications as a defence mechanism

One of the most effective ways to shield ourselves from cyber threats is by adopting secure communication practices. With a closed secure communications system like Salt Communications, no data is stored on our network and all communications are encrypted. Organisations should always be in total control of their communications and have full visibility. By having this control it means organisations have complete management on who gets invited to the system, who those users can talk to while on the system, setting up rules for data storage and retention, and arranging for any other integrations that might be necessary. Whether it's messages, calls or group chats, implementing secure communication protocols is essential to maintaining privacy and security.

As we navigate our way into 2024, staying informed and adopting proactive security measures is crucial. The threat landscape is dynamic, but with vigilance and the right precautions through the use of a closed and controlled secure communication platform, along with other preventive measures, organisations can mitigate the risks associated with cyber threats targeting mobile devices.

By incorporating these prevention tips into your digital routine, you can fortify your mobile devices against the ever-evolving challenges posed by cybercriminals. Stay informed, stay secure, and embrace a safer digital future for your organisations mobile devices in 2024 and beyond.
To sign up for a free trial or demo of Salt Communications contact us on mailto:info@saltcommunications.com or visit our website at https://saltcommunications.com/.
Discover why your organisation should consider Salt as a secure communications method.

About Salt Communications

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 https://saltcommunications.com/

References:

https://www.embroker.com/blog/cyber-attack-statistics/
https://www.globalsecuritymag.com/2024-Cybersecurity-Predictions-Insights-From-Industry-Experts.html#:~:text=Another%20threat%20to%20beware%20of,user%20or%20unlock%20the%20device.
https://www.simplilearn.com/top-cybersecurity-trends-article
https://www.govtech.com/blogs/lohrmann-on-cybersecurity/the-top-24-security-predictions-for-2024-part-2
https://www.darkreading.com/cyber-risk/cyber-threats-to-watch-out-for-in-2024

About the Author

Nicole Allen, Marketing Manager at Salt Communications. Nicole has been working within the Salt Communications Marketing team for several years and has played a crucial role in building Salt Communications reputation. Nicole implements many of Salt Communications digital efforts as well as managing Salt Communications presence at events, both virtual and in person events for the company.

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

Security: Back to Basics in 2024

By Nick Hyatt Director of Threat Intelligence at Blackpoint Cyber

New year, new you, right? Every year when the ball drops in Times Square, we make (perhaps slightly drunken) resolutions to improve our lives. Eat right, join that gym – it all sounds good until we make it halfway through February and we've reverted to our old habits because the time just got away from us. Just like in our personal lives, we often revert to old habits with security, too. I get it, security is hard! With the constant barrage of vulnerabilities, incidents, and day-to-day firefighting, even the most efficient and experienced security team can be hard-pressed to keep up. There are ways to improve your security posture without breaking the bank, buying a new tool, or even doing anything beyond the basics. Sounds too good to be true, right? Stick with me.

The first few months of the year have brought with them some concerning stories. In January, Microsoft disclosed further details of the attack they suffered from the Midnight Blizzard threat actor. Midnight Blizzard is a Russia-aligned threat actor – they're no slouches. You would think the attack they pulled on Microsoft would be some sort of incredibly spooky zero-day malware, right? Not in this case. Microsoft had a legacy system out in a tenant that had a simple password and no multi-factor authentication present, which allowed Midnight Blizzard to compromise the account and pivot internally.

This is a big story – not just because it's Microsoft, but precisely because of the nature of the attack. Threat actors love a "simple" hack. Credential stuffing is incredibly easy and presents a massive return on investment. Threat actors love legitimate credentials for multiple reasons, including:

1. **Access** - Once I have credentials, I have access to the environment.
2. **Observation** – I can sit quietly in an environment and watch what happens – how does the IT team work? What do your security people monitor for?
3. **Escalation** – Threat actors can profile out a network and deploy further tools to harvest more credentials, deploy malware, or as we saw in the Midnight Blizzard attack, read emails.

As a threat actor, if all I must do is compromise an account, then I already have what I would normally have to expend a lot of effort to gain – legitimate credentials. Once I have legitimate credentials in an environment, it's much easier to monitor traffic and learn what I need to do to mask my activity, making it that much harder for defenders to catch me. There's a reason the cybercriminal ecosystem exists – by harvesting credentials and compiling them, threat actors can perpetrate these sorts of attacks and gain legitimate access to environments, at which point the ball is in their court and they have control of the game.

So how does all this tie into returning to basics? The important thing about the Microsoft story is not that it was Midnight Blizzard – it's that it was a basic credential stuffing attack against an unprotected account. Microsoft is a three-trillion-dollar company – if this happened to them, it certainly could happen to you. Credentials are traded by cybercriminal organizations all the time, both on the clear web and the dark web. Ensuring you are doing your level best to protect your systems against these sorts of attacks will reduce your threat profile and make it that much harder for a threat actor to gain access to your environment. Be sure, they will gain access, but if they have to expend additional effort to get into your environment rather than a simple credential stuffing attack, that gives you that much more time to detect and evict them before they can wreak havoc.

How do you return to the basics? Take these as action items for your 2024 Back to Basics checklist:

1. **Use complex, unique passwords**. The proliferation of password management software makes generating unique complex passwords for accounts extremely simple. NIST recommendations around password management involve changing passwords only when compromise is suspected, or every 365 days. This puts less pressure on your users to constantly evolve passwords they have to memorize and gives you easier monitoring for your security team. Combined with password managers, it is relatively easy to drastically improve the security of your passwords beyond using !Spring2024!.
2. **Use multi-factor authentication**. It is 2024, not 2004. Multi-factor authentication being enabled wherever possible is a must, not a maybe. The internet is chock-full of automated attacks just waiting for an unsecured account. Multi-factor authentication comes with its own challenges, but *something* is better than *nothing* when it comes to delaying tactics.
3. **Monitor strange activity on accounts**. If you're using complex passwords and multi-factor authentication, then the next step is to monitor for aberrant access. If someone logs in every day from New York City, and then suddenly they log in from a foreign country, that could be an indicator of compromise. While not every odd login is malicious, all malicious logins are odd.

By doing these three basic things, you can make it more challenging for threat actors to gain access to your environment. We often get so caught up in the newest zero-day or newest technology fad that we forget threat actors use basic attacks the most. Verizon reported that 74% of all security incidents started with the person – whether that was social engineering, credential stuffing, or otherwise. By ensuring you are doing the basics correctly, you can focus on more important things – like maybe making sure you're actually *using* that gym membership you signed up for.

About the Author

Nick Hyatt is the Director of Threat Intelligence at Blackpoint Cyber. He has 20 years of experience in the cybersecurity and information technology fields. His primary focus during his career has been in digital forensics, malware analysis, and threat intelligence in myriad environments, from startups to Fortune 100 companies. He can be found on LinkedIn at https://www.linkedin.com/in/nphyatt/ and at our company website http://www.blackpointcyber.com/

The Changing Cyber Threat Landscape in the German Manufacturing Industry

By Dr. Elisa Costante, VP of Research at Forescout Technologies

A global Look

2023 was an eventful year in terms of cyber events (and not only!). The continuation of ongoing conflicts and the emergence of new ones, the mass exploitation of critical vulnerabilities and the ever-increasing threat of cybercrime were some of the key factors influencing the year.

Forescout Technologies, recently released its 2023 Threat Roundup where its researchers look back at all the data they have collected relating to attacks and the threat landscape of 2023 and offer organizations tactical insights and strategic recommendations for improved defense.

From the report, it emerges how cyber-attacks originated from 212 countries. The top 10 countries (see Figure below) account for 77 % of the malicious traffic, with a spike in attacks originating from China.

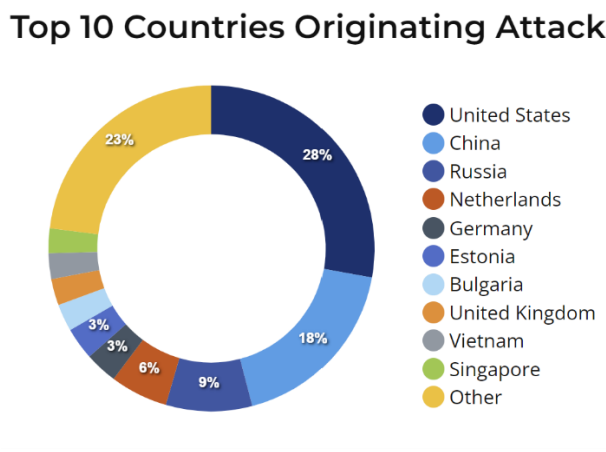


Figure 1: Top 10 Countries for Originating Attacks (Source: https://forescout.vederelabs.com/)

At Forescout we track and monitor around 600 threat actors. In 2023, they targeted 163 countries. The United States was the most targeted by far, in the second place came the Unted Kingdom, then **Germany,** India and Japan. The vast majority of threat actors originated from **China, Russia and Iran.** Together, these three countries accounted for almost half of threat actor groups in our database. Government, Financial Services, and Media and Entertainment were the industries most targeted by these actors.

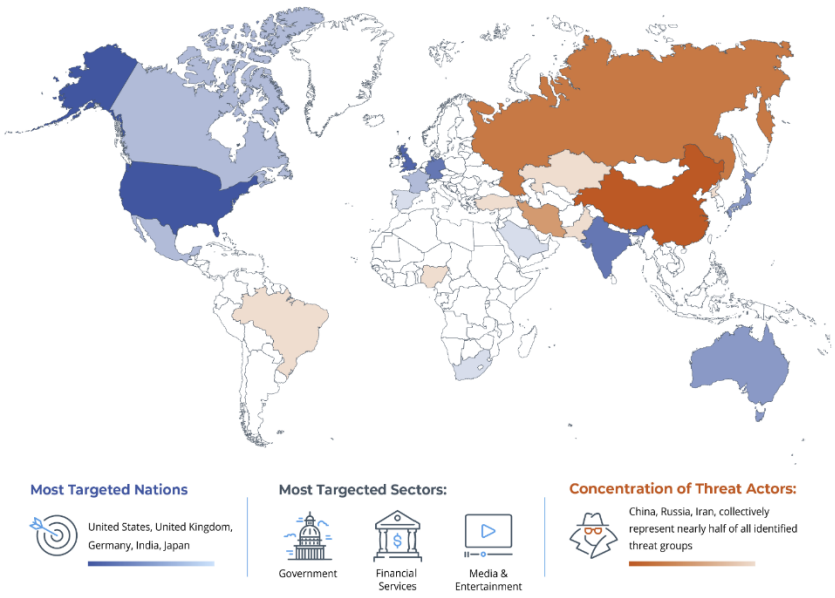


Figure 2: Threat actors targeted 163 countries. The United States stands as the primary target, with 168 malicious actors setting their sights on the nation. Other countries include the United Kingdom (88) and Germany (77) (Source: https://forescout.vederelabs.com/)

The researchers observed an increase in the use of compromised devices to launch attacks, whether directly or via "residential proxies". This is reflected by the fact that 48% of attacks came from IPs managed by ISPs, 32% from organizations in business, government and other sectors, and 10% from hosting or cloud providers.

Web applications and **remote management** are the most attacked services. It is worth noting that remote management services were **often targeted with usernames linked to IoT devices**.

Exploits against network infrastructure and IoT devices increased. The most targeted IoT devices are **IP cameras, building automation, and network attached storage**.

Only 35% of exploited vulnerabilities appeared in CISA KEV, suggesting that defenders need to look at other sources to have a more comprehensive list of risky devices, especially when it comes to OT and IoT/IIoT.

OT keeps being a constant target. Five OT protocols were the most loved by threat actors: Modbus (a third of attacks), Ethernet/IP, Step7, DNP3 (with around 18% each) and IEC10X with 10% of attacks. The remaining 2% are divided into many other protocols, of which the majority is BACnet. **Most attacks target protocols used in industrial automation and the power sector.** Building automation protocols are less often scanned, but exploits against building automation are more common.

Post-exploitation actions focused on persistence (50%, up from 3% in 2022), discovery and execution. Most observed commands are for generic Linux systems, but there were also commands executed specifically for networking operating systems that run on popular routers.

The researchers observed an equal amount of remote access trojans (RATs) and information stealers (infostealers) as the most popular type of malware. Botnets and other downloaders come in third and fourth, followed by crypto miners and then a variety of other malware, such as keyloggers and adware. The most popular malware families observed were the Agent Tesla RAT (16%), then variants of the Mirai botnet (15%) and the Redline infostealer (10%).

Cobalt Strike remained the most popular command and control (C2) architecture (46%), followed by Metasploit (16%) and the emerging Sliver C2 (13%). Most C2s are located in the United States (40%), followed by China (10%) and Russia (8%).

A Closer Look at Germany

Germany is a focal point for cyber threats. Of the 600 threat actors we track, 82 primarily target German's organizations. These threat actors mostly originate from Russia and China. Among their targets, the government sector remains the most targeted sector. It is important to note that **the manufacturing sector is ranking as the seventh most targeted industry in Germany.** This underscores the evolving landscape of cyber threats in the region, where both nation-state (mostly interested in espionage) and non-state actors (mostly interested vin financial gain) are actively pursuing their objectives with increasing sophistication.

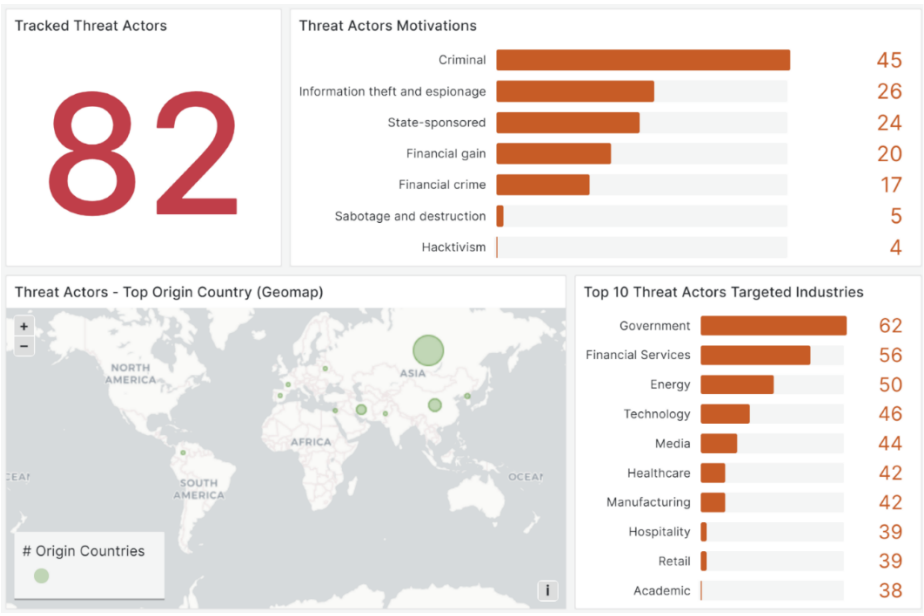


Figure 3: The Threat Landscape in Germany. Source: Forescout Technologies (www.forescout.com)

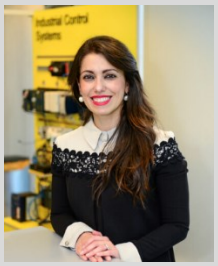
Final Remarks

We expect the cyber threats to the manufacturing sector to evolve with increasing sophistication and potentially devastating impacts. As manufacturers increasingly integrate digital technologies into their operations, including the Internet of Things (IoT), artificial intelligence (AI), and machine learning, the attack surface for cyber threats widens, making them more vulnerable to sophisticated cyber-attacks. These could include ransomware attacks that halt production lines, espionage to steal proprietary information, and sabotage that could cause physical damage to machinery. The interconnectivity of supply chains further amplifies these risks, as a breach in one area can have cascading effects throughout the sector. Manufacturers must therefore prioritize cybersecurity, adopting a holistic approach that includes regular risk assessments, employee training, and the implementation of advanced security measures to protect against future cyber threats. This proactive stance will be crucial in safeguarding the sector's digital transformation journey, ensuring resilience against the evolving cyber threat landscape.

About the Author

Dr. Elisa Costante, VP of Research at Forescout Technologies.

You can reach me via https://twitter.com/ElisaCostante



The Global Crisis Cyber Security Perspectives

By Milica D. Djekic

It appears the world has never been in a more serious crisis during this modern age as it is with a beginning of the new millennium, so far. The concerning areas, as well as terrorism are present nearly across the entire global scene and practically, there is no continent on the planet which is not affected with some critical events or at least shaken with a situation coming from a surrounding spot. Indeed, the world is obviously on test being challenged to demonstrate how well the humankind can perform over all dramas and traumas the civilization has received with the 21st century. The role of security is to manage a risk and not only so, but more likely it's needed more than ever to think hard about some controlling mechanisms that can prevent societies from being an aim of the severe criminalities. The majority of the current crimes are committed by human threats and even if the world is not yet at such a level to get machines being fully independent and a true risk to people and their infrastructure, it's clear why it matters to pay a special attention to bad actors who can make harm to an overall community, so far. In addition, the recent experience with a COVID-19 has shown that human beings can be killed even in a peaceful condition as some bioterror weapon is capable to in a totally asymmetric fashion, hurt many and even as

a military conflict takes lives of the millions of people, as well as damage health of many of so who have survived that biological strike. On the other hand, what is well-known within a modern world is anyone among defense and that is also a case with the criminal and terrorist organizations must deal with the identity and trust management systems as they are a way to assure an access to some environment, literally, to all of so who are in a register of that group that has some biometrics parameters, as well as the entire records for all such members, so far.

It's quite difficult getting trusted with any organization even being governed by any criminal or terror group as those units have their members internationally and usually transfer their messages over the globe, and it is pretty trickery to anyone either in legal or unlawful community to be familiar with any networking member in a transnational context. In other words, for such a reason many transnational organized crime and terrorist rings must rely on a fingerprint checking system which serves to confirm an identity, as well as manage trust to those trying to get provided an access to such an organization, so far. As it is well-known, many defense services with a capacity to combat organized crime and terrorism will monitor on the criminality group members mainly their couriers who would need to get confirmed once they come with the secret information. In order to make so they will be checked by online checking assets which could use a fingerprint reader to scan someone's finger and do some recalling from that cloud application making a connecting with some server or datacenter which accommodates records of those persons.

This is possible through the visible web infrastructure, but there could be some challenges if that querying would go via some decentralized communication system as in such a case, the entire records would be very hidden and a bit dangerous than those going through the surface internet. Apparently, there is a word about the online applications which could be available via some Darknet platform and if the authorities catch such an information exchange, they could cope with some straggling attempting to take out data from such a dynamic server. Hence, in a sense of the Tor privacy browser, it's clear those secret spots could belong so some onion domains and if an endpoint uses some reliable web link such as, say, a satellite network the track could be camouflaged as the deep web communication goes via relays and very sophisticated cryptosystems making it hard to trace such a data transfer, so far. Also, sometimes the Darknet communication might collapse, but that risk is equally frequent as losing connection with any visible web online grid as such an incident always can be predicted and, in that manner, no one will be distracted with so.

The majority of criminality actors work for a profit and in a case of the terrorism, it's necessary to assure some finances that some terror spreaders could spend on their training, staying, travelling and so on getting in mind by that some transnational organized crime groups could sponsor their activities at the global level trying to cause conflicts, unrest and troubles to communities they want to make to capitulate in front of their dominance assuring for themselves a pawn over some territory or region, so far. The point with so is the good guys can make some high-tech tracking giving them an opportunity to figure out when someone of the lawbreakers is uncovered, but it yet looks like that there are truly a plenty of the methods to avoid the rules and count on someone's situational unawareness and sometimes a lack of the helpful skills in fighting against the crime. In total, some studies suggest that those being in a criminal business will not that easily give up from their illegal activities, but more likely try to trick the law proposing new criminal schemes which will deal with an awareness about what the investigations really look for and getting such a finding could be feasible if some of the officers or at most their commanders are corrupted and willing to sell some professional secrets for a couple of millions of dollars putting in such a sense,

the entire community and the legal system under the threat which will always provide an advantage to the bad guys even if a mission of the security is to get ahead a step in front of the threatening actors, so far.

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.

The Pros and Cons of Artificial Intelligence in Healthcare

Examining the Benefits and Downsides of Artificial Intelligence and How It Can Be Used in Healthcare

By Veronika (Nikki) Jack, Student Majoring in Information Technology-Cybersecurity, Intern at the IT Security Office, George Mason University

While artificial intelligence (AI) is evolving each day and can help us with many tasks that offer unprecedented opportunities for innovation, efficiency, and advancement, its implementation also brings forth significant ethical, societal, and economic challenges.

The benefits of artificial intelligence range from an increase in efficiency to creating personalized experiences for people. AI systems can automate tasks and processes, leading to increased efficiency and productivity across various industries. This can include everything from data analysis to customer service. AI can also increase the accuracy of data and perform tasks with a high degree of consistency with less errors. In some cases, it can often outperform humans in tasks such as image recognition, data

input, and analysis. AI increases innovation and advancements in healthcare, transportation, finance, and many other fields.

On September 9th, 2023, at the BSides NoVA conference, I attended different speakers' sessions and learned many different innovations in technology. One session was presented by Quinn Palmer, who is a Security Analyst with Presbyterian Healthcare Services. The session was "A.I. in MY Healthcare? It is More Likely Than You Think." I learned about the many benefits AI can bring to the healthcare industry. They can take notes and write reports quickly for healthcare professionals so they can focus more on patient care. They can potentially improve diagnostics and can analyze medical imaging scans, such as X-rays, MRIs, and CT scans, with high accuracy, aiding in the early detection and diagnosis of diseases. AI can give a personalized experience by analyzing patient data, medical history, and lifestyle factors, to recommend treatment plans tailored to individual patients. AI technologies enable remote patient monitoring, virtual consultations, and telemedicine platforms, improving access to healthcare services, particularly in rural or underserved areas.

On the left is the author (Nikki), on the right is Quinn Palmer

However, there are some cons to using AI in the healthcare environment, because there needs to be a lot of data input to train AI to recognize disease, which can lead to diagnostic errors or unequal access to treatment. You would trust AI to diagnose a cold or the flu, but how about a rare disease that only is

found in one in a million? It will have a harder time finding the rarer diseases and can even mistreat them. People also may not trust using this technology.

We also must be careful and make sure that people's medical data isn't released to others, it needs to be secure. AI systems rely on vast amounts of sensitive patient data, raising concerns about privacy breaches, data misuse, and cybersecurity threats, particularly as healthcare data is highly regulated and prone to hacking. They must navigate complex regulatory frameworks, such as HIPAA in the United States and GDPR in Europe, to ensure compliance with data protection laws and ethical guidelines, which can pose barriers.

Another risk is overreliance on AI technologies which leads to less jobs in the healthcare profession, potentially causing unemployment in certain sectors. Over-reliance on AI systems may lead to dependency issues, and their reliability can be compromised in certain situations, such as unexpected scenarios or system failures.

While AI excels at tasks involving data and logic, it lacks the creativity and intuition that humans possess. The use of AI raises ethical questions, especially in areas like privacy, surveillance, and decision-making autonomy.

Overall, artificial intelligence holds immense promise in transforming industries, enhancing efficiency, and driving innovation in numerous aspects of modern society. As I learned from attending the session on AI in our healthcare, I heard what benefits AI can bring to the workplace. I also see the reasons why having more reliance on artificial intelligence has some drawbacks and security concerns.

About the Author

My Name is Veronika (Nikki) and I am a student at GMU (George Mason University) student majoring in Information Technology with a concentration in Cybersecurity.

I am an IT Security Office Intern at George Mason University.

Nikki can be reached online at mailto:njack4682@gmail.com

The State of AI in Cybersecurity

Transforming Cyber Defense in the Modern Era

By Joe Ariganello, Vice President Product Marketing, MixMode

As organizations navigate an increasingly complex and dynamic cybersecurity landscape, artificial intelligence (AI) has become pivotal in fortifying defenses and combating evolving cyber threats.

With the rise and adoption of ChatGPT, one could argue that artificial intelligence is one of the most important technologies of our time. AI is driving major technological and societal transformations and will continue to revolutionize how businesses operate and how people work and live. While AI does pose some risks, the tremendous benefits far outweigh the potential downside. Responsible development and regulation of AI will allow enterprises to thrive in the modern era and an understanding of the possibilities can be transformational.

To further understand the perception of AI with enterprise organizations, MixMode commissioned the Ponemon Institute to survey cybersecurity professionals and gauge how AI is used for cybersecurity in their organizations. The State of AI in Cybersecurity 2024 report offers valuable insights into the adoption,

challenges, and transformative potential of AI-driven security technologies and provides a comprehensive analysis of how AI is reshaping the cybersecurity landscape. This article delves into the report's key findings, highlighting the evolution of AI in cybersecurity and exploring how organizations can harness the full potential of AI to safeguard their digital assets and infrastructure.

Key Findings in the State of AI in Cybersecurity 2024 Report

Threat Landscape and AI Adoption

The evolution of artificial intelligence in cybersecurity has significantly transformed how organizations approach threat detection, response, and their overall security posture. The report underscores the prevalence of cyberattacks, with 45% of organizations experiencing various attacks within the last year, including phishing/social engineering, web-based attacks, and credential theft.

In response to these threats, organizations are turning to AI for support. Notably, 53% of respondents indicated their organizations are in the early stages of AI adoption for cybersecurity, highlighting the growing recognition of AI's potential in fortifying security measures.

Challenges and Current Usage of AI

While AI presents significant opportunities for enhancing cybersecurity, organizations face challenges in its adoption. These include difficulties complying with privacy and security regulations, integrating AI-based security technologies with legacy systems, and increasing in-house expertise. Despite these challenges, organizations are leveraging AI to detect attacks across cloud, on-premise, and hybrid environments, increase the productivity of IT security personnel, and address the shortage of cybersecurity expertise.

Realizing the Benefits and Value of AI

The report emphasizes the benefits of using AI in cybersecurity, including prioritizing threats and vulnerabilities by minimizing false positives, identifying application security vulnerabilities, and accelerating the containment of infected endpoints. However, it also highlights that the full value of AI is yet to be realized, with only 44% of respondents expressing high confidence in accurately identifying areas where AI would create the most value.

The Evolution of Using AI in Cybersecurity

The evolution of using AI in cybersecurity has been marked by significant advancements and transformative impacts on how organizations detect, respond to, and mitigate cyber threats. Over the years, AI has revolutionized the cybersecurity landscape, offering innovative solutions to address the growing complexity and sophistication of cyberattacks.

Early Applications of AI in Cybersecurity: The early adoption of AI in cybersecurity focused on rule-based systems and signature-based detection methods. These systems were effective in identifying known patterns of malicious activity, such as viruses and malware, but were limited in their ability to adapt

to new and evolving threats. As cyber threats became more sophisticated, traditional security measures struggled to keep pace, leading to the need for more advanced and adaptive solutions.

Machine Learning and Behavioral Analysis: The integration of machine learning algorithms marked a significant turning point in the evolution of AI in cybersecurity. Machine learning enabled security systems to analyze massive amounts of data, identify patterns, and learn from past incidents to improve threat detection and response. Behavioral analysis, a key application of machine learning, allowed security systems to understand normal user behavior and detect anomalies that could indicate potential security breaches.

Advancements in Threat Detection and Response: As AI technologies continued to evolve, they became instrumental in enhancing threat detection and response capabilities. AI-powered security solutions could proactively identify and mitigate emerging threats, analyze complex data sets to uncover potential vulnerabilities, and automate response actions to contain and neutralize security incidents in real-time. This proactive and adaptive approach to cybersecurity significantly bolstered organizations' ability to defend against various potential threats.

Current State: Adopting AI as a Cornerstone of Cybersecurity: In the present day, AI has become a cornerstone of modern cybersecurity strategies. Organizations are beginning to leverage AI for various security applications, including threat intelligence, anomaly detection, predictive analysis, and automated incident response. AI-driven security technologies are capable of processing and analyzing massive volumes of data, identifying subtle indicators of compromise, and adapting to dynamic threat landscapes, thereby empowering organizations to stay ahead of cyber adversaries.

Increase in Adversarial Attacks

Integrating AI into the cyber threat landscape has ushered in a new era of challenges for security teams. AI has also revolutionized the capabilities of cyber attackers, enabling them to launch more sophisticated and targeted attacks.

The increased sophistication, evolving threat vectors, scale and speed of attacks, and the emergence of adversarial AI have raised the bar for cybersecurity defenses, presenting opportunities and challenges for security teams.

Sophisticated Cyber Attacks: AI has empowered cyber attackers to develop more sophisticated and evasive attack strategies. With AI-driven tools, attackers can automate the identification of vulnerabilities, personalize phishing attempts, and launch stealthy, multi-stage attacks that can bypass traditional security measures. This heightened level of sophistication has made it increasingly challenging for security teams to detect and mitigate cyber threats effectively.

Evolving Threat Vectors: The use of AI by cybercriminals has led to the emergence of new threat vectors and attack methodologies. For example, AI-powered malware can adapt its behavior to evade detection. At the same time, AI-generated deepfakes can be used for social engineering attacks, posing significant challenges for security teams in identifying and responding to these novel threats. Additionally, AI has

facilitated the rapid development of zero-day exploits and polymorphic malware, further complicating defending against cyber attacks.

Scale and Speed of Attacks: AI has enabled cyber attackers to scale their operations and launch attacks at unprecedented speeds. AI-powered tools can scan vast networks for vulnerabilities, execute attacks at machine speed, and exploit security gaps with minimal human intervention. As a result, security teams face the daunting task of defending against a high volume of rapidly evolving threats, requiring them to adopt agile and adaptive security measures.

Adversarial AI: The use of AI in cybersecurity has also given rise to adversarial AI, where attackers leverage AI algorithms to bypass security controls and deceive AI-powered defense systems. Adversarial attacks can manipulate AI models, generate convincing fake data to evade detection and exploit vulnerabilities in AI-based security solutions. This adversarial use of AI poses a significant challenge for security teams, requiring them to continuously adapt their defenses to counter evolving attack techniques.

Looking Ahead: AI's Role in Shaping Cybersecurity

Looking ahead, the evolution of AI in cybersecurity is poised to continue, focusing on further advancements in areas such as explainable AI, generative adversarial networks, and AI-driven predictive analytics. These developments will enable security teams to gain deeper insights into adversarial attacks, enhance the accuracy of threat predictions, and fortify their defenses against emerging cyber risks.

Maximizing the Value of AI for Cybersecurity

Moving forward, organizations can take strategic steps to derive the best value from AI for cybersecurity. This includes:

1. Investing in Advanced Analysis Methods and Generative AI: With 69% of respondents emphasizing the importance of integrating advanced analysis methods, organizations should prioritize the adoption of generative AI to enhance threat detection and response capabilities.

2. Addressing Privacy and Security Challenges: Given the challenges related to privacy and security regulations, organizations should focus on identifying vulnerabilities, ensuring comprehensive record-keeping, and educating the workforce about AI-related risks and privacy protection policies.

3. Enhancing Expertise and Integration: Organizations should invest in increasing in-house expertise, streamlining security architecture, and integrating AI-based security technologies with legacy systems to maximize their effectiveness.

4. Realizing the Full Potential of AI: To fully realize the value of AI in cybersecurity, organizations should strive to identify areas where AI can create the most impact, leveraging AI-powered solutions to bolster security infrastructure and threat detection capabilities.

MixMode: Leading the Way for Utilizing AI Effectively in Cybersecurity

The "State of AI in Cybersecurity" report underscores the pivotal role of AI in fortifying organizations' security posture. As the threat landscape continues to evolve, the strategic adoption of AI-based security technologies, coupled with a focus on addressing challenges and maximizing the value of AI, will be instrumental in safeguarding organizations against cyber threats.

MixMode is at the forefront of revolutionizing cutting-edge artificial intelligence for threat detection and response. Through harnessing the contextual adaptation, explainability, human-AI collaboration, and adaptive learning capabilities of AI, MixMode enables organizations to bolster their defenses against novel attacks and emerging threats with unparalleled efficacy and agility.

Download the full report here or reach out to learn more.

About the Author

Joe Ariganello, Vice President Product Marketing, MixMode. Joe is the VP of Product Marketing at MixMode. He has led product marketing for multiple cybersecurity companies, with stops at Anomali, FireEye, Neustar and Nextel, as well as various start-ups. Originally from NY, Joe resides outside Washington DC and has a BA from Iona University.

He can be reached online at joe.ariganello@mixmode.ai and at our company website https://mixmode.ai/

Three Tips for Federal CIOs to Improve Cyber Resilience in 2024

By Gary Barlet, Federal Chief Technology Officer, Illumio

The threat of ransomware looms large in 2024. We continue to witness firsthand the fallout from devastating supply chain attacks such as the MOVEit breach, which affected millions of customers and compromised several federal agencies, and see critical infrastructure sectors (like water management operators) face a near-constant barrage of everyday attacks.

The reality is that while ransomware attacks persist, federal agencies still face significant resourcing challenges – including shortages in funding, staffing, and comprehensive guidance, making it difficult to address the scope of these dynamic threats. With $88.1 trillion in debt globally, agencies are hard pressed to do more with less when responding to and preparing for today's attacks.

But there are proactive measures that federal Chief Information Officers (CIOs) can take to enhance their cyber resilience plans and better protect their own IT environments in the year ahead. By shifting their mindsets towards smaller and more achievable goals, recognizing that cyber resilience is an ongoing

strategy, and encouraging cross-functional collaboration to reach and maintain tailored security objectives, federal agencies can better navigate the evolving threat landscape in the months ahead.

Stop Chasing Cyber Perfection

In 2024, rather than concentrating solely on shoring up individual layers of security, agencies must focus on building a comprehensive security posture that encompasses the entire IT ecosystem – prioritizing progress over perfection. For example, instead of working to perfectly shore up each pillar of CISA's Zero Trust Maturity Model (identity, devices, networks, applications and workloads, and data), agencies should first take a step back and identify where their greatest vulnerabilities lie across pillars. Then, implement measures to address those weaknesses accordingly.

Moving away from a linear, perfection-centric mindset towards a proactive and adaptive approach can help CIOs shift from a checklist mentality to a more sustainable strategy that addresses multiple security facets simultaneously. This not only affords agencies a greater ROI on their cybersecurity investments (enabling them to more quickly quantify successes across a larger margin), but it also goes a long way in shoring up agencies' expansive attack surface as the digital landscape evolves and widens.

Adopting a more customizable, holistic approach also enables agencies to think more proactively when it comes to risk mitigation and breach containment. In Zero Trust terms, we like to call this adopting an "assume breach" mindset, which actively encourages agencies to put solutions in place to minimize a breach's impact when it inevitably occurs. This ensures that regardless of where a breach originates – an endpoint device, a vulnerable network, a compromised cloud environment – attackers cannot move unimpeded across sensitive IT infrastructure.

By focusing on incremental progress and adopting an "assume breach" mindset, agencies reap numerous benefits, including ensuring that everyday attacks don't turn into mission-impacting breaches. Additional strategies, like ensuring cross-agency visibility, strategic asset segmentation, and the use of tools and practices for comprehensive threat modelling and understanding, are also crucial for effective and lasting resilience.

Cyber Resilience is Not One-Size-Fits-All

Rejecting the notion of a "one-size-fits-all" approach to security is paramount in fostering effective cyber resilience, especially for federal agencies. Rather than seeking a singular, universal solution, it's essential that agencies prioritize strategic enablers like visibility, and embrace a customized approach that aligns with the specific needs and vulnerabilities of their organization.

Stagnation in cybersecurity can leave agencies vulnerable to threats, highlighting the necessity for an ongoing approach that allows for continuous learning and evolution. By starting small, and by building basic cybersecurity hygiene practices into more facets of the organization, agencies can boost their cyber resilience across the board. This can include:

Prioritizing visibility: Visibility is the cornerstone of Zero Trust; you can't secure or defend against what you can't see. Gaining visibility across environments and controls, particularly for federal agencies, is an essential starting point for Zero Trust, and it plays a crucial role in enabling any Zero Trust strategy.

Adopting segmentation: Incorporating proactive technologies like Zero Trust Segmentation into the security stack, which can play a pivotal role in ensuring that when cyberattacks occur, they're quickly contained to limit the "blast radius" of the breach. Essentially, ensuring critical assets remain safeguarded and operations can continue even while an agency is under active attack.

Offering security trainings: Providing regular trainings on concepts like phishing to all staff members enhances their understanding of modern cybercriminals' tactics, contributing to the prevention of cyber breaches and fostering a more cyber-literate agency environment.

Implementing multifactor authentication: Another critical Zero Trust technology that can help agency's shrink their attack surface by practicing least privilege through continuous verification.

Own the Cybersecurity Narrative

It will take a collective effort for federal cybersecurity strategies to be successful. Gone are the days when security was solely the IT team's responsibility. Today, it requires cross-team collaboration and accountability.

To this end, advocating for the integration of cybersecurity discussions into broader organizational strategies and decision-making is essential to ensure that security is prioritized at all agency levels. And establishing regular communication channels between IT and agency leaders will facilitate greater transparency and accountability – ensuring alignment across security objectives, investments, and broader agency goals.

With federal cybersecurity guidance, like The White House's National Cybersecurity Strategy, continuing to be rolled out, it's clear that cyber is top of mind when it comes to strengthening national security. For agencies, and federal CIOs, looking to make good on their cybersecurity roadmaps in the year ahead, resilience and the ability to make good on Zero Trust progress will boil down to these key things: collaboration, accountability, proactivity and progress.

Together, by prioritizing these four elements, agencies will be better equipped to mitigate risks and strengthen their cyber defenses against everyday cyberattacks, ultimately enabling them to better protect the integrity and reliability of critical assets, essential operations and sensitive data as threats persist and evolve.

About the Author

Gary Barlet is the Federal Chief Technology Officer at Illumio, where he is responsible for working with government agencies, contractors and the broader ecosystem to build in Zero Trust Segmentation as a strategic component of the government Zero Trust architecture. Previously, Gary served as the Chief Information Officer (CIO) for the Office of the Inspector General, United States Postal Service. He has held key positions on several CIO staffs, including the Chief of Ground Networks for the Air Force CIO and Chief of Networks for the Air National Guard CIO, where he was responsible for information technology policy and providing technical expertise to senior leadership. He is a retired Lieutenant Colonel from the United States Air Force, where he served as a Cyberspace Operations Officer for 20 years. Gary can be reached online at https://www.linkedin.com/in/gary-barlet-4384115/ and at our company website https://www.illumio.com/.

Top 4 Takeaways from Fortra's 2024 Cyber Survey

By Antonio Sanchez, Principal Cybersecurity Evangelist, Fortra

What were the biggest cybersecurity challenges companies faced in 2023? And what will security leaders focus on in 2024? Fortra launched its inaugural State of Cybersecurity Survey to help answer pressing questions like these and provide insight to the industry. There were over 400 responses to our inaugural survey representing 40 different industries across the world. Here are the big takeaways from this year's survey.

Phishing and Smishing

Four out of five people cited phishing and smishing as their top risk for 2024. To gain initial access, phishing is still the most common tactic used in an attack campaign and it continues to evolve with new innovations. Early 2023 saw a sudden rise in popularity of ChatGPT, which has been used to create more

enticing emails in cleaner grammar and punctuation in many languages. Smishing is also rising in popularity as employees use their personal mobile devices for business. In both instances, the bad actor wants the victim to let down their guard for just a moment and click on a link. This allows the bad actor to gain entry and continue the attack sequence. Organizations should ensure their employees use multi-factor authentication (MFA) and ongoing security awareness training to help protect themselves.

Hybrid Cloud Security

Sixty-four percent of respondents said they plan to have a hybrid IT model of both cloud and on-premises. Digital transformation initiatives have driven cloud adoption with strategies of being cloud-preferred and cloud-first, but there is still a need for an on-premises footprint for many organizations. Customers have shared that mission-critical workloads may remain on-premises as the preferred choice for data sovereignty requirements. Others said certain workloads have architectural limitations in the cloud or the resource requirements for refactoring don't justify moving to the cloud. Whatever the reason, on-premises footprints will always be part of the IT estate for the majority of organizations now and into the future, requiring security leaders to develop a holistic approach for securing a hybrid environment. This includes visibility and consistency across all environments for things like threat management, identity and access management, and misconfigurations.

Vendor Consolidation

Vendor consolidation is something that two out of three organizations will be focusing on in 2024. In years past, when there was a new attack vector, there would be a new category of tools to address that problem. Security teams wanted the best-of-breed tooling to address each new attack vector; this has resulted in tool sprawl, creating an operational nightmare. Customers have told us there is now a higher priority on solutions that are tightly integrated and solve a broad set of use cases. Being best-of-breed is a bonus, but not the primary driver anymore. Organizations cite overlapping capabilities in tools as one of the drivers that helps reduce vendors, along with simplified operations, which reduce costs and operational overhead.

Third-Party Support

One of the more interesting takeaways from the survey is that over half of respondents are either using or planning to use a third party to help secure their organization. Transferring a portion of the operational burden to a managed security service provider (MSSP) allows the organization's security team to focus their efforts on more impactful and higher value projects. The areas where respondents most often say they are using an MSSP include email security and anti-phishing (58%), vulnerability management (52%), and data protection (51%). In most instances, an MSSP can manage the operational burden of a security control for less than the cost of a skilled full-time headcount.

A few final thoughts from our survey. First, make sure you do the basics well. Patching is not exciting, but it is still one of the most effective ways to reduce your attack surface so make sure you have disciplined patch management program. Second, focus on your vital few. Digital transformation continues to accelerate so focus your priorities that align to the business. Finally, invest in your people. The tools continue to get better, but nothing takes the place of highly skilled people.

The complete results of the 2024 Fortra State of Cybersecurity Survey are available on the Fortra website. Fortra also led a discussion with three cyber experts, providing additional context and insights on the results.

About the Author

Antonio Sanchez is Principal Cybersecurity Evangelist at Fortra. As a subject matter expert for Fortra's security portfolio, Antonio helps drive market recognition for the Fortra brand. He joined Fortra from Alert Logic in 2023, where he developed the messaging, positioning, and technical content for the Managed Detection and Response (MDR) business. Alert Logic was acquired by Fortra in 2022.

Antonio has over 20 years in the IT industry focusing on cybersecurity, information management, and disaster recovery solutions to help organizations of all sizes manage threats and improve their security posture. He is a Certified Information Systems Security Professional (CISSP).

Antonio has held various product management, technical sales, and strategic marketing roles with Dell, Forcepoint, and Symantec. At the latter, he was responsible for developing and leading the Competitive Intelligence Program for the core security unit.

www.fortra.com

Traditional Access Control is Outdated

How passwordless authentication and conditional access shine as beacons of hope, signaling a safer, more user-friendly future for digital access

By Denny LeCompte, CEO, Portnox

In the fast-paced and evolving landscape of cybersecurity, Chief Information Security Officers (CISOs) are under immense pressure to minimize risks, optimize budgets, and adapt to increasingly sophisticated threats. One area of critical concern is access control. With the Cambrian explosion of IoT, the rapid adoption of bring your own device (BYOD) policies, and the expansion of networks in all directions, traditional mechanisms of access control simply aren't up to the task anymore. Today's cybersecurity landscape demands more robust solutions. Enter the revolution we've been waiting for: passwordless authentication and conditional access.

The Shortcomings of Traditional Access Control

At the epicenter of our cybersecurity conundrum lies the antiquated mechanism of traditional access control. Predominantly reliant on static passwords, it predicates its security on users' capacity to remember and secure intricate combinations of alphanumeric and special characters. Despite its longstanding position as the linchpin of cybersecurity, this mechanism carries with it a host of vulnerabilities.

To begin with, the inherent human propensity to forget complicates matters, making passwords a notoriously fallible method of protection. Coupled with this, the unwieldy nature of complex passwords often incites users to take shortcuts - sharing and reusing passwords or storing them in insecure locations - creating gaping security holes that are ripe for exploitation.

Moreover, the intricate dance of managing, updating, and resetting passwords commands an inordinate amount of time and resources, distracting cybersecurity teams from more pressing and strategic tasks. This often leads to a myopic focus on password management, inadvertently neglecting other facets of cybersecurity that require immediate attention.

The last straw is the static nature of traditional access control, providing little room for adaptability in the face of evolving threats. Unlike the more dynamic and context-aware conditional access, traditional systems remain rigid, failing to adapt to the ever-morphing landscape of cyber threats.

The Promise of Passwordless Authentication

Transitioning to passwordless authentication marks a significant advancement in the realm of cybersecurity. By discarding the need for conventional password-based systems, this innovative approach alleviates a myriad of security concerns and fundamentally redefines the user experience. As the name suggests, passwordless authentication eschews the need for users to remember or input passwords, replacing them with more secure and user-friendly mechanisms such as biometrics, security tokens, or single-use codes.

This ground-breaking approach harbors several noteworthy advantages over its conventional counterparts. Most importantly, by eliminating the need for passwords, it obviates a key vector for cyberattacks. With no passwords to crack, steal, or guess, cybercriminals are deprived of a principal avenue of attack, markedly enhancing the security of our systems.

On the user front, passwordless authentication greatly simplifies the interaction with digital systems. The arduous process of memorizing, managing, and periodically updating complex passwords becomes a thing of the past. The convenience provided by biometric authentication or single-use codes not only fosters user satisfaction but also enhances security, as users are less likely to resort to unsafe practices such as password sharing or reuse.

Raising the Bar with Conditional Access

While ditching passwords signifies a good first step in improving one’s organizational security posture, embracing the revolution of conditional access represents a game-changing shift in overall cybersecurity strategies. It represents a dynamic departure from the static nature of traditional password-based systems, by ushering in a sophisticated, context-based paradigm that relies on encrypted digital certificates which offer an exponentially greater degree of security. This transformative approach evaluates a multitude of real-time indicators before granting access, rather than merely relying on static passwords.

Under this model, an assortment of factors comes under scrutiny. These include user and device behavior patterns, geographical location, the health status of the device, and even the timing of the access request. Through this rigorous evaluation, the system capably adapts to the ever-changing threat landscapes and provides access only when the circumstances meet security requirements.

The true value of conditional access lies in its data-driven, real-time security assessments. It doesn't just ask 'who' is attempting to access the system but delves deeper into the 'why', 'how', 'when', and 'where'. This nuanced, context-aware approach offers a potent line of defense against cyber threats, making it indispensable in our modern digital landscape.

Conditional access ushers in a new era of cyber vigilance, embodying a more intuitive, adaptive approach that outpaces the linear defenses of yesteryears.

How to Get Started

Embracing a passwordless environment may seem complex but if the implementation process is meticulously broken down into strategic steps, the transition can be incredibly streamlined and productive.

The initial step revolves around selecting the right kind of technology. With the help of digital certificates, organizations can encrypt communications, endorse emails and files, ensure integrity and proof of origin, and perhaps most critically, provide robust authentication services. Unlike passwords, digital certificates provide cryptographic proof of the user's identity which substantially diminishes the probability of successful impersonation or man-in-the-middle attacks.

The subsequent step involves incorporating an access control system that is not only proficient in delivering centralized Certificate Authority (CA) services but also seamlessly fits into the existing network infrastructure. A modern, flexible network access control (NAC) platform will deliver just that – and can use machine learning to identify behavioral patterns, layer on multi-factor authentication, and detect any anomalies in real-time.

But implementing digital certificates without an overarching cyber security strategy might still leave loopholes. That's why conditional access should be part of the overall approach. It aids in building granular control by imposing 'conditions' based on user identity, location, device health, and so on. Incorporating conditional access with certificate-based authentication makes sure only verified identities can access sensitive information.

Next, testing the entire setup is crucial. CISOs should look to stress-test the implementation in real-world scenarios, mitigating vulnerabilities and addressing unforeseen risks. Here, aspects like user experience should not be overlooked, ensuring that robust security measures do not hinder employee productivity.

Lastly, while staff training cannot be emphasized enough, people will always continue to make mistakes. It’s what makes us human. Thus, implementing tools that can automatically enforce passwordless authentication, access control, and risk mitigation policies is necessary.

Artificial Intelligence, Access Control & the Road Ahead

The migration from antiquated access control systems to the novel arenas of conditional access and passwordless authentication is a calculated stride towards an enhanced cyber fortress.

Furthermore, expectations are rapidly mounting as developments in the realms of hyper-personalized AI and Explainable AI algorithms mature, bringing to the fore cutting-edge prospects for personalized security measures. Considering the swift advancements in AI and machine learning, it won't be surprising to witness these technologies shaping access control and security policies on a more individual level within the next few years.

With hyper-personalized AI, systems can customize security protocols for each user and device (i.e. BYOD, IoT, or managed) by analyzing their behavioral patterns, risk profiles, and access needs. Additionally, Explainable AI will pave the way for greater transparency in automated decisions in access control. This would provide a much-needed insight into why specific security actions are taken, effectively making the entire system more accountable and trusted among CISOs and other stakeholders.

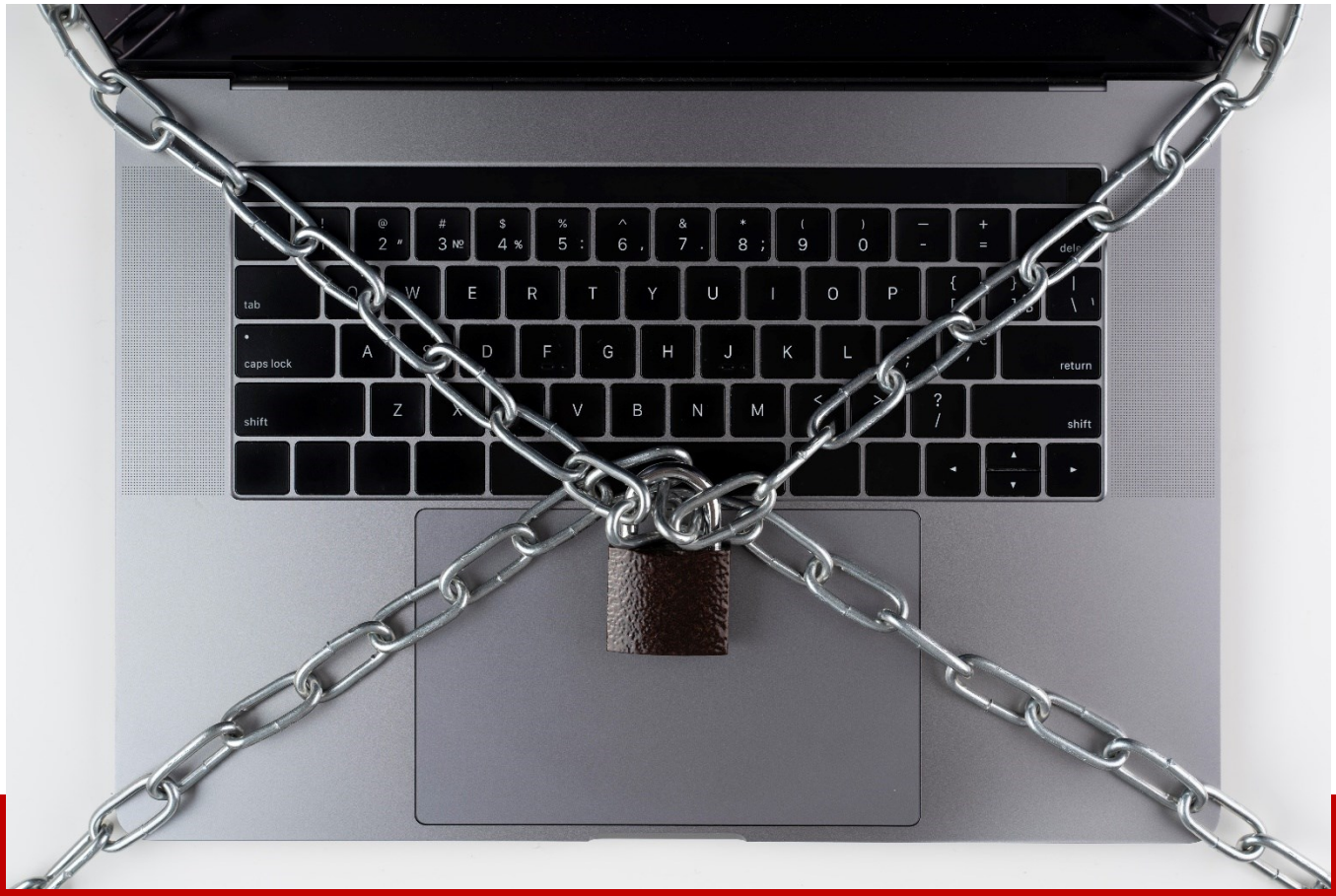
To remain ahead in this competitive, rapidly evolving cyber world, it is essential for security leaders to embrace this shift towards more adaptive, intelligent, and explainable security infrastructures.

About the Author

Denny LeCompte is the CEO of Portnox. He is responsible for overseeing the day-to-day operations and strategic direction of the company. Denny brings over 20 years of experience in IT

infrastructure and cyber security. Prior to joining Portnox, Denny held executive leadership roles at leading IT management and security firms, including SolarWinds and AlienVault. Denny holds a Ph.D. in cognitive psychology from Rice University.

Denny can be reached online at denny@portnox.com and at our company website https://www.portnox.com/.



Unleash Innovation by Replacing Barriers with Guardrails

By Craig Burland, CISO, Inversion6

Gandalf defiantly shouted – "You shall not pass!" – and erected a magical barrier that halted the advancing Balrog, a massive, fiery demon, momentarily saving the company from certain destruction. Then the barrier failed, and the demon dragged Gandalf into the depths.

Don't be like Gandalf.

In the rapidly evolving digital landscape, the need for robust cybersecurity measures has never been more critical to save organizations from certain risks. However, the traditional approach to cybersecurity, characterized by procedural roadblocks and carefully crafted checkpoints, has proven to be a double-edged sword. While this approach mitigates risks, it inadvertently stifles innovation, decelerates the pace of business, and incentivizes rule-breaking to get things done. This flawed and failed approach must be

jettisoned in favor of a new model that flips the paradigm, acknowledging that the pace of business shouldn't be slowed, but that cybersecurity must be sped up!

Removing Barriers

Traditional cybersecurity thinking creates a heavily guarded road with speed bumps, stop lights, and guarded checkpoints to protect organizations from risk. Every new initiative or innovative project must run this gauntlet to expose potential threats and ferret out uncertainty, inevitably leading to significant delays. This "security first mentality" is fraught with bad friction and inadvertently creates a culture of inhibition where the fear of potential threats overshadows the potential benefits of innovation. As businesses today need to be agile and innovative to stay competitive, this model is increasingly untenable.

Now imagine pulling those barriers off the road, turning them 90 degrees, and lining them up as guardrails to clearly mark the approved path. Expressed as a vision: transform 42nd Street in Manhattan into the Autobahn. Expressed in ASCII: Turn these | | | | into these = = = =. Unlike the bad friction of roadblocks and barriers, guardrails don't aim to stop movement but to guide it safely and efficiently forward. This approach encourages a culture of security mindfulness where everyone understands the importance of cybersecurity, is equipped to make decisions that balance innovation with risk, and is aligned with the business's goals.

Building Guidelines and Guardrails

The essence of exchanging bad friction for good friction lies in transitioning from strict barriers and controls to less prescriptive and restrictive guidelines and guardrails. Instead of requiring every decision to go through a central security team for approval, organizations adopt a thoughtful, balanced framework of decision-making. These guidelines and guardrails provide teams with the boundaries within which they can operate safely. They are designed to be broad enough to allow for innovation and agility but narrow enough to protect against significant risks.

For instance, a guideline might dictate that any new software development must undergo a security review before being deployed, but it leaves the choice of technology and implementation strategy up to the individual teams. A guardrail may monitor for software deployed with known vulnerabilities that exceed risk appetite. This approach not only speeds up the development process but also empowers teams to take ownership of their security practices.

Fostering Security Awareness

The shift towards good friction is not just about changing policies but about fostering a culture of security awareness. It requires educating all members of the organization about the importance of cybersecurity and how they can contribute to it. When employees understand the rationale behind the guidelines and see how they enable rather than restrict their work, they are more likely to embrace them.

This culture change also involves recognizing and rewarding good security practices. By highlighting instances where teams have successfully balanced innovation with security, organizations can demonstrate the value of good friction in action. This not only reinforces the desired behavior but also shows that the organization values security as an enabler of innovation.

Challenges and Considerations

Adopting a system of guidelines and guardrails is not without its challenges. It requires a delicate balance between providing enough freedom to innovate and ensuring adequate security measures are in place. Organizations must clearly articulate the rules to avoid ambiguity that could lead to security lapses. They must monitor the guardrails to ensure no one leaps over them to run outside the business' chosen path. Critically, this approach demands a higher level of security awareness among all employees, necessitating ongoing education and engagement initiatives.

The transition to good friction requires a shift in mindset at all levels of the organization. It involves trusting teams to make the right decisions within the defined guardrails and being open to adjusting these guidelines as the business and its security needs evolve.

Conclusion

In the quest for robust cybersecurity, replacing bad friction with good friction represents a paradigm shift towards a more agile, innovative, and secure organization. By adopting a system of clear guidelines and guardrails instead of barriers, businesses can empower their teams to make informed decisions that balance the need for innovation with the imperative of risk management. This approach not only synchronizes cybersecurity to the pace of business, but also cultivates a culture of security mindfulness that permeates every level of the organization. As we move forward in this digital age, embracing good friction in cybersecurity is not just beneficial; it's essential for maintaining competitive advantage in an increasingly complex landscape.

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 http://www.inversion6.com.

Unveiling the Cyber Threats to Healthcare in the USA

By Thomas Leahy, SVP Sales, SureShield

The healthcare industry is a critical sector in the US, responsible for the health and wellness of millions of people. Unfortunately, it is also a prime target for cybercriminals who aim to exploit healthcare organizations' valuable and confidential data or disrupt their operations and services. As a result, the industry is vulnerable to cybersecurity threats that can cause significant harm.

Here, we will delve into the significant cybersecurity threats and challenges that the healthcare industry in the United States encounters. We will examine how these risks impact patient care and safety and discuss potential vulnerability management solutions and best practices to help manage these risks and improve the healthcare system's cybersecurity.

Cyber Threats and Challenges

A report by Statista has revealed that in 2020, the healthcare sector in the US suffered the highest number of data breaches and compromised records. A total of 599 breaches occurred, affecting 26.4 million records. Cyberattacks on healthcare organizations cost an average of $4.99 million, a 13% increase from the previous year.

Some of the most common and dangerous cyber threats and challenges that the healthcare industry faces are:

Ransomware

Ransomware is malware that encrypts the victim's data or systems and demands a ransom for their decryption. These attacks can severely affect the functioning and services of healthcare organizations, as they can prohibit access to critical medical records, devices, and systems. For instance, in September 2020, a ransomware attack on Universal Health Services, one of the largest hospital chains in the US, impacted more than 250 facilities and disrupted patient care for several days.

Cloud Compromise

This attack exploits vulnerabilities or misconfigurations within healthcare organizations' cloud-based services or applications. When a cloud is compromised, it can lead to data breaches, data loss, or unauthorized access to sensitive information. A real-life example of this happened in July 2019, when a cloud-based vendor for American Medical Collection Agency, a billing service provider for healthcare organizations, experienced a data breach that exposed the personal and financial data of 20 million patients.

Supply Chain

Supply chain attacks are cyber-attacks aimed at third-party vendors or partners of healthcare organizations who provide software, hardware, or services integrated with their systems or networks. These attacks can compromise the security and integrity of healthcare organizations and their data since they can introduce malicious code or backdoors into their systems or devices. An example is the massive supply chain attack in December 2020, which targeted SolarWinds, a software company that provides network management tools to various sectors, including healthcare. This attack affected several federal agencies and private companies, exposing their sensitive data and systems.

Business Email Compromise (BEC)

BEC is a phishing attack where the attacker impersonates a legitimate individual or organization to deceive the recipient into acting, such as transferring money or disclosing sensitive information. These

attacks can cause significant financial losses, data breaches, or damage to the reputation of healthcare organizations. In January 2020, a BEC attack on the Children's Hospital of Philadelphia resulted in a loss of $1.3 million, as the attackers posed as a construction company and requested payment for a project.

Impact on Patient Care and Safety

Cyberattacks on healthcare organizations can have severe and potentially life-threatening consequences for patient care and safety, as they can:

- Delay or disrupt the diagnosis, treatment, or monitoring of patients, especially those who require urgent or critical care.
- Compromise patient records' accuracy, availability, or confidentiality, which can lead to misdiagnosis, medication errors, or identity theft.
- Affect the functionality or performance of medical devices, such as pacemakers, insulin pumps, or ventilators, which can endanger the lives of patients who depend on them.
- Cause physical or psychological harm to patients, staff, or visitors due to the stress, anxiety, or fear caused by the cyberattacks or their aftermath.

A study conducted by Vanderbilt University has revealed that hospitals that suffer a data breach tend to have a higher mortality rate among heart attack patients. Such hospitals also require more time to conduct an electrocardiogram and a more extended stay. The study estimated that every year in the United States, around 2,100 additional deaths could be linked to data breaches in hospitals.

Solutions and Best Practices

To protect the healthcare industry from cyber threats and challenges and to ensure the safety and quality of patient care, there are some possible solutions and best practices that can be implemented, such as:

- Adopting a risk-based and proactive approach to cybersecurity that identifies and prioritizes the most critical assets, systems, and processes and implements appropriate controls and measures to protect them.
- Implementing a comprehensive and robust cybersecurity framework that covers cybersecurity's technical, organizational, and human aspects and follows the standards and guidelines of relevant authorities, such as the FDA, the HIPAA, or the NIST.
- Enhancing the awareness and training of healthcare staff, vendors, and partners on cyber threats and challenges and the best practices and policies to prevent, detect, and respond to them.
- Investing in the latest and most secure technologies, tools, and solutions can improve the IT security risk management and resilience of healthcare systems, networks, and devices and enable the detection and mitigation of cyberattacks.

- Collaborating and sharing information and intelligence with other healthcare organizations, industry associations, government agencies, and cybersecurity experts to learn from each other's experiences, challenges, and best practices and to coordinate the response and recovery efforts.

Conclusion

The healthcare industry is currently dealing with an increasing and changing threat landscape related to cybersecurity. This poses significant risks and challenges to the safety and privacy of healthcare systems and data and the quality of patient care. To address these challenges and mitigate the risks, the sector must adopt a comprehensive and collaborative approach towards cybersecurity that incorporates best practices and solutions while adhering to regulatory and ethical standards.

About the Author

Thomas Leahy is the SVP of Sales at SureShield. He brings a successful track record within the software and services industry in compliance, security, and risk management and is a noted business development executive introducing the first cloud-based healthcare analytic workflow tools in quality, patient safety monitoring, and pay for performance programs. He has led several companies from founding to exit and has extensive experience in sales management, contracting, partnership, re-seller, and OEM sales distribution. Thomas can be reached online at (tleahy@sure-shield.com, https://www.linkedin.com/in/thomas-leahy-a497aa4/) and at our company website https://sure-shield.com/

Why 97% of US CIOs are Concerned with Cybersecurity

By Tracy Collins, VP of Sales, Americas, Opengear

Cybersecurity has always been top-of-mind for business leaders – namely, CIOs. Cybercriminals constantly search for network vulnerabilities, like system errors, misconfigurations and out-of-date or unpatched software. Due to the rapid rate of digital transformation, these vulnerabilities continue to increase, resulting in a higher frequency of breaches and network downtime, compromising critical operations. According to a report from Radware, an application-distributed denial-of-service (DDoS) attack can cost an organization $6,130 per minute on average.

Last year, a global and comprehensive study conducted by Censuswide on behalf of a leading Out of Band management solutions provider discovered that an overwhelming 97% of surveyed US-based CIOs expressed serious concerns about at least one cybersecurity threat – including malware, spam and phishing, social engineering and insider threats. While these threats aren't particularly new, current cybercity concerns are through the roof among CIOs. The obvious question is: why are CIOs so concerned?

The Cybersecurity Implications of Talent Shortages and Inadequate Network Investment

As business leaders, CIOs must ensure company-wide adherence to security programs that help promote uptime and decrease downtime. Nevertheless, it is challenging to maintain best security practices when there is a lack of experienced network engineers. Technology professionals, like network engineers, are so high in demand they exceed the supply; according to Gartner, almost 86% of CIOs reported facing more competition for qualified candidates. Additionally, network engineers are retiring at a worrying rate. The global study of CIOs found that 86% of US-based CIOs predict that at least 25% of their network engineers will retire in the next five years.

The lack of personnel will likely increase the mismanagement of networks, thereby allowing cybercriminals to exploit vulnerabilities easily, negatively affecting business continuity. In fact, 95% of US CIOs stated that a lack of engineers resulted in a greater inability to manage networks. At the same time, inadequate network investment – such as not implementing proper software and network upgrades – can expose businesses to more cybersecurity threats. That same study, which also surveyed network engineers, revealed that 59% of US-based network engineers felt insufficient investments increased the risk of cyberattacks and/or downtime. Alarmingly, 27% of US network engineers are currently looking to leave their organizations because of inadequate funding.

Understaffed Teams Can Combat Cyberattacks with Out of Band Management

CIOs are rightfully concerned about the cybersecurity implications of talent shortages. However, there are several solutions, like Out of Band management, that CIOs can deploy to help their limited teams more effectively manage business networks. Out of Band management provides a secure connection to IT network environments, enabling engineers to access and manage networks from local and remote sites, even during an outage caused by a cyberattack. In fact, by setting up serial console servers, engineers will have an alternative path via a separate management plane to perform remediation on physical or virtually connected network devices.

Should malware or ransomware cause a breach, engineers can use Out of Band management to isolate the incident by locking down network elements and prohibiting access to impacted equipment through a console port. Likewise, engineers can leverage these network solutions to temporarily disconnect WAN connections and shut down servers to protect private data. Should network assets remain inaccessible, leading Out of Band solutions permit engineers to power off using remote PDU control capabilities and rebuild device configurations via the console port.

Out of Band solutions empower shorthanded network and IT teams to do more with less, helping them not only streamline remediation processes but also optimize everyday management. Specifically, it gives network engineers the visibility to make more informed decisions in real time. Also, best-in-class offerings include automation features, such as automatic configuration and preemptive failover, which help reduce time-consuming processes while preventing downtime for under-pressure engineers. Likewise, some Out of Band solutions will send automated SMS alerts to employees concerning IT infrastructure, ISP or – most importantly – cybersecurity-related incidents.

Why Out of Band is a Necessity and Not a Luxury

The cybersecurity implications of intensifying talent shortages and mass engineer exoduses continue to worry CIOs. Businesses can, however, mitigate these challenges and safeguard their networks by leveraging Out of Band management. Nevertheless, many companies hesitate to invest in such technology as the ongoing economic downturn squeezes budgets. This sentiment assumes incorrectly that Out of Band is a luxury. In reality, it is a necessity. Moreover, the benefits of Out of Band, including improved network reliability and availability, are a small price to pay compared to the consequences of prolonged network downtime.

About the Author

Tracy Collins, VP of Sales, Americas. Tracy has over 25 years of experience in leadership positions in the IT and Infrastructure industry. Prior to joining Opengear, Tracy led the Americas business for EkkoSense, the leading provider of AI/ML software that allows data center operators to operate more efficiently. Prior to joining EkkoSense, Tracy was the CEO of Alabama based Simple Helix, a regional colocation data center operator and MSP. Tracy spent over 21 years with Vertiv, in various leadership positions including leading the global channel organization.

Tracy has an extensive background in sales leadership, and channel development with a strong track record of driving growth while improving profitability. Tracy holds both a Bachelor of Science, Business Administration, and a Master of Science in Management from the University of Alabama – Huntsville.

LinkedIn:

Website https://opengear.com/


EVENTS

BAPCO

The Annual Event

RESERVE A FREE PASS

6-7 MARCH 2024

COVENTRY BUILDING SOCIETY ARENA

THE UK'S LEADING PUBLIC SAFETY EVENT

80+ public safety technology companies

Gain valuable insights from

world-class speakers

3 captivating theatres

NEW product launches

BAPCO-SHOW.CO.UK

@BAPCOEvent BAPCO Annual Event

American Conference Institute

Enhance your understanding on Government/DoD plans and policies to transform intelligence to maintain a global defensive superiority.

Learn about the latest on advancing decision excellence with advanced analytics.

Meet policymakers, subject matter experts, and strategy leaders to inform your policy, transform concepts of operation, and enhance operational effectiveness.

Understand building cyber resilience into data-driven ecosystems to protect sensitive information, to ensure the integrity of critical systems and safeguarding the advantage gained through advanced analytics and AI.

DoD Big Data & Cyber Resilience Summit

March 18–19, 2024 • Washington, DC

To Learn More or Register:

AmericanConference.com/DoD-Big-Data-Cyber-Resilience
1-888-224-2480
LINKEDIN: Defense & Government: U.S. Military/Government Personnel and Defense Industry Professionals

Save 10%
WITH PROMO CODE
D10-999-CDM24

DGI GEOSPATIAL INTELLIGENCE FOR DEFENCE AND SECURITY

20TH ANNIVERSARY

THE WORLD'S LEADING GEOSPATIAL INTELLIGENCE EVENT

USE CODE: CDM10 FOR 10% OFF

Focus Day. 11 March, 2024
Main Event. 12 - 13 March, 2024
The QEII Centre, London

800+ Geospatial Intelligence Professionals to Network With

100+ Geospatial Intelligence Experts Sharing Their Practical Insights

50+ Nations Represented from Around the World

15+ Hours of Invaluable Networking Time

3 DAYS of Insightful Content

In Collaboration With: סייבר ישראל Cyber Israel | Ministry of Foreign Affairs Israel | Ministry of Economy and Industry Foreign Trade Administration | TEL AVIV תל אביב יפו | אוניברסיטת בן-גוריון בנגב جامعة بن غوريون في النقب Ben-Gurion University of the Negev

CYBERTECH GLOBAL TEL AVIV 2024

Join our growing cyber, tech, and innovation community - tens of thousands strong.

April 8-10, 2024 | Expo Tel Aviv

Registration is open: **www.cybertechisrael.com**

E: cyber@cybertechconference.com | **T:** +972-74-7031211 | **W:** www.cybertechconference.com

10TH ANNIVERSARY

IDENTITY MANAGEMENT SYMPOSIUM

ELEVATING NEXT-GEN IDENTITY & ACCESS MANAGEMENT FOR GOVERNMENT

April 10-11, 2024 | NATIONAL HARBOR, MD

CONFIRMED SPEAKERS

LESLIE BEAVERS, SES
PRINCIPAL DEPUTY CIO,
DOD CIO

LEONEL GARCIGA, SES
CIO,
U.S. ARMY

SAM YOUSEF, SES
DIRECTOR,
DEFENSE MANPOWER
DATA CENTER

FREE FOR ACTIVE DUTY MIL/GOV

IDENTITYMANAGEMENT.DSIGROUP.ORG

CALL & CONTACT CENTER EXPO

APRIL 24 - 25 2024

LAS VEGAS CONVENTION CENTER

SHOW SPONSOR | smile.cx AI powered by HUMANS

THE LEADING EVENT FOR CONTACT CENTER PROFESSIONALS TO ENHANCE CUSTOMER ENGAGEMENT

@CallContactUS #CCCLV24

ANSWER THE CALL TO INNOVATION & SUCCESS THROUGH:

60 HOURS OF CONTENT

UNMISSABLE SPEAKER LINE-UP

INNOVATION AWARDS

+ MUCH MORE!

SECTORS SUCH AS:

- HEALTHCARE
- FINTECH
- RETAIL
- FUTURE TECH
- HOSPITALITY

& MORE

CC CONNECT NETWORKING HUB

TICKETS

callandcontactexpo.us

HOSTED BY
مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

OFFICIAL GOVERNMENT CYBERSECURITY PARTNER
مركز دبي للأمن الإلكتروني
DUBAI ELECTRONIC SECURITY CENTER

OFFICIALLY SUPPORTED BY
وزارة الداخلية
MINISTRY OF INTERIOR
شرطة دبي
DUBAI POLICE
TDRA
هيئة تنظيم الاتصالات والحكومة الرقمية
TELECOMMUNICATIONS AND DIGITAL GOVERNMENT REGULATORY AUTHORITY

ORGANISED BY
مركز دبي التجاري العالمي
DUBAI WORLD TRADE CENTRE

PRIVACY-ENHANCING TECHNOLOGY SUMMIT NORTH AMERICA

MAY 7, 2024 | NEW YORK

SECURELY UNLOCKING THE TRUE VALUE OF DATA

Register Today & Quote CYBERDEFENSEMAGAZINE10 to save 10%

UNDER THE PATRONAGE OF

H.E. MR. AHMAD AL HANANDEH

MINISTER OF DIGITAL ECONOMY AND ENTREPRENEURSHIP

4TH DIGITAL TRANSFORMATION JORDAN

BUILDING DIGITAL ECOSYSTEMS THROUGH COLLABORATION, CONNECTIVITY AND CONVERGENCE FOR BETTER EXPERIENCES AND ENGAGEMENTS

8 – 9 MAY 2024

ST. REGIS - AMMAN, JORDAN

ENDORSED BY

Ministry of Digital Economy and Entrepreneurship

ORGANIZED BY:

GM EVENTS

WWW.DIGITALTRANSFORMATIONJORDAN.COM

Strategic Partner

شرطة أبوظبي
ABU DHABI POLICE

Organised by

ADNEC GROUP
مجموعة أدنيك

In association with

وزارة الداخلية
MINISTRY OF INTERIOR

Register for your FREE pass

www.emergencytechshow.com

ITS World Congress | 16-20 September 2024 | Dubai World Trade Centre

DUBAI
ITS World Congress
16 -20 September 2024
Mobility Driven by ITS

Join us in Dubai to shape the future of ITS and Smart Mobility at the 30th ITS World Congress

Be part of #ITSDubai2024: itsworldcongress.com

ORGANISED BY ERTICO ITS EUROPE

CO-ORGANISED BY ITS AMERICA, ITS ASIA-PACIFIC

HOSTED BY RTA

SUPPORTED BY DUBAI, DXB, Best Cities Global Alliance

YOUR CONTRIBUTION TO THE TECHNICAL PROGRAMME

DUBAI
ITS World Congress
16 -20 September 2024
Mobility Driven by ITS

The submission portal stays open until 15 January 2024.

ITS World Congress | 16-20 September 2024 | Dubai World Trade Centre

The response to our call for contributions has been nothing short of inspiring. Thank you for your ongoing enthusiasm and dedication to making the Congress a resounding success.

More info: itscongress.com/technical-programme

ORGANISED BY ERTICO ITS EUROPE

CO-ORGANISED BY ITS AMERICA, ITS ASIA-PACIFIC

HOSTED BY RTA

SUPPORTED BY DUBAI, DXB, BestCities GLOBAL ALLIANCE

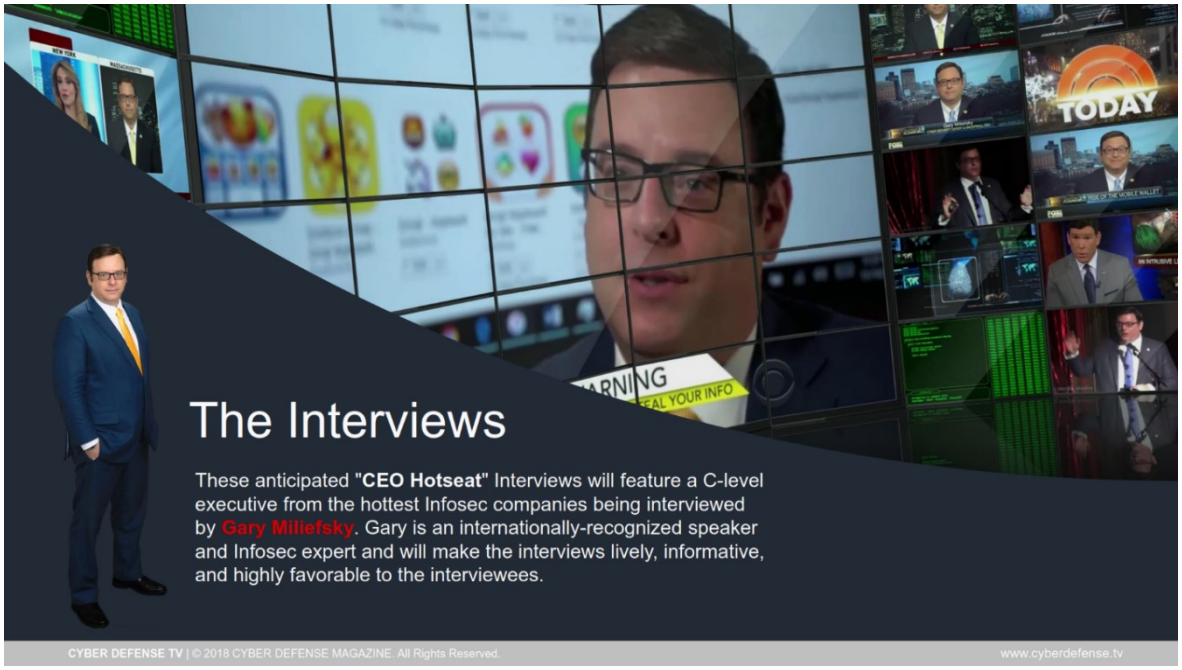
CYBER DEFENSE TV

INFOSEC KNOWLEDGE IS POWER

CyberDefense.TV now has 200 hotseat interviews and growing…

Market leaders, innovators, CEO hot seat interviews and much more.

A division of Cyber Defense Media Group and sister to Cyber Defense Magazine.



Free Monthly Cyber Defense eMagazine Via Email

Enjoy our monthly electronic editions of our Magazines for FREE.

This magazine is by and for ethical information security professionals with a twist on innovative consumer products and privacy issues on top of best practices for IT security and Regulatory Compliance. Our mission is to share cutting edge knowledge, real world stories and independent lab reviews on the best ideas, products and services in the information technology industry. Our monthly Cyber Defense e-Magazines will also keep you up to speed on what's happening in the cyber-crime and cyber warfare arena plus we'll inform you as next generation and innovative technology vendors have news worthy of sharing with you – so enjoy. You get all of this for FREE, always, for our electronic editions. Click here to sign up today and within moments, you'll receive your first email from us with an archive of our newsletters along with this month's newsletter.

By signing up, you'll always be in the loop with CDM.

Cyber Defense Magazine

276 Fifth Avenue, Suite 704, New York, NY 1000

EIN: 454-18-8465, DUNS# 078358935.

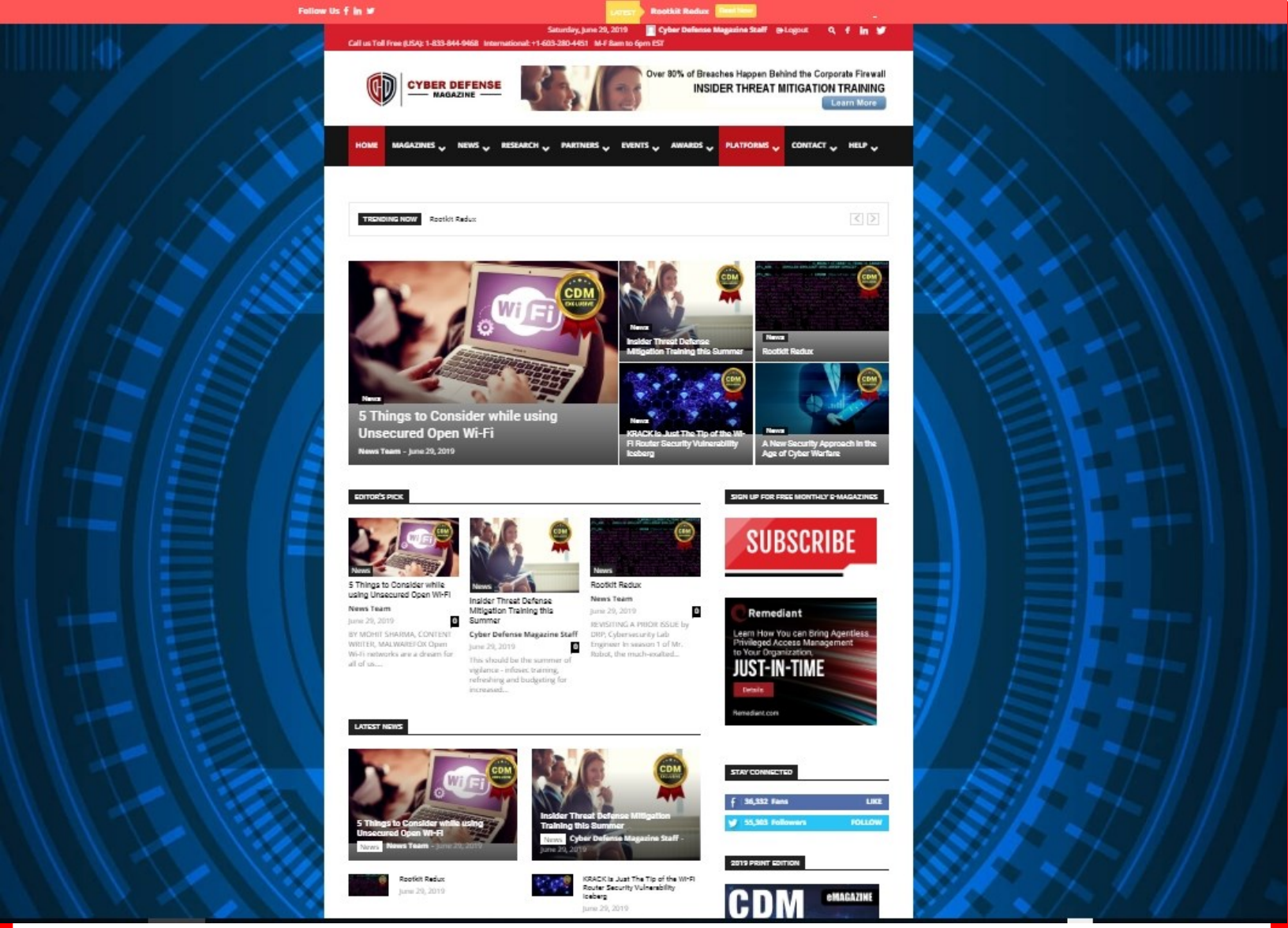
All rights reserved worldwide.

marketing@cyberdefensemagazine.com

www.cyberdefensemagazine.com

NEW YORK (US HQ), LONDON (UK/EU), HONG KONG (ASIA)

Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 03/04/2024



Books by our Publisher: [Amazon.com: CRYPTOCONOMY®, 2nd Edition: Bitcoins, Blockchains & Bad Guys eBook : Miliefsky, Gary: Kindle Store (with others coming soon...)]

12 Years in The Making…

Thank You to our Loyal Subscribers!

We've Completely Rebuilt CyberDefenseMagazine.com - Please Let Us Know What You Think. It's mobile and tablet friendly and superfast. We hope you like it. In addition, we're past the five nines of 7x24x365 uptime as we continue to scale with improved Web App Firewalls, Content Deliver Networks (CDNs) around the Globe, Faster and More Secure DNS and CyberDefenseMagazine.com up and running as an array of live mirror sites. We successfully launched https://cyberdefenseconferences.com/ and our new platform https://cyberdefensewire.com/

CYBER DEFENSE MAGAZINE

WHERE INFOSEC KNOWLEDGE IS POWER

www.cyberdefensewire.com
www.cyberdefensetv.com
www.cyberdefenseradio.com
www.cyberdefenseawards.com
www.cyberdefenseconferences.com
www.cyberdefensemagazine.com

RSAConference™2024

San Francisco | May 6 – 9 | Moscone Center

LEARNING. NETWORKING. INNOVATION.

THE TRIPLE THREAT FOR CYBERSECURITY SUCCESS.

RSA Conference 2024 will bring the cybersecurity community together again in San Francisco for four industry-shaping days, and you can be a part of that important conversation.

From May 6 – 9, you'll be able to:

- See what the future holds with the hottest industry topics and emerging trends
- Expand your knowledge and be inspired by forward-thinking Keynotes
- Demo the latest products to find real-world solutions from over 600 companies
- Enhance your career through valuable networking opportunities

Let's redefine The Art of Possible by shaping solutions, tackling challenges, and encouraging the collective strength of coming together as a community.

Act now for the biggest discount!

Visit www.rsaconference.com/cyberdefense24 to learn more and register.

#RSAC

FOLLOW US

THE ART OF POSSIBLE

*** with help from writers and friends all over the Globe.**