CYBER DEFENSE MAGAZINE

eMAGAZINE

AUGUST 2023

In This Edition

Implementing a Modern, Holistic Approach to Tech Sector Security

Transformative Benefits of ML&AI in Cybersecurity

Policy: The Silent Sentinel of Your Cybersecurity Defenses

…and much more…

MORE INSIDE!

`

CONTENTS

@MILIEFSKY

From the

Publisher…

TOP INFOSEC INNOVATOR
CYBER DEFENSE MAGAZINE
2023

Dear Friends,

From the publisher’s desk, we continue to see developments involving both developers and regulators, in private and government sectors, reflecting the needs of our professionals in understanding how these rapid changes will benefit or harm all of us.

On July 26th, 2023, the SEC voted 3-2 to adopt new rules on cybersecurity disclosures. These rules are designed to help investors make informed investment decisions by providing them with more information about the cybersecurity risks facing public companies. These rules also aim to encourage public companies to take steps to improve their cybersecurity posture.

There is no shortage of concerns voiced by practitioners in nearly all types of cyber security endeavors. Artificial intelligence continues to be the wild card, and its potential effect on almost every sector has heightened the level of discussion and possible means of dealing with AI as both a threat and an opportunity.

We believe that the role of the CISO and related professionals will provide the most effective and efficient way to optimize the future integration of AI into our economy and society. This holds true across the board, recognizing the rapid development of applications based on artificial intelligence, such as privacy, identity theft and fraud, and consumer protections. We honor those CISOs and a select group of Top InfoSec Innovators from our 11th Annual Awards program at https://www.cisoconference.com.

As always, it’s important for us to be mindful of the mission and contribution we have undertaken, to provide the most professional and up-to-date forum for keeping our readers informed of challenges and responses in today’s cyber world. With the support of our contributors and readers, we continue to pursue our role as the premier publication in cybersecurity.

Warmest regards,

Gary S. Miliefsky

Gary S.Miliefsky, CISSP®, fmDHS
CEO, Cyber Defense Media Group
Publisher, Cyber Defense Magazine

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

1717 Pennsylvania Avenue NW, Suite 1025
Washington, D.C. 20006 USA
EIN: 454-18-8465, DUNS# 078358935.

PUBLISHER
Gary S. Miliefsky, CISSP®

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

11 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 VENTURES WEBINARS
CYBERDEFENSECONFERENCES

Welcome to CDM's August 2023 Issue

From the Editor-in-Chief

Both the scope and depth of our CDM articles this month continue to accelerate in response to the interests and needs of our readers and contributors. We count Cyber Defense Media Group and the eMagazine fortunate to rely on both our contributing authors and our growing group of readers.

As we experience a period of rapid growth in the cyber security industry, we observe a divergence between regulatory developments and private rights of action, many of which come into play as artificial intelligence continues to grow and spread through many areas of endeavor. We mention this because it appears that compliance with regulatory requirements cannot be relied upon to provide a bullet-proof defense against claims arising out of cyber security failures.

The spread of cyber threats and responses continues unabated in the world of cybersecurity professionals. While we must address the future of AI, there is no room for anyone to become complacent in assuring that all the everyday measures are completed to prevent cyber breaches.

As always, we are delighted to receive both solicited and unsolicited proposals for articles. Please remember to submit all articles on the Cyber Defense Magazine writer's kit template, which incorporates the major terms and conditions of publication. We make every effort to close out acceptance of articles by the 15th of each month for publication in the following month's edition.

Wishing you all success in your cybersecurity endeavors,

Yan Ross

Yan Ross
Editor-in-Chief
Cyber Defense Magazine

About the US Editor-in-Chief

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

SPONSORS

unknown
CYBER

2001 2023

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	cyberGRX	DRAGOS	CONCEAL	varmour

ALLEGISCYBER
CAPITAL

www.allegiscyber.com

ARTICLES

Implementing a Modern, Holistic Approach to Tech Sector Security

By Sean Malone, Chief Information Security Officer, Demandbase

Technology has given rise to many comparisons in the past few years, but the train comparison is one of my favorites. In this analogy, the tech sector is like a fast-moving train that constantly gathers speed, bringing new opportunities and challenges along the way. One of the challenges it brings is the ever-increasing danger posed by cyber threats, requiring a modern approach that goes beyond traditional security practices.

Robust security measures are a vital factor in this rapidly evolving landscape. To effectively safeguard your organization, a unified strategy that brings together IT, Enterprise Security, and Product Security under the guidance of a Chief Information Security Officer (CISO) is critical. Here's how to implement this approach, the challenges involved, and how to structure your teams for optimal results.

Creating a Unified Voice for Security

In the traditional business model, IT and Security often operate in silos, with separate reporting structures and objectives. However, a modern approach could involve a paradigm shift by having both functions report to the CISO. The key to making this work lies in how the CISO perceives their role. Instead of viewing themselves solely as security professionals operating at the executive level, they must embrace the mindset of a business executive focused on enabling the business to achieve its core objectives without taking on unnecessary risk.

This change in perspective enables the CISO to advocate for security from a unified standpoint. By bridging the gap between IT, Engineering, and Security, the CISO can promote a culture of quality throughout your organization, ensuring security considerations are integrated across corporate processes and in every stage of the product development lifecycle. This strategy helps encourage better collaboration between teams, reduces redundancies and associated costs, and enhances your company's overall security effectiveness.

Overcoming Challenges with Relationships

While the benefits of unifying IT and Security under the CISO are clear, challenges can arise when an organization attempts to bring diverse teams together. Resistance to change, hesitation, and the need to incorporate external talent can all pose difficulties. Clearing the runway of these organizational hurdles requires a strategic—and empathetic—approach.

Building relationships is vital. Fundamental steps that need to be taken include:

- Encouraging open communication channels and fostering a culture of trust to overcome resistance and hesitation
- Establishing forums for cross-functional collaboration, such as regular meetings and joint projects, to help create shared goals and build stronger relationships between teams

It is crucial to emphasize that the goal is not to undermine existing roles but rather to leverage the collective expertise to enhance the company's security.

Additionally, you must strike a careful balance when integrating external talent. While fresh perspectives and specialized skills can bring immense value–and are frequently a necessary component of organizational transformation–you must be able to integrate these seamlessly into the existing team structure. Your organization can create an inclusive culture that values diverse contributions by providing mentorship, clearly defining roles and responsibilities, and actively promoting a growth-oriented environment.

Structuring Teams for Optimal Results

Once IT and Security are united under a CISO's leadership, it's essential to structure your teams in a way that maximizes their potential. Crucial aspects of this process include adjusting role definitions and creating growth opportunities.

For example, revisiting role definitions is necessary to ensure that your people are assigned to the right roles based on their skill sets and expertise. Redefine your job descriptions to achieve alignment, emphasizing the importance of security skills and fostering cross-functional training. Develop clear career paths for employees to nurture talent, retain top performers, and enable continuous development.

Create growth opportunities to maintain team motivation and engagement. You can achieve this by establishing learning programs, offering certifications, and providing avenues for professional advancement within the security domain. Recognizing and rewarding accomplishments, both individually and as a team, further encourages a strong commitment to security excellence. Your objective should be to maximize the amount of time that employees spend working at the intersection of expertise, passion, and company needs.

Implementing a Holistic Approach Under a Single Umbrella Strategy

A modern approach to tech sector security requires a holistic approach that unifies your IT, Enterprise Security, and Product Security under a single overarching strategy. Overcoming challenges and breaking down silos through relationship-building and trust-building efforts are essential for success. Additionally, structuring teams with the right people in the right roles, coupled with growth opportunities, ensures the continuous evolution of a robust security program that can effectively safeguard against emerging threats in the dynamic tech landscape.

By redefining the role of the CISO as a business executive focusing on security, your organization can achieve a cohesive voice advocating for comprehensive security initiatives across the board.

About the Author

Sean Malone is the Chief Information Security Officer at Demandbase. In his role, he is responsible for the information security and IT functions. Prior to joining Demandbase, Malone led information security, delivery, product, and R&D for VisibleRisk, which was acquired by BitSight Technologies. Prior to that, he was Head of Cyber Defense for Amazon Prime Video, and previously spent ten years in offensive information security, performing red team engagements and cyber defense consulting for major financial institutions, casinos, gold mines, social media platforms, and similar high-value targets. Malone holds an MS in Information Security & Assurance, as well as the CISSP, CISM, CISA, CCISO, AWS Solutions Architect, and AWS Security Specialty certifications. He's active in the security community, including presenting research at Black Hat, DEF CON, and other conferences. He has a patent pending for his work on assessing security programs and quantifying cyber risk.

Sean can be reached online at https://www.linkedin.com/in/seantmalone/ and at our company website https://www.demandbase.com/.

Transformative Benefits of ML&AI in Cybersecurity

By Gizem Yılmaz, Product Owner, Nextray AI

In the modern digital era, the significance of cyber security has escalated. With the growing dependence of businesses and organizations on technology, their susceptibility to cyber attacks has also risen. Due to the ever-evolving nature of cyber attacks, it is practically impossible for an individual to manually detect and mitigate all the threats faced by a company. Hackers continuously devise new attack methods with specific objectives in mind. To counter these threats, cyber security experts must constantly adjust their strategies. Take the case of log4j, for instance, which went unnoticed for a long time before resurfacing in December 2021. Introducing such unknown threats into a network can result in significant damage, potentially impacting the organization in profound ways if not promptly detected, identified and prevented. Artificial intelligence (AI) has emerged as a valuable tool in this realm, offering promising solutions. Let's delve into the exciting realm of ML-powered NDR and discover the transformative impact it has on safeguarding networks against evolving cyber threats.

Increased efficiency with the analysis of large volumes of security data

In the realm of cybersecurity, the volume and complexity of security data continue to grow exponentially. Analyzing large volumes of data in cybersecurity for threat detection is challenging due to the need for real-time analysis, handling diverse data sources and formats, identifying subtle patterns or indicators of threats amidst noise, and ensuring the accuracy and reliability of the detection algorithms to minimize false positives and negatives. Machine learning (ML) brings efficiency to analyzing large volumes of data in cybersecurity for threat detection by leveraging its ability to process data at scale, detect complex patterns and anomalies, identify previously unknown threats, and automate the analysis process. ML algorithms can quickly analyze vast amounts of data, allowing for real-time threat detection, reducing response times, and improving the accuracy of threat identification. ML's efficiency in handling large data volumes enables security teams to effectively detect and respond to threats, minimizing the risk of potential damages and enhancing overall cybersecurity posture.

Improved accuracy with ability to continuously learn and adapt

The accuracy of AI in cybersecurity is strengthened because it can constantly learn and adjust. By training machine learning algorithms on extensive datasets that cover a wide range of threat scenarios and behaviors, they become better at detecting threats as time goes on. As AI algorithms acquire new data, they can fine-tune their models and detect emerging threat patterns more accurately. This adaptable characteristic of AI enables organizations to proactively address evolving cyber threats and significantly improves the precision of their cybersecurity defenses.

Empowering security with unveiling Unknown Threats

AI's advanced algorithms and capabilities enable the unveiling of hidden dangers, empowering security teams to stay one step ahead of cybercriminals. Artificial Intelligence (AI) is instrumental in detecting unknown threats in cybersecurity, filling the gap left by traditional signature-based methods that focus on known threats. With cybercriminals continuously evolving their attack techniques, the ability to identify and respond to unknown or zero-day threats is paramount. AI empowers security systems to employ advanced techniques like behavioral analysis, anomaly detection, and predictive analytics, enabling the detection of abnormal patterns and suspicious activities. This proactive approach enables the identification of potential threats that could bypass traditional methods relying solely on known signatures.

In summary, the advancements of ML in network detection and response revolutionize cybersecurity by offering increased efficiency in data analysis, improved accuracy through continuous learning, and the ability to unveil unknown threats. By harnessing the power of AI, organizations can strengthen their cybersecurity defenses, stay one step ahead of cybercriminals, and safeguard their networks against the ever-evolving landscape of cyber threats.

About the Author

Gizem Yılmaz is the Product Owner of the Nextray AI. Gizem Yılmaz stands out as an experienced Data Analyst and Product Owner. She focuses on value maximization, works on the discovery of features to add to the product, and manages the priorities of ongoing work. She is a professional specialized in data analysis and a person who provides significant added value to the product development process. With its data analysis skills and strategic thinking abilities, she supports the decision-making processes of the business and the product development process. Gizem also provides effective communication between teams and collaborates to ensure that projects are completed on time and successfully. With its professional experience and leadership competencies, it makes a valuable contribution to the achievement of the global goals of the enterprise.

See more information about Gizem at https://www.linkedin.com/in/gizem-yilmaz/.

Policy: The Silent Sentinel of Your Cybersecurity Defenses

By Craig Burland, CISO, Inversion6

Planning your next move to reinforce the organization’s cyber security posture? Take a moment to look away from that shiny new tool and cutting-edge technology. As impressive as “it” – XDR, AI-powered detections, orchestration -- may be, technology is not the be-all and end-all of your organization's defense. Implementing a collection of best-in-class tools may appease the board but won’t guarantee an incident-free year. Regardless of the mix of your cyber security controls, technology alone can't overcome poor decision-making, rectify deep-seated ignorance of cyber security or transform your users into cyber security mavens. Unsettling? Indeed. Unexpected? Not at all.

The reality is that the core of your cyber security posture isn't simply technological, but rather an often understated and overlooked factor: policy. An organization without policies is analogous to the American wild west of the late 19^{th} century. Laws existed but few knew them; enforcement varies wildly from town to town and situation to situation.

Policies help bring order to the chaos of a highly decentralized system by informing decision makers. Savvy organizations grasp this reality and approach the cyber security landscape with a clear perspective. They recognize that crafting comprehensive policies is a strategic investment, not a bureaucratic necessity.

As a cyber security leader, now is the perfect time to champion policies. While CEOs and CFOs fret about a recession, make policymaking your key investment for 2023. Embrace principles like "a security-centric culture" and "proactive, people-focused governance" to develop defenses that prove more robust, adaptable and cost-effective than those solely reliant on technology.

The Indispensable Role of Policies

Well-written policies represent more than a series of dos and don'ts. They serve as a roadmap, guiding your organization through the complex terrain of cyber security. They document the organization's regulatory requirements and aspirational cyber security posture. They establish norms and expectations, delineating the route for everyone to follow. Contrary to common practice, policies should be the foundation of the cyber security strategy. Whether it's enforcing multi-factor authentication, handling confidential data or adhering to incident response protocols, policies provide clarity, direction and justification.

A Guiding Force in Decision-Making

The "people, process, technology" triad is a foundational concept in cyber security. Despite having top-notch tech and processes in place, the "people" component can potentially weaken your defense. But with sound policies in place, you can transform this potential vulnerability into a strength. Policies guide individuals towards sound decision-making, fostering a culture where everyone plays a part in strengthening the defenses. They are your dependable guide in handling complex cyber security situations, offering a set of principles to help users navigate this intricate domain. Policies ensure that each decision contributes positively to your organization's defense, rather than compromising it.

Policies at the Center of Awareness

Beyond setting direction, policies serve as educational tools. Thoughtfully designed policies promote good practices and underscore the importance of compliance. Not every team member needs to be a cyber security specialist. But leaving them uninformed is a serious mistake. Once written, policies must be shared broadly and consistently. They should be the cornerstone of your awareness campaigns with constant cross-references and reinforcement. Consider a DevOps team working at high speed to deliver new functionality. An awareness of the solution development lifecycle policy may make the difference between a developer opening an unprotected cloud workload to the internet and making a smarter choice.

Leadership and Policy Implementation

Leadership's role in policy implementation is often underestimated. Management sets the tone for policy adherence, creating an environment of compliance and respect for cybersecurity rules. Leaders must not only follow these rules but hold regular discussions about security, address breaches promptly, reward compliance and encourage continual learning. Moreover, leaders should ensure that policies keep pace with the rapidly evolving cyber security landscape. This involves regular reviews and updates, reflecting the latest threats and best practices.

Technology Follows Policy

Teams all too often let technology dictate their strategy, essentially outsourcing their thinking to the vendor's protect managers. Why turn on MFA? The wrong answer is because your provider suddenly offers it. The right answer is because your policy requires it, stemming from an analysis of the regulatory environment and your threat profile. Monitoring, encryption and patching all follow a similar path. Technology should serve to enable and enforce policy rather than drive it. Post-implementation, analytics tools can monitor compliance trends and exceptions, indicating the need for additional training or stronger controls.

The Unseen Champion: Policies

In conclusion, good cyber security isn't only about state-of-the-art technology. It's centered on people – their understanding, their decisions and their actions. Guiding all these elements are your policies: the unseen champion of your cybersecurity defenses. More than a list of rules, they shape behavior, inform decisions and fortify defenses. In this evolving digital era, people are a constant. As you sit through a demo of the newest cyber security gadget, remember the silent sentinel – policies – and make the smarter investment.

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 Globhttp://www.inversion6.comal Security, and Oracle Web Center. Craig can be reached online at LinkedIn and at our company website http://www.inversion6.com.

Bot Security: The Hunt for Vulnerabilities in The Digital Realm and The Burgeoning Need to Safeguard Users, Businesses, And Global Economies

By Mohit Shrivastava, ICT Chief Analyst, Future Market Insights

Bots have incorporated themselves into our online experiences in the ever-expanding digital world. Bots have altered the way we engage with technology, from customer service and virtual assistants to automated operations. Our way of living and working has undergone a profound transformation due to the emergence of intelligent bots with abilities powered by machine learning and artificial intelligence. These bots can comprehend real language, assess emotions, and respond based on context, offering personalized experiences that were earlier unimaginable.

The usage of bots is growing, but with it emerge new difficulties, notably in the domain of security. In order to maintain the integrity and safety of our digital environment, bot security is essential.

According to Future Market Insights (FMI), a leading market research firm, the global bot security market size is predicted to surpass US$ 666.7 million in 2023. It is projected to attain a valuation of US$ 3,624.5 million by 2033, clocking a CAGR of 18.3% from 2023 to 2033.

In this article, we will delve into the evolution of the bot security market and the intelligent bot revolution that has changed how we live and work while examining the effects of bot security on users, businesses, and the global economy.

The Early Evolution Days: Protecting Simple Bots

Security in the early days of bots was largely concerned with defending against typical risks like spam, phishing, and automated assaults. To recognize and stop criminal activity, organizations have established security procedures, including CAPTCHA tests, authentication systems, and behavior tracking. These steps lay the groundwork for fundamental bot security, guaranteeing a certain level of security for customers and companies.

Fast Forward to the Rise of Advanced Attacks

As bots developed in sophistication and their ability to imitate human behavior increased, fraudsters became acquainted with fabricating complex assaults that were aimed exclusively at bots. They are implementing cutting-edge strategies like botnets, exploiting loopholes in bot frameworks, and using artificial intelligence to avoid detection. In order to protect against these changing dangers, organizations had to face new difficulties, which called for the development of bot security methods.

The Imperative of Bot Security for Customer Confidentiality and Data Protection

For customer confidentiality and sensitive data to be safeguarded, bot security is essential. As bots get more sophisticated, malicious hackers can take advantage of pitfalls to obtain unauthorized access or steal personal information. Users may enjoy a safer online environment and feel comfortable in their interactions with bots by establishing formidable bot security measures in place. Bot security also aids in reducing the dangers of phishing, spam, and social engineering assaults, giving consumers piece of mind while fostering confidence in online interactions.

The Vital Role of Bot Security for Safeguarding Trust and Reputation Among Businesses

Bot security is crucial for organizations to preserve consumer and brand confidence. Serious repercussions may result from a security breach or compromise, including monetary loss, company reputation harm, and significant legal obligations. Businesses may defend their data, safeguard their intellectual property, and guarantee the continuity of their operations by prioritizing bot security. Strong bot security measures may also shield organizations from financial losses and maintain their standing in the marketplace by preventing fraudulent behaviors like account takeovers and phony transactions.

The launch of HUMAN Bot Insights ServicesTM was announced in February 2022 by HUMAN Security, Inc.® (formerly White Ops), the industry pioneer in protecting businesses and internet platforms from sophisticated bot attacks and fraud. This service will assist customers of BotGuard for Applications in taking preventative action against sophisticated bots. Such developments are expected to uptick bot security in the coming years.

Embracing the Bot Revolution for Global Economic Resilience in the Digital Era

The rise of intelligent bots has had a significant effect on the world economy. Across sectors, bots have boosted productivity, simplified procedures, and improved consumer experiences. However, economies are susceptible to serious disruptions without adequate bot security. Malicious bot incidents, including distributed denial-of-service (DDoS) assaults or data breaches, can destroy vital infrastructure, mess up supply chains, and result in significant financial losses. By investing in bot security, governments and companies may safeguard their financial interests, advance stability, and encourage sustainable growth in the digital age.

The Way for Businesses to Ensure the Integrity of Their Bot-driven Operations

- **Considering Ethics to Promote Responsible Bot Use**

As the usage of intelligent bots increased, ethical questions about them began to surface. Deepfake bots, automated misinformation, and privacy issues all garnered attention. The ethical usage of bots is now included in the scope of bot security, which now goes beyond conventional threat mitigation. To uphold trust and ethical standards, businesses and developers must prioritize responsible bot formation, respect for privacy laws, and candidness in bot interactions.

- **Cooperation and Threat Intelligence**

Organizations started cooperating and exchanging threat intelligence as they became aware of the interrelated nature of bot security. The overall defense against bot assaults has been reinforced by pooling resources and exchanging knowledge about new dangers, attack methods, and detection tools. This cooperative strategy has produced more thorough security plans and quicker reaction times to reduce the hazards associated with bots. Cooperation and threat intelligence can pave the way for staying ahead of sneaky bots.

Current Trends in Bot Security: Businesses Ravel the Power of Protection

- **Advances in Bot Security**

Bot security solutions combine biometric authentication approaches to counter the dangers posed by conventional authentication procedures. By reducing the possibility of unwanted access and averting bot-driven assaults, facial recognition, voice authentication, and fingerprint scanning provide extremely secure methods of confirming user identification.

- **Developments in Natural Language Processing (NLP)**

NLP developments are essential for improving the security of chatty, interactive bots. Sophisticated NLP algorithms examine language patterns and semantic interpretations to find potentially damaging information or suspicious intent. Organizations may recognize and reduce risks related to social engineering attacks and harmful interactions by utilizing NLP skills.

- **Real-Time Threat Hunting**

In the bot security market, real-time threat-hunting solutions are gaining popularity. These cutting-edge systems use big data analytics and machine learning algorithms to continually monitor network traffic. Organizations may improve their security posture by proactively neutralizing new bot risks by spotting and analyzing unusual activity in real time.

Strategies to Gain Advanced Bot Security

- Comprehensive Bot Governance: Develop a framework for comprehensive bot governance that covers the creation, deployment, monitoring, and retirement phases of bot lifecycle management. To guarantee standardized and safe bot operations, this framework should include security rules, standards, and processes.
- Bot Identity and Access Management: Set up reliable authentication and authorization procedures for bots to guarantee that only authorized bots may access critical systems and data. Secure API keys, digital certificates, or token-based authentication can be used in this.
- Monitoring based on behavior: Use monitoring to find unusual bot activity. Organizations can spot potentially harmful bots and respond appropriately in real time by setting baseline behavior and regularly monitoring for variations.
- Bot Behavior Analysis: To distinguish between trustworthy and malicious bots, use cutting-edge techniques like bot behavior analysis. Response timings, session patterns, and interaction behavior analysis can be used to spot suspicious activity and reduce risks.
- Automation in security: Use automation to speed up security procedures and reaction times. Automated systems may swiftly identify and counter bot attacks, speeding up reaction times and lessening the effect of security problems.
- Continuous Security Education and Training: Encourage a culture of security awareness by giving employees and developers access to continued security education and training. This guarantees that everyone is aware of the dangers posed by bots and follows security best practices while developing and deploying bots.

The Future Will Constantly Require Adaptation and Cutting-Edge Methods

The development of bot security is a continuous process. Attacks will get more sophisticated as bot capabilities develop further. The use of cutting-edge methods and ongoing modifications are key to future bots' security. To keep ahead of new threats and ensure the resilience of bot-driven ecosystems, predictive analytics, anomaly detection, and real-time threat intelligence will be essential.

Conclusion: Evolution of Dynamic Bot Security Landscape for a Secure Future

Bot security has evolved due to the necessity to defend against sophisticated assaults, assure responsible bot usage, and address ethical issues. The evolution of bot security, in tandem with remarkable technological advancements, can pave the way for a more secure future. Organizations must maintain vigilance, adopt cutting-edge security measures, and promote cooperation as the bot landscape changes in order to safeguard the intelligent bot revolution and enjoy its full advantages. We can create a world where savvy bots and strong security coexist peacefully by doing this.

About the Author

Mohit Shrivastava, Chief Analyst ICT at Future Market Insights. Mohit Shrivastava has more than 10 years of experience in market research and intelligence in developing and delivering more than 100+ Syndicate and consulting engagements across ICT, Electronics, and Semiconductor industries. His core expertise is in consulting engagements and custom projects, especially in the domains of Cybersecurity, Big Data & Analytics, Artificial Intelligence, and Cloud. He is an avid business data analyst with a keen eye on business modeling and helping in intelligence-driven decision-making for clients.

Mohit holds an MBA in Marketing and Finance. He is also a Graduate in Engineering in Electronics & Communication.

https://www.linkedin.com/in/shrivastavamohit/

Future Market Insights (FMI), is an ESOMAR-certified market research and consulting market research company. FMI is a leading provider of market intelligence and consulting services, serving clients in over 150 countries; its market research reports and industry analysis help businesses navigate challenges and make critical decisions with confidence and clarity amidst breakneck competition. Now avail flexible Research Subscriptions, and access Research multi-format through downloadable databooks, infographics, charts, and interactive playbook for data visualization and full reports through MarketNgage, the unified market intelligence engine powered by Future Market Insights. Sign Up for a 7-day free trial!

Our company website https://www.futuremarketinsights.com/

Achieving Optimal Zero Trust Maturity: The Role of Data and Governance

By Carolyn Duby, Chief Technology Officer, Cloudera Government Solutions

The federal government has placed a stronger emphasis on zero trust since OMB's federal zero trust strategy memo from the beginning of 2022, requiring agencies to have a security model in place that assumes every device, application, or user attempting to access a network cannot be trusted.

Most recently, the Cybersecurity and Infrastructure Security Agency (CISA) issued a second version of its Zero Trust Maturity Model (ZTMM 2.0), which provides a roadmap to guide agencies to a zero trust model by 2024. The ZTMM is a combination of five pillars: identity, devices, networks, applications and workloads, and data. It also addresses four levels of maturity, providing useful information for agencies regardless of their location on the zero trust journey (traditional, initial, advanced, optimal).

With the impending deadline, the Department of Defense is feeling the pressure and making strides toward implementing the ZTMM to reach the "optimal" stage of maturity. DOD's approach to a zero trust strategy will equip the Department with the guidelines to instill the "never trust, always verify" mindset, along with a map of how to implement the zero trust strategy across all components of the agency, including capabilities, technologies, solutions, and processes.

While making this progress, agencies must understand the impact a successful zero trust process can have on data and the future of government decision-making. There are also key strategies and data governance policies that agencies can implement to abide by the CISA guidelines and find achievable solutions for a zero trust future.

How Agencies Can Safeguard Their Data

The updated ZTMM from CISA claims that agency data should be protected on devices, in applications, and on networks in accordance with federal requirements, and that agencies should inventory, categorize, and label data; protect data at rest and in transit; and deploy mechanisms to detect and stop data exfiltration.

Zero trust is all about enhancing your security posture. The balancing act of security and accessibility is possible through platforms that can operate independently from compute and storage layers which offer integrated security and governance based on metadata. The ideal zero trust approach will contain a data security platform capable of contextualizing across analytics and cloud environments while simplifying data delivery and access with a unified multi-tenant model.

Ultimately, the approach of utilizing a secure platform to assist with zero trust will result in reduced cybersecurity risk and operational costs, all while allowing faster deployment of governed and secured data lakes for broader responsibly safeguarded data access.

Role of Data in the Zero Trust Journey

With data as one of the five main pillars of the ZTMM, it is critical that DOD moves to optimal maturity to properly secure our nation's data and privacy. The DOD has already shared various plans and guidelines that focus heavily on data protection and management, so movement to an optimal zero trust position greatly aligns.

Therefore, implementing the ZTMM will eliminate unauthorized access by bad actors and safeguard data from non-trusted sources. This is essential as data continues to play a key role in the federal government's mission-critical operations. The optimal maturity of zero trust will better position defense agencies to protect their essential data, ranging from citizen services to military intelligence; all government data will be protected and safeguarded.

Proper Governance Supports the Trek to Optimal

Governance is a need as CISA also stated that agencies should carefully craft and review data governance policies to ensure all data lifecycle security aspects are appropriately enforced across the enterprise. When you have proper governance with zero trust, it frees up the data so you can share it effectively within the organization. The data is protected and highly accessible by the team members who need it most.

Adhering to the guiding principles of a zero trust architecture requires a multifaceted approach.

First, verification using multi-factor authentication everywhere provides a normalized SSO token for the representation of the authenticated user. Using least privileged access will allow agencies to incrementally grant access on an as-needed basis.

Next, in order to minimize the blast radius of a breach through segmented data access, the ideal support platform will be given access to the appropriate zone key to decrypt the underlying data. This combined with complete auditing through long-term retention of data and robust machine learning, will provide a powerful tool for threat hunting, investigation, and remediation.

Lastly, governance, compliance, and data cataloging – allows teams to better understand and protect your data efficiently. These approaches provide a high transparency level to each task that allows decision-makers and those tackling key missions to see specifically what is going on throughout the process. When followed effectively, teams are able to smoothly move along the zero trust journey to optimal.

Achieving the required deadline demands respecting the role of data in the zero trust journey, understanding how agencies can best protect their data, and how proper governance supports the trek to optimal maturity. As a constant and evolving mission, the nation is working to protect our country from cyber adversaries and secure its intelligence, including DOD missions.

This comes with the help of platforms that are prepared to fulfill a balance of security from bad actors and access to the right members of the DOD, all while maintaining zero trust and abiding by the CISA guidelines. A platform that operates independently from compute and storage layers will offer integrated security and governance based on metadata, while a simplified data delivery and access model will reduce risks and costs while enabling faster deployment. Implementing an effective zero trust approach and reaching the optimal maturity level will better secure the nation's cyber and technological landscape, and understanding the role of data and governance within the process can lead to greater mission success.

About the Author

Carolyn Duby is the current Field CTO and Cybersecurity Lead at Cloudera Government Solutions. With nearly three decades of experience, Carolyn spearheads the digital transformation efforts for Cloudera's customers and delivers high-performance, data-intensive applications in a variety of industries. She can be reached online at our company website https://www.cloudera.com/solutions/public-sector.html

Securing the Cloud

Organizational Data Security Strategy - Bring Your Own Key (Byok)

By Chris Allen, Senior Solutions Architect, Cryptomathic.

Cloud computing is now the norm. Up to 94% of enterprises reportedly use cloud services, which has forced organizations to rethink their approach toward security. Instead of focusing on securing the perimeter of a local database, a cloud-first approach necessitates safeguarding the data itself.

Encryption solutions can protect data at rest or in motion, but cloud computing raises security concerns relating to encryption keys. Companies frequently struggle with ownership and visibility of encryption keys, which are typically controlled by the cloud service provider. As a result, customers are understandably concerned about the security of their data, as someone else could potentially access their encryption keys.

The Bring-Your-Own-Key (BYOK) approach has emerged as a solution to data encryption key vulnerability. Let's examine the workings of BYOK and explore the business benefits and challenges associated with the technology.

How BYOK Works

BYOK is a data security method that allows organizations to bring their own encryption keys to a cloud environment, providing some level of control and management of them. This helps address concerns around key visibility and ownership, preventing infrastructure providers like cloud service providers (CSPs) from accessing those keys unencrypted.

It must be noted that organizations store and safeguard such BYOK keys in the cloud environment, which limits the control provided by a BYOK environment. However, the cloud service providers incorporate their BYOK capabilities with a traditional hardware security module (HSM) - so that they are protected from unauthorized access.

Benefits of BYOK

Data is a crucial element for companies in the current business environment. As a company's most important non-human asset, additional safeguarding measures such as BYOK can be beneficial. Let's examine some of the business advantages that BYOK can offer.

BYOK can enhance data security as part of a comprehensive security program. It enables organizations to utilize data as needed, including cloud data analytics and internal sharing, while preserving the highest security standards. BYOK can be a potential control mechanism for compliance regulations such as GDPR, which mandate advanced data protection practices, including "the right to be forgotten".

BYOK offers enhanced data control for organizations. Previously, cloud-stored data was encrypted with keys owned by CSPs, leaving companies without control over their own data. This is especially concerning for highly regulated industries like finance and healthcare. With BYOK, organizations can manage their own keys and regain control over their data.

BYOK offers increased flexibility for organizations operating across multiple geographies as it enables the use of the same keys to safeguard data regardless of the cloud service provider. Additionally, it allows for customization of key management systems to meet specific security requirements.

Organizations assume data breaches will happen, but BYOK can minimize the impact of such breaches. As the root keys are controlled by the customer, data that are protected through BYOK makes it unreadable and useless to inside attacks (within the CSP) and external hackers alike. BYOK can also prevent potential compliance fines and lost business that a breach can create. It serves as an indirect cost-savings method.

Potential challenges associated with BYOK

When implementing any technology, including BYOK, organizations should be aware of potential drawbacks and have a plan in place to address them.

Implementing BYOK requires a transfer of control to the data owner, which includes greater responsibility over data and keys. The CSP must enable key generation and provide a reliable mechanism for protecting data in the cloud environment.

The meaning of BYOK varies among different CSPs and not all BYOK options may be fully compatible with CSPs. Therefore, conducting extensive research in the initial stages of finding a BYOK solution is crucial to avoid wasting time on meetings with vendors who may not meet one's requirements.

There are additional expenses associated with setting up and managing BYOK. Depending on the level of service provided by the vendor, additional staff may be required to maintain the system. Organizations may also need to invest in HSMs, which can increase costs.

Three questions you need to answer

While cloud computing undeniably offers a plethora of benefits and efficiencies for organizations, it simultaneously creates new security concerns. For organizations looking to leverage a BYOK security strategy, there are a few key considerations:

1. **Is the service user friendly?**

It might seem an obvious point, but most organizational encryption strategies are run by the organization’s Chief Security Officer, who is typically not an expert in cryptographic encryption. It is important to ensure that whoever is responsible for the encryption strategy can understand and leverage the service without issues.

2. **Does the service use hardware security modules?**

By using hardware security modules as the foundation for data security, organizations can safely store, manage and push their own encryption keys. This provides added peace of mind in a rapidly evolving digital landscape. Being rooted on hardware security modules provides an extra layer of protection against unauthorized access from third parties.

3. **Does the service include key movement tracking?**

Some services cover key movement tracking requirements with time stamps and the identity of users administrating keys. This is vital for setting up comfortable audits to meet regulatory compliance standards.

BYOK can reduce the risk of data loss during data transfer, but it relies on an organization's ability to safeguard the keys. It is important to have a strategy for securing, replacing, and retiring keys.

Due to the shift towards cloud technology and the increasing importance of data, all organizations, particularly those in regulated industries, must adopt a security approach that prioritizes data protection. This involves incorporating features that restrict access to data and prevent exposure in the event of a security breach. BYOK is a helpful tool for achieving this goal and has become essential for contemporary security implementations

About the Author

A graduate of Cambridge University in Computer Science, Chris has spent the majority of his career involved with the development of Hardware Security Modules (HSMs) specializing in the on-board programming of HSMs. Chris is now the Senior Solutions Architect at Cryptomathic. Chris can be reached online on LinkedIn or at our company website https://www.cryptomathic.com/

Will Zero Trust Replace SD-WAN?

By Jaye Tillson, Director of Strategy, Axis Security

A question I get asked frequently is, “Will zero trust replace SD-WAN?”. Let's take a deeper look at both and assess their compatibility and potential to coexist or replace each other.

In today's digital landscape of the hybrid worker, organizations are constantly seeking robust and secure network solutions to meet their ever-evolving requirements. Data, services, systems, users, and their devices are now everywhere and two prominent approaches to assist with this world of access complexity have gained traction. They are Zero Trust and Software-Defined Wide Area Networking (SD-WAN).

Over the years SD-WAN has proven its value in optimizing network performance, there is a growing discussion in our industry about whether Zero Trust will eventually replace SD-WAN as the preferred network architecture of choice.

Understanding SD-WAN:

SD-WAN is a technology that allows organizations to connect and manage various types of networks, including MPLS, broadband, and cellular, through software-defined control and centralized management. It enables organizations to improve network performance, enhance security, and reduce costs by intelligently routing traffic based on application, bandwidth requirements, and network conditions. SD-

WAN provides a flexible and scalable solution for organizations with geographically distributed branches, enabling them to leverage multiple network links efficiently.

Exploring Zero Trust:

Zero Trust is a security concept that challenges the traditional perimeter-based security model that we are all familiar with. Instead of assuming trust within our network, Zero Trust assumes zero trust, and every user, device, and network element must be authenticated and authorized before gaining access to resources. It employs granular access controls, continuous monitoring, and adaptive authentication to ensure that only authenticated and authorized users can access specific resources. Zero Trust minimizes the risk of lateral movement within the network, mitigating the potential impact of breaches and insider threats.

The Relationship Between Zero Trust and SD-WAN:

Zero Trust and SD-WAN have different primary objectives. SD-WAN focuses on optimizing network performance, while Zero Trust emphasizes security. However, I believe they can complement each other to create a more robust and secure network infrastructure.

Zero Trust can enhance SD-WAN's security capabilities by adding an additional layer of authentication and access control. By implementing Zero Trust principles, organizations can ensure that only authorized users and devices can access the SD-WAN network and its associated resources. This prevents unauthorized access and strengthens the overall security posture.

On the other hand, SD-WAN can improve the performance and efficiency of Zero Trust implementations. SD-WAN's ability to dynamically route traffic based on network conditions and application requirements can be used to enhance the user experience and minimize latency associated with Zero Trust security measures.

Will Zero Trust Replace SD-WAN?

While Zero Trust and SD-WAN can work together to provide a comprehensive network solution, I believe that it is unlikely that Zero Trust will completely replace SD-WAN. Both approaches serve different purposes and address distinct aspects of networking and security.

SD-WAN offers significant benefits in terms of network performance optimization, cost reduction, and efficient resource utilization. It is particularly useful for organizations with distributed branches that require reliable connectivity and application performance across diverse network links.

On the other hand, Zero Trust is primarily concerned with security and ensuring that only authorized entities can access resources. It addresses the evolving threat landscape and provides a more proactive approach to securing networks and protecting sensitive data.

To conclude, in the ever-evolving landscape of network architecture and security, both Zero Trust and SD-WAN have emerged as practical approaches. While SD-WAN excels in optimizing network performance and reducing costs, Zero Trust focuses on securing access to resources. I believe that these two concepts are not mutually exclusive; instead, they can complement each other to create a more robust and secure network infrastructure.

The collaboration between Zero Trust and SD-WAN allows organizations to achieve enhanced network performance and security. It is crucial for organizations to understand their specific requirements and align their network strategy accordingly, leveraging both Zero Trust and SD-WAN to create a comprehensive and future-proof networking solution.

About the Author

Jaye Tillson, Director of Strategy, Axis Security. Jaye is a technology leader with a proven track record in delivering global strategic and enterprise wide programmes totalling over $1billion. He provides technical advisory to global mergers and acquisitions across multiple countries and cultures, large scale global transformation programs, enterprise-wide cyber security governance, digital strategic planning, and the creation of operational efficiencies.

He has spent over 20+ years understanding the challenges of defining and implementing enterprise strategies and translating these into the design and deployment of enterprise-wide platforms and infrastructures. His expertise includes the globalisation of IT platforms to create cost and resource efficiencies, resilience, and improved information flow to support executive decision making.

Jaye has led multiple large strategic technology programmes and is a critical asset for the success of organisations undergoing global transformation. He has built and trained several globally reaching teams, capable of successful execution of strategic plans. He is currently responsible for the budget, costing, fiscal planning, cost reduction and global people management at a large technology manufacturing organisation.

He is recognised as a mentor and coach in his area of expertise and observes industry and market trends to ensure his technology recommendations fit the business strategy. He is a senior technical lead, is seen as the go-to person within the business for all technical questions and is seen as a role model in the organisation.

Ensuring Container Security: Safeguarding the Future of Cloud Computing

Containerization has revolutionized the world of software development.

By Divakar Kolhe, Digital Marketer, Market Research Future (Part of Wantstats Research and Media Private Limited)

In today's fast-paced digital landscape, containerization has emerged as a game-changer for software development and deployment. Containers offer a lightweight and scalable solution, enabling organizations to rapidly deliver applications across different environments. However, as containers gain popularity, ensuring robust container security becomes imperative. This blog post will delve into the world of container security, highlighting its significance, the risks involved, and effective strategies to fortify your containerized infrastructure.

Containerization has revolutionized the world of software development and deployment, enabling organizations to achieve scalability, flexibility, and efficiency. However, with this innovation comes the pressing need for robust container security practices. As containers become more prevalent in the cloud computing landscape, ensuring their security becomes paramount. So, in this article, we will delve into the key aspects of container security, exploring the risks and challenges involved and presenting best practices to mitigate vulnerabilities.

Understanding Container Security

Containers provide isolated and lightweight environments for running applications, but they can introduce security risks if not properly managed. One primary concern is the potential for a compromised container to spread malware or gain unauthorized access to sensitive data. Moreover, container orchestration systems, like Kubernetes, introduce additional complexities, making it crucial to adopt a multi-layered security approach.

Basically, container security refers to the practice of implementing measures to protect containerized applications and the underlying infrastructure from potential threats. Containers provide isolation for applications, but if not adequately secured, they can become vulnerable entry points for cyberattacks. By exploiting weaknesses in container configurations or utilizing compromised container images, malicious actors can gain unauthorized access, compromise data, or execute malicious code.

Let us understand one of the aspects here, which is how to integrate the security testing and automate the deployment of the container security model. Such systems must be deployed carefully and according to established SOPs, which is a chaotic task. Once the construction is complete, it is necessary to manage them in accordance with industry standards, such as those published by the National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS).

Understanding how to automate policies to indicate builds with security flaws, especially as new vulnerabilities are discovered, which is the trick in this situation. Vulnerability scanning is still crucial, but it is only one of many security measures used to safeguard your container settings.

Security testing should incorporate strategies that prompt automated rebuilds because patching containers is never as effective of a fix as rebuilding them. The initial element of this process is using component analysis tools that can track and flag problems. The establishment of tooling for automated, policy-based deployment is the second step.

The following inquiries must be answered when integrating security testing and automated deployment:

- Do any containers have known flaws that need to be corrected before they can be used in a real-world setting?
- Are the deployments set up properly? Exist any containers with excessive privilege that don't require the increased privilege? Do we have a root file system that is read-only?
- What is the CIS Benchmarks compliance posture?
- Are any workloads deemed sensitive being isolated using default features like network policies and namespaces?
- Are we making use of SELinux, AppArmor, and seccomp profiles, among other built-in security and hardening tools?

Key Challenges and Risks

1. Vulnerabilities in Container Images: Containers rely on pre-built images, often sourced from public repositories, which may contain unpatched software or misconfigurations. This increases the risk of exploitation by attackers.
2. Container Breakouts: Weak isolation between containers or improper privilege management can allow attackers to break out of one container and gain unauthorized access to the underlying host or other containers.
3. Container Sprawl: Unmonitored and uncontrolled container proliferation can result in a large attack surface, making it challenging to detect and manage potential security breaches.
4. Inadequate Network Segmentation: Insecure network configurations can lead to unauthorized lateral movement between containers or allow attackers to eavesdrop on container communications.

Best Practices for Container Security

1. Secure Container Images: Regularly update and patch container images, ensuring they are sourced from trusted repositories. Scan images for vulnerabilities and enforce image signing and integrity verification.
2. Implement Role-Based Access Controls (RBAC): Apply granular RBAC policies to restrict container access and prevent unauthorized modifications to containers or their configurations.
3. Container Runtime Security: Utilize container runtime security tools to monitor and control container behaviour, detect anomalies, and prevent container breakouts.
4. Network Segmentation and Policies: Implement network segmentation to isolate containers and define strict network policies to control traffic flow between containers and external systems. Use secure network protocols and encryption to protect container communications.
5. Continuous Monitoring and Logging: Deploy robust monitoring and logging solutions to detect and respond to security incidents promptly. Monitor container activity, collect and analyze logs for security events, and enable automated alerts.
6. Regular Vulnerability Scanning and Patch Management: Conduct periodic vulnerability scans on container images and apply patches promptly to address any identified vulnerabilities.
7. Secure Container Orchestration: Harden the container orchestration system by implementing strong authentication mechanisms, securing control plane components, and regularly updating the orchestration software.

Why is the Container Security market fostering?

According to Market Research Future's latest research report on Container Security Market, the growing popularity of microservices and digital transformation has led to impeccable growth in the market.

Container security could have been the most prolific market segment if there were a huge number of applications running in the containers used in businesses.

In order to modernize outdated IT infrastructures, several governing authorities across the globe have opted to virtualize their data and the massive workloads in containers as a service module. These containers are pivotal in accelerating such a transition from the conventional to the modern path of cloud security.

With the several benefits the container security offers including prompt responses, increased revenue, swift business decision-making ability, etc., several businesses around the globe have started embracing this technological advancement to automate their business and have customer-centric services that aid in their customer acquisition and retention.

With this, the continuous interaction between the applications running in the container and the deployment of several applications across the open-source software development platform enhances the platform's portability, improves traceability, and utilizes and reallocates the container with a minimal data loss in any case of emergency or any casualties. All these reasons are pivotal in the overall growth of the container security market, which is eventually helping this technology reach every fraction of the global industry.

Conclusion

Container security is a critical aspect of maintaining a secure and resilient cloud computing environment. By understanding the risks and implementing the best practices outlined above, organizations can enhance their container security posture. Regular vulnerability scanning, strong access controls, and continuous monitoring are essential to mitigating risks associated with containers. As the use of containers continues to grow, a proactive and comprehensive approach to container security will be fundamental to safeguarding the future of cloud computing.

Reference - Market Research Future

About the Author

Divakar Kolhe is a highly skilled and experienced digital marketer who has dedicated his career to driving online success for businesses. With a strong passion for data-driven strategies and a deep understanding of consumer behavior, Divakar has become an invaluable asset in the field of digital marketing.

Divakar Kolhe - divakar.kolhe@marketresearchfuture.in
Website: https://www.marketresearchfuture.com

Key Factors and Measures to Address Burnout in The Cybersecurity Field

The underlying threat to organizations

By Kunal Purohit, Chief Digital Services Officer, Tech Mahindra

In Today's world Cyber-attacks may be on the rise, but one of the biggest threats to an organization's cybersecurity isn't just hackers — it's burnout among cybersecurity teams. The responsibility of cybersecurity specialists has grown because of the evolution of technology and the rise in cybercrimes and threats. Professionals in the fast-paced and demanding field of cybersecurity require a high degree of expertise and focus. They must keep up with the most recent threats, vulnerabilities, and technology because it is a sector that is continuously changing. This can be time-consuming and demanding, particularly when combined with a heavy workload.

2022 data from a survey shows that 84% of cyber security professionals experienced extreme stress or burnout, 65% have considered leaving their job because of stress, and 53% of workers have resigned.

Employee burnout in the cybersecurity field is detrimental for several reasons. It leads to increased mistakes as overworked cyber defenders tend to overlook essential details, it causes a lack of motivation needed to come up with critical solutions, and it results in higher resignation rates that trigger further burnout, as teams don't have the workforce to complete all the tasks needed for a job that runs 24/7.

The talent shortage within the cybersecurity industry continues to be a persistent issue and was cited as a top reason for burnout among cybersecurity professionals. There are nearly 770,000 unfilled cybersecurity positions in the U.S alone. When there's a gap in the workforce, employee burnout tends to increase. When teams are left with an insufficient number of cyber defenders, those remaining are expected to work in multiple different roles, sometimes more than they can handle. This often means signs of stress and burnout are ignored, and it leaves no room for career growth. Leaders that prioritize work over their employees' wellbeing will eventually create an unproductive work environment where employees will disengage or leave.

Other key contributors to burnout are inefficient work processes. There are often too many security tools and too little communication among teams. Tools that are not integrated increase frustration, as additional unnecessary steps may be required to complete a single task on list that keeps growing. Traditionally, information technology (IT) and security departments have operated in rigid silos, with cybersecurity working behind closed doors in solitary environments and, as a result, creating a fragmented security framework. This lack of integration creates challenges for teams as they are reacting to changes in IT solutions and policies being implemented, making it harder to operate efficiently.

Cyber security workplace burnout is not an unsolvable problem; there are ways to address them. Following are the measures that organizations can adopt and educate their customers about it as well.

Re-evaluate and Better your Recruiting processes - This means recruiters should prioritize specific characteristics and soft skills, such as critical thinking, communication and problem-solving, that make a great cybersecurity professional rather than wait for the perfect resume. This will expand the talent pool and encourage innovative ideas essential for solving today's significant cybersecurity challenges.

Better training programs – Help the potential recruits develop the necessary skills for the job while emphasizing the education of their employees. Even for those with years of experience in cybersecurity, education is a constant aspect of the job, especially as the threat landscape continues to evolve. One of the most effective methods is to use phishing simulations and exercises. These can help employees understand the importance of cyber security and the potential consequences of a breach.

Creating a positive work environment – attracts and retains talent is equally vital to recruiting talent. A people-first culture where team members feel empowered and prepared to face whatever threats they encounter is the ultimate solution. Leaders should encourage employees to try new projects and roles and voice their opinion on what needs to shift, whether it be team structure, changes to work schedules, or training opportunities.

Use security automation to enhance human analysts - Humans are the weakest link in any organization's security posture. No matter how many technological security layers you have in place, it only takes one person to click on a malicious link or open a malicious attachment to potentially bring down your entire operation. By automating repetitive and mundane tasks, security analysts can free up their time to focus on more strategic tasks that require human expertise.

Outsource some security tasks - By working with a security provider like Tech Mahindra, businesses can tap into a team of experts who religiously keep up with the latest threats and vulnerabilities. This way, companies can be sure that their data and systems are always protected against the latest threats.

Create a comprehensive security plan – The feeling of being constantly on alert can often lead to burnout. Creating a comprehensive security plan can help to ease some of this burden, as it can provide a clear and concise overview of the steps you need to take to keep your data and systems safe. By taking the time to sit down and create a plan, you can make sure that you cover all the bases and reduce the chances of becoming overwhelmed or burning out.

Get rid of unrealistic expectations of cyber security professionals - When people are constantly being told that they need to be "on the lookout" for new threats, it can lead to feelings of anxiety and inadequacy. It's important to remember that no one is perfect and that it's impossible to anticipate every single threat.

Take some burden off your IT team by ensuring that your whole organization is cyber security aware - By doing this, you're not only easing your IT team's workload but also giving them the bandwidth to focus on bigger projects.

To Summarize, the leaders must hold themselves accountable to reinvent the way they manage their teams to promote better collaboration and growth. As a result, this will foster a work culture where cyber defenders can do their best work. In a world full of unknown threats, the threat of employee burnout among cybersecurity teams can and must be controlled.

About the Author

Kunal Purohit is the Chief Digital Servies Officer at Tech Mahindra. He heads TechM's digital and analytics capability solutions units (CSUs) globally. These units build new solutions for enterprises going through digital transformation.

Kunal can be reached online on LinkedIn and at Tech Mahindra | Connected World, Connected Experiences.

Six Must-Focus Cybersecurity Areas in Network Sprawl

By Zachary Folk, Director of Solutions Engineering, Camelot Secure

The anticipated benefits of 5G's faster speed, lower latency, and greater capacity to accommodate many connected devices hold tremendous potential and promise. The Ericsson Mobility Report predicts that 5G subscriptions will reach 4.4 billion globally by the end of 2027 and reach 48% of total global mobile subscriptions. However, every new technology has the downside of bringing additional attack surfaces, exacerbating cybersecurity problems.

In addition to the massive number of new devices shuttling data over 5G networks, the stay-at-home workforce also adds to cybersecurity issues. In this relatively new environment, employees use personal devices to connect with corporate networks. Many of these devices don't have the most recent security patches installed, which opens doors to advanced persistent threats.

Another "plus" in the cyber-attackers column is that many organizations are significantly understaffed with cybersecurity experts to monitor network traffic, identify the anomalies considered a top priority, and execute a process to contain threats. As attack surfaces grow, skilled IT staffs continue to dwindle. No matter what the cybersecurity staff size is, they must continue to focus on these six areas:

1. Awareness and Monitoring - Get familiar with your attack surface and make sure you have up-to-date documentation of all connected assets. Use a Security Information and Event Management (SIEM) baselining software, a rogue system detection device, and a vulnerability scanner to help with the identification.
2. Cybersecurity Training - It's crucial to ensure the IT team knows how to identify potential compromises and the knowledge to report and escalate a response when needed correctly.
3. Impact Reduction - Limit sensitive information and connectivity to vulnerable systems and have a well-trained Incident Response Plan (in-house or third-party) to address cyber threats.
4. Vulnerability Management - A Vulnerability Management program will collect the latest threats and vulnerabilities, including threat intelligence. The data for the intelligence collection can be produced by a vulnerability scanner tailored to individual networks with a SIEM.
5. Threat Information Sharing - Participation in threat information sharing platforms such as the Cybersecurity and Industrial Security Agency's Automated Information Sharing program and the Cybersecurity Incident Response Center's (CIRCL) Malware Information Sharing Platform (MISP), which is also known as the Open Source Threat Intelligence Platform (OSTIP) is highly recommended.
6. Incident Response Training -Finally, prioritized training for SOC/NOC personnel that emphasizes how to conduct the processes outlined in the Incident Response Plan is needed, along with periodic (monthly) reviews of the Vulnerability Management Plan to ensure that it accurately incorporates assets and addresses all vulnerabilities.

New technologies indeed bring advancements in communication and computation. But these advanced technologies come with the warning that each newly connected device holds an additional gateway for hacker entrance. Enterprises are facing new vulnerability challenges against the backdrop of inadequate IT protection.

Cybersecurity professionals must automate network security using SIEM, rogue systems detectors, and vulnerability scanners to identify potential threats. For organizations lacking cybersecurity personnel or the necessary monitoring/analyzing tools, highly-trained, third-party cybersecurity professionals can perform all these preventative threat measures—often at a lower cost than one highly-trained cybersecurity professional.

Outsourcing cybersecurity responsibilities to a third-party security provider is similar to outsourcing data storage and processing to a cloud provider. Both bring cost, scale, and expert knowledge advantages to the table. As the border of today's enterprise networks continues to creep beyond the confines of corporate walls, more skilled cybersecurity teams and advanced automation tools are needed to mitigate risks and diminish attack surfaces.

About the Author

Zachary Folk currently serves as the Director of Solutions Engineering at Camelot Secure. As an experienced Cyber professional, he has worked in roles ranging from System Administration to Information System Security Management. This experience allows him to help companies integrate technical solutions for compliance and security standards. He holds several top-level Cybersecurity Certifications and a bachelor’s degree from the University of Alabama in Huntsville. Additionally, he has served 14 years as an Officer in the Alabama National Guard. Zachary can be reached online at zachary.folk@camelotsecure.com and at https://camelotsecure.com/.

From Chaos to Control: The Crucial Role of Cyber Incident Response for SMBs

How to create a well-defined incident response plan

By David Chernitzky, Co-Founder and CEO, Armour Cybersecurity

Cybersecurity incidents can result in significant financial losses, damage to reputation, and compromised customer data – which is especially devastating for small and medium businesses (SMBs) because they often lack the resources to properly react and rebuild after an attack. That's why it's crucial for SMBs to prioritize incident response preparedness. Organizations must have a well-defined incident response plan in place. But what does that look like in practice for SMBs?

Create a Cybersecurity Incident Response Playbook

If your organization is hit by a cybersecurity attack, it’s important to respond quickly, efficiently, and effectively. You need a plan. A cybersecurity incident response playbook is a step-by-step guide for handling potential security incidents. Creating an effective incident response playbook for a SMB must include the following steps:

- Identify key stakeholders and their roles: Clearly define the responsibilities of internal teams, such as IT, legal, PR, and HR, as well as external partners and vendors.
- Document incident response procedures: Document the necessary actions, communication protocols, and decision-making processes to ensure a swift and coordinated response.
- Tailor playbooks to specific threats: Customize playbooks to address the specific cybersecurity threats most relevant to your organization, such as malware attacks, data breaches, or social engineering attempts.

Perform Regular Table-Top Exercises

But what good is a plan if you’re not ready to execute it? This is where table-top exercises come in. Table-top exercises are simulated scenarios designed to test an organization's incident response plan. These exercises help identify gaps and areas for improvement, ensuring that the response plan is effective and the team is well-prepared. Be sure to conduct regular table-top exercises that accomplish the following:

- Create realistic scenarios: Develop scenarios based on real-world threats and recent cybersecurity incidents to accurately reflect potential challenges.
- Involve all relevant stakeholders: Include representatives from different teams and departments to promote cross-functional collaboration and enhance understanding of each team's role.
- Evaluate and update the incident response plan: Use the outcomes of table-top exercises to identify weaknesses and update the incident response plan accordingly. Continuously refine and improve the plan based on lessons learned.

Foster Awareness with Management and Executives

Without support and buy-in from management and executives, your incident response plan isn’t complete. In fact, with the rise of social engineering attacks targeting top personnel it’s more important than ever to educate these key stakeholders. Keep the following in mind when raising awareness with management and executives:

- Communicate the potential impact: Present cybersecurity statistics and case studies to highlight the financial and reputational damage that can result from inadequate incident response preparedness.
- Emphasize the importance of proactive measures: Stress the significance of investing in incident response capabilities as a proactive approach to mitigate risks rather than reacting after an incident occurs.

- Encourage a culture of cybersecurity: Management and executives should lead by example when it comes to cybersecurity best practices, such as regular training, password management, and data protection.

Enhance Cybersecurity Controls

SMBs should focus on building cyber resilience to effectively manage and recover from cyber incidents. Consider the following measures:

- Implement robust backup and recovery procedures: Regularly back up critical data and test the restoration process to ensure data availability in case of an incident.
- Engage third-party cybersecurity experts: Consider partnering with external cybersecurity firms that can provide specialized expertise and support during incident response.
- Stay informed about emerging threats: Continuously monitor the threat landscape, participate in information sharing forums, and leverage threat intelligence to stay ahead of evolving cyber threats.

New cyber threats are emerging every day, and smaller businesses are especially vulnerable to cybercriminals. In the event of a cyber incident -- such as business email compromise, ransomware, or an attack on its supply chain -- a rapid yet well-thought-out response makes all the difference. By taking proactive measures to mitigate risks and build cyber resilience, SMBs can strengthen their defenses and respond quickly to attacks, limiting damage to networks and compromises to data.

About the Author

David Chernitzky is the Co-Founder and CEO of Armour Cybersecurity. David specializes in helping businesses protect their assets from cyber threats. He served as an officer in the elite technology unit of the Israeli Defense Forces Intelligence Corps and spent many years working for multinational enterprises in technology and business functions. For more information, visit https://www.armourcyber.io/

Lessons Learned: Cyberattack Shutters Five Illinois Healthcare Facilities

Growing Cyber Attacks Pose Existential Threats to Business – Can More Connected and Efficient Security Help Organizations Gain the Upper Hand?

By Emily L. Phelps, Director & Cybersecurity Advocate, Cyware

St. Margaret's Health of Illinois was forced to shut down two hospitals and three clinics, almost two years after struggling to recover from a prolonged ransomware attack in 2021. Even veteran cybersecurity experts accustomed to troubling breach and impact news took note.

The attack had persistent impacts; it kept their network down for three months and prevented them from billing insurers, Medicaid, or Medicare for months afterward.

"We could not access any of our information system, including email and the EMR," said Linda Burt, vice president of quality and community service at St. Margaret's Health. "We had to resort to paper for medical records. It took many months, and in some service lines, almost a year to get back online and enter any charges or send out claims. Many of the insurance plans have timely filing clauses which, if not done, they will not pay. So, no claims were being sent out and no payment was coming in."

The ransomware attack shut down the spring valley hospital computer network and ceased all web-based operations, including the patient portal. Coupled with the impacts of the COVID-19 pandemic, the attack's cascading impacts proved insurmountable.

St. Margaret's 18-plus month recovery effort failed and on June 16, 2023, the five facilities closed for good.

A Hidden Culprit – Security Data Silos

One of the frustrations security practitioners experience with cyberattacks like this is that while the ransomware spread quickly, the data that could have helped the team defend against it didn't. Threat intelligence data is often stranded – isolated in 'data silos' separately managed within various functional groups.

The average organization of St. Margaret's size uses dozens of discrete security tools, many of which don't share their data or connect directly to other security tools, outside of their own application and assigned management group.

Given the high volume of threats and security alerts flooding analysts, these data silos can lead to dangerously slow responses. While tools are helpful – and necessary – cybersecurity pros need more than point solutions to defend against collaborative, persistent attackers.

This is where orchestration across silos, AI-driven automation, and collaboration tools can play an important part. AI and machine learning don't replace humans, but they can pull together diverse data streams, consolidate redundant data to reduce the noise, integrate threat intelligence into SOC operations, and enable security teams to automate some responses and act immediately on others.

Equally important and often overlooked is the need to automate alerts with the right information, and get them to the right people as quickly as possible. The status quo for many teams is to track threats on spreadsheets and communicate by email, if at all. Best case – it can take days to weeks to alert the right people and concisely tell them what they need to know.

But by automating the tedious work and sharing context-rich information immediately, security experts can pinpoint attacks and take intelligent action – before irreparable damage occurs.

The TIP-ing Point: Leveraging Existing Intel to Thwart Future Attacks

The path to integrate threat intelligence platforms (TIP) with data orchestration and workflow automation (SOAR) seems daunting for many organizations.

It doesn't have to be.

First, we need to think more proactively – reacting to incident alerts and then scrambling to identify the best response leaves adversaries with an advantage. But proactive security certainly has its challenges; trying to spot looming threats has been dismissed as too difficult and expensive.

Frankly, wading through millions of data points is not a human-scale problem. Without tools to effectively process, analyze, and prioritize data, these internal clues often remain undetected, or are discovered forensically, long after attacks have occurred.

Today's security challenges are less about detection than they are about connecting the dots. With the growing number of tools, there is lots of overlap, and adding new tools has diminishing returns. Ultimately, we need better ways to integrate, connect, and orchestrate action across the security tools we already have.

St. Margaret's serves as a stark reminder of the worst-case scenario for a small healthcare organization. Without enough resources to invest in robust security, updated systems, and without having a clear recovery plan, these important local providers can be put out of business, leaving their communities with limited – if any – healthcare services.

This is an industry-wide problem, yet we expect our under-resourced teams to defend themselves against perpetual threats. Visibility is critical to detection. Automation is critical to scale. Intelligence and alerting are critical in order to take action. But we can't rely solely on independent tools. We must invest in pragmatic systems that can integrate, share, and contextualize quickly, reliably, and with confidence, and make these capabilities available as managed services for smaller organizations.

About the Author

Emily L. Phelps has written about and worked in the cybersecurity space for nearly a decade. Throughout her career, she has helped translate complex technical material into digestible insights for business leaders, and she has supported cybersecurity initiatives and solutions in order to assist practitioners in their day-to-day work. Emily is a fierce advocate for pragmatic cybersecurity programs that enable organizations to operate, uninterrupted, by cyber threats.

Emily can be reached on Twitter at @CywareCo and at the Cyware website: https://cyware.com/

What is Malvertising?

Best practices for avoiding novel threats online

By Tom McVey, Senior Sales Engineer EMEA, Menlo Security

Artificial intelligence has transformed digital marketing.

From tracking customer conversations to measuring engagement with content, it’s a technology that’s enabling organisations to unlock incremental competitive advantages through productivity improvements, data-informed service enhancements, and enhanced customer interactions.

However, there are two sides to every coin.

Research conducted by CensusWide for Menlo Security reveals that one in three UK consumers believe that over half of all advertisements on websites or social media sites are generated by AI. The merits of AI in marketing and advertising are clear – it’s an undoubtedly useful resource. Yet it also opens up opportunities for malicious actors.

With the increasing use of AI in digital advertising, we at Menlo anticipate a major spike in ‘malvertising’ due to the rise in convincing fake ads created by AI tools like ChatGPT and image generators such as Midjourney and DALLE.

What is malvertising?

Malvertising is a form of highly evasive threat where malware is embedded into online or social media ads.

Malvertising can be particularly tricky to detect for both internet users and publishers, with malicious ads typically serving consumers through legitimate advertising networks; all internet users encountering them are at risk of infection.

Not only is malvertising novel, it's typically complex, and usually comprises several rungs in the attack chain.

Attackers will usually begin by breaching a third-party server to inject malicious code within a digital advert, such as a banner advert, or video. If clicked by a website visitor, the corrupted code will lead to the installation of malware on the user’s endpoint device or direct a user to a malicious website.

Indeed, some advertising attacks involve the use of exploit kits – created with the intention of surveying a system to then identify and exploit vulnerabilities. And, if installed, malware can wreak untold damage.

Threat actors may delete, modify, or encrypt data. Further, malware may be used to corrupt files, redirect internet traffic, monitor user activity, steal data or develop backdoor access routes to a system.

Awareness of malvertising is currently low

Given this is a relatively novel and innovative attack method, awareness of the threats of malvertising remains low at present.

In our survey conducted with CensusWide, we found that while seven in ten consumers say they currently click on advertisements on the internet ‘to some extent’, the vast majority (70%) of respondents simply didn’t know they can be infected with malware by clicking on a brand logo.

By comparison, almost three-quarters (73%) understand they can be infected by malware hidden in an email link.

The research also revealed that around half (48%) are unaware they can be infected via a social media ad, while 40% didn’t know they can be infected by clicking on pop-ups and banners. Furthermore only 32% wouldn’t trust any website not to contain malvertising.

These statistics are concerning. Indeed, it’s estimated that approximately one out of 100 online ads is currently malicious, and we now expect this to rise even further as more AI tools and software become increasingly available and easy to use.

Malware-as-a-service and AI generated text and images are already accessible, meaning even attackers with little or no skills can create convincing ads and powerful evasive malware to boot. We're expecting a big uptick in malvertising as a result.

Best practices for avoiding malvertising

Awareness of the risks needs to increase so that anyone online applies caution to clicking on adverts on any website – no matter how much they trust it.

Some people may be shocked to learn that even the most credible websites are not immune to malvertising. Indeed, we recently found that the top three brands impersonated by malicious threat actors attempting to steal personal and confidential data over a 90-day period were Microsoft, Facebook, and Amazon.

So, how can consumers ensure they don't become the victim of malvertising?

First, it's important to carefully check website URLs before clicking. This can be done by hovering your mouse over the advert until the URL appears. Threat actors can often use convincing domain names by replacing certain characters to trick the eye, but they won't be able to use the actual domain of the site you think you're clicking on. Therefore, meticulously checking links for discrepancies is important.

Second, web users should check the brand logo to see if it looks genuine. When logos are copied, they can appear stretched, squashed, or pixilated. This could be a sign that it's not legitimate – large companies tend to have strict branding guidelines that malvertising attackers won't necessarily follow.

It's also worth considering what the advert is asking you to do. Legitimate brands often place adverts to increase brand awareness. Malvertising campaigns do not care about these impressions. They will be more direct, asking you to 'click here' or 'buy now'.

In this sense, it's important to be cautious of redirections. If you do click on an advert and it takes you through to the site you expected, be aware that the more ads you click on the higher chance you have of encountering malware.

Our research has found that you're only 3-7 clicks away from malware online. And the growing prevalence of AI generated content online will only fuel highly evasive threats such as malvertising further.

Ultimately, the key is taking a cautious approach to adverts. No website is immune to malvertising. By staying vigilant and always following best practices, you're much more likely to stay protected.

About the Author

Tom is a Senior Sales Engineer at Menlo Security for the EMEA region, a leader in cloud security. In this role, he works closely with customers to meet their technical requirements and architects web and email isolation deployments for organisations across different industries. Coming from a varied background in cyber, Tom provides expert cybersecurity advice and strategic guidance to clients.

Prior to Menlo Security, Tom previously worked for LogRhythm and Varonis. Tom is experienced at speaking at live events, including Infosecurity Europe, and presenting on webinars and podcasts.

www.menlosecurity.com

Why You Should Prioritize Your Privacy Policies

By Jason M. Schwent, Senior Counsel, Clark Hill

The enactment of the California Online Privacy Protection Act of 2003 created a need for commercial websites in the United States to provide an online privacy telling visitors how a company collects information from visitors of the site, how that information may be shared with others, and information on the process for accessing that information. Since that time, privacy policies became a somewhat routine and ubiquitous part of commercial websites. The preparation of those privacy policies was fairly innocuous and straight forward—often little more than a simple, accurate, recitation of company practices would suffice. But with the proliferation of state consumer data privacy laws and more enforcement activity by the Federal Trade Commission ("FTC"), the simple privacy policy is fast becoming a key regulatory disclosure, uniquely indicative of a company's compliance practices and procedures.

Modeled in part on the expansive European Union's General Data Protection Regulations (GDPR) which went into effect in 2018, state consumer privacy laws push companies to be more open with the public about their collection, use, and sharing of information they collect. Since 2018, the number of state consumer data privacy laws has quickly increased. Following the GDPR lead, states, again starting with California and the California Consumer Privacy Act, began passing comprehensive consumer data privacy regulations aimed at giving consumers increased rights in and to the information they provide to companies. Similar bills have now been passed in Colorado, Utah, Virginia, Connecticut and have been updated in California with the California Privacy Rights Act of 2020. In the past year alone, legislatures in the states of Iowa, Indiana, Tennessee, Montana, Florida, and Texas have each passed more comprehensive state consumer data privacy laws with more laws contemplated in even more states.

These state consumer data privacy laws require companies to provide information to the public about the information they collect, why they collect that information, what they do with the information, with whom they share that information, if they sell that information, how they protect that information, and when they delete that information. These statutes also provide the public with certain rights concerning the data that is collected from them by companies, including the right know what information is collected, to delete information, to prevent the sale of information, to correct erroneous information, and to transfer their information to another business. Regulations mandate that this information is required to be provided to the public prior to or at the time the information is collected.

Because commerce is increasingly conducted via the internet and mobile applications and since almost every company has a presence on the internet or a mobile application, website and mobile application privacy policies have become a key way companies can satisfy the requirements of these data privacy laws by making the required disclosures and allowing for inquiries to be made from the public. This elevates the importance of the privacy policy to one of the key documents in this entire regulatory process. For all companies, the privacy policy is key to satisfying regulatory obligations. But for companies operating in multiple states, the privacy policy must do more than simply report on the activities of the company—it must simultaneously satisfy multiple, specific regulatory requirements under multiple laws. Crafting a compliant privacy policy to meet the requirements of the increasingly complex patchwork of state consumer privacy regulations in place in the United States requires considerable analysis and consideration. These privacy policies must be thorough and attentive to all laws and regulations applicable to a business both currently and in the foreseeable future. They must be accurate (as false statements concerning data privacy practices can be considered an unfair or deceptive practice by the Federal Trade Commission and create liability for the company). And they must be updated regularly to account for the changing practices of the company and various laws. For too many companies, the thoroughness, attentiveness, accuracy, and contemporaneity required by these statutes and regulations is not reflected in their privacy policies, which leads to problems with the second reason these policies are so important.

The second reason that privacy policies are important is that they are a revealing window into the compliance operations of a business. As state regulations and laws have increased regarding consumer data privacy, so too has the need to enforce those regulations and laws. Doing so requires information on a company's data collection, use, protection, transfer, and deletion practices - all information found in a well-crafted privacy policy.

For those working in data privacy and working with the ever-increasing regulations concerning the collection, use, protection, transfer, and deletion of consumer data, privacy policies are particularly enlightening documents. As noted earlier, because most companies' compliance activities are internal to the organization and not readily ascertainable, without an audit of a company's compliance program, it can be difficult to assess the thoroughness, thoughtfulness, and sophistication of a company's compliance efforts. A privacy policy can provide insight in these areas. By examining the public privacy policy posted by a company on its website or mobile application, a regulator can quickly and accurately assess the compliance maturity and sophistication of the company. For a person familiar with data privacy law and the applicable regulations, the description provided in a privacy policy, the language used, the positions taken, and the policies set forth are as clear an indication of the business' data privacy sophistication and posture as can be gleaned without an internal investigation of the business. And if that privacy policy has not been updated, uses language that is out of date or improperly addresses data privacy concerns, or if the privacy policy was simply copied from some other business and, is out of place or otherwise ill-fitted to the business otherwise described on the website or application, it will be glaringly obvious to those familiar with data privacy law. To a skilled regulator looking for a company which has not complied with state law, reading a website privacy policy that fails to address or improperly addresses consumer rights and business responsibilities can provide more than enough grounds to open an investigation into the company.

All of this regulatory activity now makes website and mobile application privacy policies key regulatory company documents. Careful thought should be given to the preparation of these documents as would be given to any other regulatory disclosure. These policies should be drafted with care by a skilled data privacy professional familiar with the regulatory requirements at issue in careful consultation with company officials. They should not be prepared from a form or borrowed from another company's website. These policies should also be updated regularly to reflect current company practices, as an outdated privacy policy is an inaccurate privacy policy and equally troublesome from a regulatory perspective and potentially a source of regulatory liability.

There is no reason to believe that the regulatory wave of comprehensive state consumer data privacy laws is going to do anything but increase. So it is imperative that companies carefully consider their website privacy policies now, and moving forward.

The views and opinions expressed in the article represent the views of the author and not necessarily the official view of Clark Hill PLC. Nothing in this article constitutes professional legal advice nor is it intended to be a substitute for professional legal advice.

About the Author

Jason M. Schwent is Senior Counsel at Clark Hill, an international law firm. He is experienced in data privacy, intellectual property, and litigation making him a fierce advocate for his clients. His passion for protecting clients' assets is evident whether negotiating a complicated enterprise software agreement with a Fortune 100 company or counseling a client following a data breach that exposed millions of users' data,

Jason can be reached online at jschwent@clarkhill.com.

Closing The Gap: Resolving Human Error in Cloud Security

By Patrick Pocalyko, GM North America, CYREBRO

Cybersecurity technology is critical to securing the cloud but it's easy to forget that people also play an important role. And the fact is that the vast majority of security and cloud security incidents are still caused – directly or indirectly – not by technology, but by people. Here are some of the most common human errors that leave cloud deployments vulnerable, and how to rectify them.

Amendable Human Error #1 – Misunderstanding Shared Security Responsibility

It's a common misperception that once you migrate data, apps or any type of computing resources to the cloud, the cloud provider is then responsible for security. In fact, the exact opposite is true. All major cloud providers operate on what's referred to as a shared security responsibility model.

The term “shared” is somewhat misleading. It’s more like “divided.” The cloud provider’s responsibility ends with their infrastructure. Everything you bring into their environment is your responsibility. This means that upwards of 90% of the cloud security burden rests with the users. And that’s likely why Gartner concluded that 99% of cloud security failures are the customer’s fault.

Solution:
Knowledge is power. Understand the extent of protection your cloud provider offers, and make sure you have the in-house or outsourced skillset to make up the difference.

Amendable Human Error #2 - Misconfigurations

The good news is that security professionals know that a properly configured cloud environment is actually rarely breached. The bad news is that the vast majority of cloud environments are not properly configured, to say the least.

A great example of this is a recently exposed breach at automaker Toyota. Resulting from a cloud misconfiguration, this breach went on for over a decade and affected over two million customers.

Why does this happen? Under the shared security responsibility model, your IT teams need to do a lot of manual security configuring. But IT teams are not always cloud security experts (or even cloud experts, for that matter). Frequently, these teams rely on default provider settings – settings which threat actors love, of course. These settings leave, for example, 55% of companies with one or more databases that are publicly exposed to the internet due to misconfigured routes or authentication requirements. What’s worse, the sheer scalability of cloud deployments magnifies the ramifications of even a single misconfigured setting.

The under-skilled cloud admins deploying your sensitive data and proprietary applications to the cloud may not be aware of the intricacies of integration, prioritization, segmentation and permissions. It’s possible they don’t know they should conform with industry best practices and maintain separate cloud accounts for CI/CD, production, development, customer service, and more. They may not know how to handle the flood of cloud security issues raised by Cloud Security Posture Management (CSPM) systems.

Solution:
Hire skilled resources. It’s true that skilled cybersecurity professionals are hard to come by. In fact, there was an estimated cybersecurity workforce gap of over 3 million people in 2022 – and that number is still growing. To mitigate this, many organizations are outsourcing cloud security to MSSPs or other security solution providers.

Amendable Human Error #3 – Lack of Training

Sit a roomful of sales pros down and ask them to answer this question honestly: how many of you have ever copied a document with sensitive business data from an enterprise cloud database onto your laptop, so you can work on it on a flight? The majority of them will inevitably answer in the affirmative. And they are, of course, inadvertently guilty of both violating data security and creating shadow data. In doing so, their actions pose serious risks to your data security, compliance, and governance.

Solution:

This is a training issue, cut and dry. Because you can create all the policies you want and deploy all the security tools on the market – but if data can be seen on a screen, it can become unsecured shadow data. Create in-house training regimes that help cloud users better understand the implications of their everyday actions on organizational security.

The Bottom Line

As security professionals, it's easy to focus on the technological aspects of cloud security. Yet human error can be a major cause of vulnerabilities in the cloud – and is addressable. By spotlighting rectifiable human errors—understanding shared security responsibility, tackling misconfigurations, and providing proper training—we can enhance cloud security and keep our data and our businesses safer.

About the Author

Patrick leads client engagements in North America for CYREBRO, and is responsible for regional growth, business development and partnerships. Patrick brings Fortune 500 management experience in addition to 10 years in Navy military service with expertise in Intelligence and Reconnaissance, including multiple international combat tours. Patrick can be reached online at LinkedIn and at http://www.cyrebro.io.

Effective Workplace Education is Built Around Incentives

How Companies Can Personalize Cybersecurity Awareness Training

By Asaf Kotsel, CEO, Dcoya

The key to a successful workplace education platform is providing compelling behavioral incentives that keep employees engaged and help them apply what they learn. Too many employers treat workplace education as a box to check – they want to say the company has programs in place, but they aren't willing to put in the necessary work to ensure that those programs are effective.

There are many ways companies can construct incentives that will educate employees and drive healthy behavioral change. For example, they can draw a link between educational programs and professional advancement. Over the past several years, employees have become increasingly focused on talent mobility and educational opportunities that will allow them to advance their careers. It's also crucial to provide engaging and personalized educational content that maintains employees' attention and leads to long-term information retention. Companies can't check the training box if employees aren't actually learning, and employees won't benefit from educational programs that don't provide information they can retrieve and deploy in the real world.

When companies give employees convincing reasons to learn and keep them engaged as they do so, they won't just build a healthier workforce – they will also secure positive learning outcomes. When it comes to cybersecurity awareness training, this means employees will be equipped to keep the company safe from cyberattacks that can have devastating operational, financial, and reputational consequences. But no matter what you're training employees to do, the process is all about finding the right incentives.

Meeting the demand for professional development

Employees recognize that workplace education is necessary to help them compete in an increasingly skills-based and global job market. A remarkable 77 percent of employees say they're ready to learn new skills or completely retrain, while almost three-quarters say training is a matter of personal responsibility. It's no surprise that the top action employers are taking to address skills and labor shortages is upskilling workers – a goal that's even more important when there are two open jobs for every candidate who's actively seeking work.

Employees want workplace education, but training content can't be generic – it has to be relevant to their unique responsibilities, skill sets, and professional aspirations. A critical aspect of cybersecurity awareness training is real-world applicability. Employees have to understand exactly why they're learning about common cyberattacks such as phishing – it's extremely likely that they will encounter one of these attacks at some point, and they need to know what the red flags are and how to react.

Despite persistent inflation, the possibility of a recession, and other economic woes, the labor market remains strong. Companies are struggling to fill skills gaps, and they're increasingly turning to workplace education to build a more productive and loyal workforce. When companies excel at talent mobility, they retain employees for nearly twice as long as companies that struggle with it. Considering the role of workplace education in facilitating mobility, companies will rely on it even more heavily in the coming years.

Give employees a reason to keep paying attention

Any professional can tell you horror stories about sitting through exhausting, repetitive, and dull training content at some point in their lives. This content isn't designed to keep employees engaged, help them retain what they learn, or secure sustainable behavioral change – it only exists as a superficial form of due diligence. Instead of meeting employees' demands for professional development and building a better-educated workforce, too much workplace training alienates and frustrates employees.

One of the most reliable ways to keep employees engaged and help them fully absorb the information they learn is to personalize their educational content. This means content should be customized on the basis of each employee's individual abilities, personality traits, and learning style. Personalized education offers several advantages: it reinforces learners' strengths while identifying and addressing their weaknesses, tailors educational content to different roles and responsibilities within the company, and accounts for behavioral differences.

For example, some employees may be more curious than others, which increases the likelihood that they will click on a corrupt link in a phishing email. Others may be more fearful, which cybercriminals could exploit to coerce them into providing sensitive information or access. When companies focus on these individual characteristics, they will simultaneously provide the individual assistance employees need while capturing their attention with content that's hyper-relevant to their specific circumstances.

Workplace education should never be an imposition

It's common for emails and other prompts about workplace training to include the word "mandatory," along with a demand for employees to complete the course by a specific date. At a time when employees are asking for professional development and educational programs, this is a tremendous wasted opportunity. Ninety-three percent of companies are concerned about employee retention, and the top strategy they're deploying to improve retention is providing learning opportunities. However, if training content is monotonous and disengaging, employees will view it as a chore instead of a benefit.

According to Gallup, around one-in-five employees say they're engaged at work – a situation which has led to huge decreases in morale and productivity around the world. Gallup reports that key elements of engagement include the availability of "opportunities to learn and grow" and the encouragement of employee development. This is yet another reminder that the evidence for the value of workplace education is overwhelming, and it demonstrates that training should never be forced on employees. Rather, training is a mutually beneficial way to help employees pursue their professional aspirations while creating a more capable corporate workforce.

The incentives to develop a personalized and engaging educational platform have never been clearer, and companies should be capable of articulating these incentives to their workforces. By getting all stakeholders on board with your workplace training program, you will ensure that this program leads to long-term behavioral change while increasing employee loyalty and productivity along the way.

About the Author

Asaf Kotsel is the Co-Founder and Chief Executive Officer of Dcoya, a NINJIO subsidiary offering a sophisticated simulated phishing platform that helps cybersecurity leaders identify and address their employee's individual vulnerabilities while tracking organizational risk reduction. With two decades of experience in sales and customer service, Asaf specializes in developing innovative business strategies and leading cross-functional teams to deliver class-leading solutions and enterprise growth.

Asaf can be reached on his LinkedIn page, as well as through the Dcoya website.

8 Tips for Best Results in Red-Teaming

By Zac Amos, Features Editor, ReHack

In cybersecurity, a red team exercise is a unique way to ensure businesses can respond to cyberattacks appropriately. While it’s generally beneficial, taking extra steps can ensure they get the best results.

What Is a Red Team Exercise?

Red-teaming is the practice of using ethical hackers to intentionally attack internal software. The purpose is to see how the company’s cybersecurity — or blue — team would react to a real-world security threat. While it’s similar to a penetration test, no employee has advance notice, targets are variable and the “attackers” test all systems simultaneously.

They use various tools to mimic an attacker’s movements, including system reconnaissance, vulnerability exploitation and data exfiltration. The process provides an organization with a life-like simulation, accurately informing them of potential risk areas. How can businesses get the most out of their red team exercise?

1. Explain Limitations

Businesses should carefully communicate any limitations with the red team before moving forward. Even though they aim to mimic a real-life cyberattack, it's OK to tell them certain areas are off-limits. Even if they don't test some things, the best results are still achievable.

The process could result in file corruption or system downtime if they're not careful, which is why having an in-depth conversation is so important. Everyone needs to clearly and thoroughly discuss what actions are acceptable. It can help them prevent critical errors or data leaks.

2. Identify Goals

The entire red team process is only genuinely useful with proper goal identification. While generally improving security is a good starting point, it's better to be specific. Industry type, hardware and software can help inform it.

Cybersecurity professionals should also consider which security threats are relevant because cybercriminals constantly adapt their approaches. In fact, organizations experienced a 35% increase in the proportion of cyberattack methods and malware types during the pandemic.

Businesses must recognize their security needs and determine how red-teaming can align with them. For example, they could decide to focus on how easily an attacker can access and exfiltrate files. It can help them define their next steps once the process is over.

3. Treat the Process as Training

Even though the red team exercise may seem like a test, businesses should treat it as training. Instead of considering it a pass-or-fail situation, they should view it as a series of learning opportunities. Every internal and external party aware of the process should record successes and failures to identify potential areas of improvement.

Thorough documentation ensures it translates into something actionable. For example, recognizing unusual network activity may take the blue team longer than their employers initially anticipated. Instead of facing punishment, they should learn how to improve. It can help them appreciate the situation and get something valuable out of it.

4. Cover All Attack Surfaces

The red team must have comprehensive knowledge of every attack surface to perform their duties adequately. While a business may only want to consider its most sensitive hardware, cybercriminals can get in through anything. For instance, testing the old servers or storage systems is just as essential.

Threat actors constantly look for better ways to gain access. Although critical systems may have thorough protection, they can still get in if they take advantage of forgotten hardware. Red-teaming is only genuinely successful when it encompasses every possible attack surface.

5. Keep the Exercise Secret

Although the blue team's aim is to defend the business against the red team, they shouldn't be aware of the exercise's existence. The entire point is to simulate a real cyberattack, so they should not know it's coming.

An organization can get more accurate and valuable information about its threat detection and incident response when it keeps the process a secret. Cybersecurity teams that assume any unusual activity is a legitimate concern will respond much more realistically than during a regular penetration test.

6. Recognize the Legal Obligations

Although red-teaming is supposed to simulate an actual cyberattack, certain actions should still be off-limits. Most organizations have a legal duty to protect their customers' details, so they must ensure the team's efforts comply with applicable laws and regulations.

For example, the Payment Card Industry Data Security Standards dictate that organizations must protect customers' financial files or face regulatory action. Other acts cover health records or personally identifiable information. Their relevance depends on the company's location.

Organizations that allow data security testing must ensure everything remains encrypted throughout the process. Alternatively, they could instruct red teams to only act in compliance with regulations. Recognizing legal obligations can protect a company's reputation.

7. Stay Within Policy

A comprehensive red team exercise typically addresses all attack vectors. However, some things may be off-limits. For example, a cloud storage service provider may have specific rules regarding penetration testing. Organizations must inform their vendors of the process or ensure they stay within their policies. It can help them protect their business relationship.

8. Protect Valuable Assets

Creating an asset list is crucial before a red team exercise begins. Businesses take inventory of everything to recognize where they should focus. Also, it can help them identify potential areas of concern. The process can come with risks — like data corruption — so they should take relevant preventive measures.

Although red-teaming only mimics a cyberattack, it can still lead to adverse outcomes. An organization should identify the hardware, software, intellectual property and sensitive information the red team will interact with. It should then create backups of everything.

Get the Best Results

While the red team process is generally smooth and secure, organizations should consider their obligations and goals to ensure they get the best results. The exercise can be incredibly beneficial if they take additional steps beforehand.

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.

Evolving Data Landscape: Rethinking the Privacy-Security Dichotomy in A Data-Centric World

By Ani Chaudhuri, CEO, Dasera

The EU-US Data Privacy Framework is a product of years of painstaking negotiation, a well-intended attempt to tread the tightrope between national security and personal privacy. This balancing act, both intricate and essential, echoes the broader complexities we grapple with in a hyperconnected, data-driven world.

While the framework is laudable on many fronts - providing avenues for EU citizens to challenge perceived infringements by US intelligence agencies and promising that data protections will 'travel with the data' - it may be overly optimistic. A closer examination of the practicalities and underpinnings of this pact raises more questions than it answers. Can we genuinely maintain privacy and security concurrently in an increasingly digital world?

Let's unpack this.

Data has transitioned from an abstract concept to the lifeblood of modern economies, fueling everything from commerce to communication. Without this transatlantic agreement, we would be staring at a chaotic landscape for multinationals that have woven data flows into the very fabric of their operations. Nonetheless, despite its merits, this new framework feels more like a short-term fix, a plaster over a festering wound. It replaces the invalidated Privacy Shield and in doing so, inherits many of its predecessor’s challenges.

The reason is twofold. Firstly, the framework is built on an assumption of trust between EU citizens and American intelligence agencies. It presumes that a complaint-based system, supervised by an independent body, will offer sufficient recourse. But let's question this - how many Europeans will muster the courage to voice their grievances? And among those who do, how many genuinely believe their concerns would be impartially and effectively addressed?

Secondly, the framework glosses over the heart of the matter. It posits the question - as brought up by privacy activist Max Schrems - of whether alterations in US surveillance laws can truly safeguard Europeans' privacy rights. In the current context, my stance is a definitive "no."

But let's dig deeper. We're not grappling merely with a policy issue; we're grappling with a paradigm issue. The EU-US Data Privacy Framework signifies progress, but it stops short of tackling the real elephant in the room - striking the right balance between privacy rights and national security concerns in a world obsessed with data.

We're ensnared in a model that justifies mass data collection and surveillance, forcing us to trade personal privacy for the illusion of security. But isn't it time we reframed the narrative? Isn't it time we challenged the assumption that privacy and security are a zero-sum game?

Technology holds the keys to redefining the privacy-security narrative. Emerging advancements are enabling us to safeguard security without intruding on privacy. This is not an unrealistic aspiration but a palpable possibility in today's rapidly evolving technological landscape.

Consider the potential of technologies that can detect and respond to threats in real-time and learn and adapt to ever-changing risk scenarios. Then there's the promise of homomorphic encryption, a cryptographic method that allows computation on encrypted data, offering unprecedented levels of data protection. Similarly, developments in federated learning allow for data analysis and model training on decentralized networks, thereby ensuring privacy and confidentiality.

Moreover, the rise of privacy-enhancing technologies (PETs) such as differential privacy and zero-knowledge proofs are introducing innovative ways to anonymize data, making it possible to use and share data without compromising the privacy of individuals.

We are at a turning point in the digital age. Technology provides us with new tools and methods to ensure that 'protection travels with the data.' It is more than a lofty ideal - it can be a tangible reality. By leveraging these advancements, we can ensure that as data traverses across borders, our fundamental rights are not left at the checkpoint."

As we navigate the uncharted waters of the digital age, we must rethink our approach to privacy and security. We need to challenge the status quo, question assumptions, and harness the power of technology to ensure that as our data crosses borders, our fundamental rights do too."

About the Author

Ani Chaudhuri is an award-winning executive and entrepreneur with a track record of building successful products, businesses and teams. Ani is driven to bring important solutions to market, and has founded four technology companies to date: eCircle, acquired by Reliance in India; Opelin, acquired by Hewlett-Packard; Whodini, acquired by Declara; and Dasera. Prior to Dasera, Ani worked at McKinsey, HP and Tata Steel.

Ani can be reached online at LinkedIn and at our company website www.dasera.com.

Fend Off the Next Phishing Attack with A "Human Firewall."

Implement the 'Mindset - Skillset - Toolset' triad

By Dr. Yvonne Bernard, CTO, Hornetsecurity

Spear phishing continues to be the most popular cyberattack, and those companies without proper cybersecurity measures are at most risk of being compromised by one. Surprisingly, having proper cybersecurity measures in place may be less common than you think. A recent Hornetsecurity study found that 43% of IT professionals rate their confidence in their remote security measures as "moderate" or "worse". Establishing a sustainable safety culture is a must to prevent future attacks as cyber hacking methods become more advanced.

How hackers are using AI to their advantage

The introduction of generative AI has given hackers the opportunity to automate and simplify their process of creating spear phishing attacks. With these AI tools, malicious actors only require a few pieces of information, such as personal or professional email addresses or phone numbers. The AI will then sift through social media and the Internet to find additional information, such as a job title, community affiliations, etc.

Using this data, hackers can tailor spear phishing emails to the individual, have them automatically generated and quickly sent, while simultaneously dispatching different versions to multiple target victims. As a next step, threat actors can then use Generative AI to quickly adapt and optimize their messages based on success rates, with little effort.

A "human firewall" is your best defense

The best line of defense for companies to combat cyberattacks is to establish a sustainable security culture. This includes having a "human firewall" – meaning employees have been trained to be well-versed to recognize potential cyberattacks. To help implement these preventative measures, companies need to utilize the "Mindset - Skillset - Toolset" triad.

Mindset: Raise the cybersecurity awareness of employees. Although IT tools are helpful, blind trust in them may lead to not properly vetting potential phishing attacks and email traffic.

Skillset: Combine theory and simulation to educate employees on cyberattack methods and realistic phishing simulations. Paired with general knowledge, these simulated attacks will help strengthen their understanding of phishing emails and how to identify them.

Toolset: Install tools and implement processes to thwart potential attacks and strengthen employees' security behavior. These tools will help identify attacks and encourage safe habits.

Choose the right amount of cybersecurity knowledge to share

As cyberattacks become more sophisticated, IT managers have many tools, methods, and programs to train their employees to fight against them and to enhance good cybersecurity habits. It is imperative to train employees on these potential risks, but companies must be careful to not overwhelm them with information or training – for example, employees should not be required to know in detail about endpoint detection software, digital firewalls, or network monitoring tools – which may lead to defensiveness and resistance.

What employees need to be familiar with are the knowledge and tools they will use on a daily basis. This includes educating the team on how to identify and report suspicious emails, understanding proper password management, and implementing multi-factor authentication (MFA).

Good password hygiene is one area that is crucial yet often overlooked, so it is important to build a culture that implements best practices and security habits. Employees should create a unique password for each of their digital accounts and applications, as well as turn on MFA where possible for an added layer of security.

Another important habit employees should add to their daily routine is checking emails for authenticity from the moment they read them. This allows them to not be pressured to engage with different phishing emails, even during stressful situations. If an email seems questionable and suspicious, reporting the incident to the IT security department will allow them to address the situation and confirm whether it is a potential cyberattack.

Security-awareness training is the foundation to your organization's cybersecurity

Companies that focus on security-awareness training are setting themselves up to successfully combat cyberattacks. Establishing a "human firewall" will increase employees' abilities to assess potential threats and thwart them from the get-go. IT managers need to stay vigilant in upskilling their company employees with new, easy-to-use, up-to-date tools and more sophisticated phishing attacks to ensure their systems will not get compromised due to preventable human error. These actions will help your employees stay ahead of hackers, and keep your organization safe even as cyberattacks become increasingly sophisticated amid the ever-changing digital environment.

About the Author

Dr. Yvonne Bernard is CTO at Hornetsecurity, the global Cloud Security, Compliance and Backup pioneer founded in Hannover, Germany. With a Ph.D. in Computer Science, she has a technical background and is responsible for strategic and technical development in the areas of Product Management, Software Development, Innovation & Research, Security Lab and Cloud Infrastructure. Learn more at https://www.hornetsecurity.com

4 Secure Framework Considerations Before Deploying Workloads in The Public Cloud

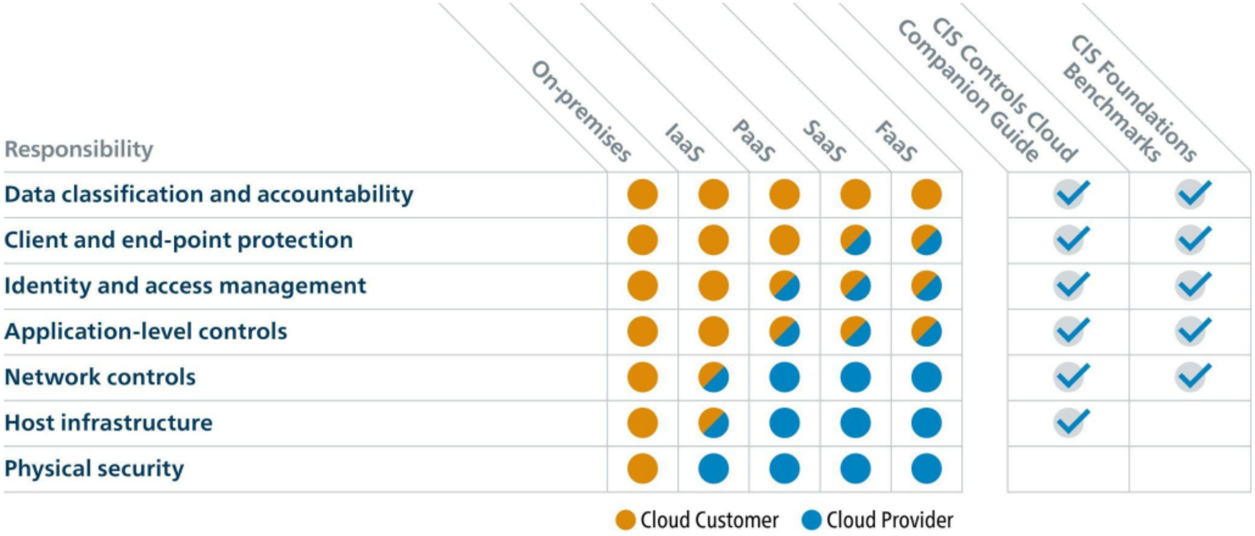
By Jhilam Biswas, Customer Engineering Manager, Google Cloud

Enterprises are adopting public cloud providers like never before. Gartner estimated the global forecasted spend on public cloud services to grow by 20% from 2022. Enterprises adopt cloud for several reasons - a couple of them being pay-as-you-go flexible pricing models and scalability. However, when moving infrastructure to the cloud - be it core compute services, serverless technologies, databases, analytics stack etc., security is often left as an afterthought. The repercussions of that mindset are huge, sometimes leading to significant financial losses, irreversible damages and a negative impact on the enterprise's brand image. Hence moving to the cloud requires a thorough evaluation of potential risks, compliance obligations and assessment of your business requirements. A recent Gartner report calls out "Through 2025, 99% of cloud security failures will be the customer's fault." In this article, we'll cover 4 secure framework considerations that an enterprise should absolutely be considering before making the move to the cloud.

1. Review Shared Responsibility Matrix in the Public Cloud

It is important to clearly understand the shared responsibility model when you think about securing workloads in the cloud. The shared responsibility matrix is a consolidated framework that categorizes the security and compliance responsibilities of public cloud providers and customers of the cloud provider. At a high-level, the cloud provider is responsible for the physical security of the core cloud infrastructure, including the data centers, networks, and hardware and the customer is responsible for securing their data and applications, including configuration of access control and data encryption.

What is extremely critical to bear in mind is that nobody knows the security and compliance requirements for your business better than you, and so before you run your workloads in the cloud, you must identify the security guardrails that you need to protect your proprietary data and adhere to regulatory requirements deemed by the industry you operate in. The following diagram shows how responsibilities are shared between the cloud provider and customer.



Responsibility	On-premises	IaaS	PaaS	SaaS	FaaS	CIS Controls Cloud Companion Guide	CIS Foundations Benchmarks
Data classification and accountability	🟠	🟠	🟠	🟠	🟠	✓	✓
Client and end-point protection	🟠	🟠	🟠	🟠🔵	🟠🔵	✓	✓
Identity and access management	🟠	🟠	🟠🔵	🟠🔵	🟠🔵	✓	✓
Application-level controls	🟠	🟠	🟠🔵	🟠🔵	🟠🔵	✓	✓
Network controls	🟠	🟠🔵	🔵	🔵	🔵	✓	✓
Host infrastructure	🟠	🟠🔵	🔵	🔵	🔵	✓	
Physical security	🟠	🔵	🔵	🔵	🔵		

🟠 Cloud Customer 🔵 Cloud Provider

Image Source:

https://www.cisecurity.org/insights/blog/shared-responsibility-cloud-security-what-you-need-to-know

2. Identify Risks to Your Organization

Risk assessment is a prudent ongoing process of methodically identifying, evaluating, and mitigating risks to an organization's assets. It is a process that should be repeated and conducted regularly as your organization's assets and risks change. Before you move workloads to the cloud, it is imperative to complete a risk assessment to determine what security features you need to meet your internal security requirements and external regulatory requirements. It is important to involve all stakeholders in the risk assessment process, including your cybersecurity teams, IT, and business users. Various risk assessment frameworks such as the Cloud Security Alliance's Cloud Controls Matrix (CCM) are widely used across industries. After you have identified your risks using such frameworks, you need to determine how to address them. This may involve accepting, avoiding, transferring, or mitigating the risks. You can choose to mitigate risks either using technical controls such as using built-in cloud native features or contractual protections such as ISO or SOC 2/3 certifications that the cloud provider commits to undergo periodically. The results of the risk assessment should be documented thoroughly and should form the basis of your security readiness in the cloud.

3. Assess Your Compliance Obligations

When you think of your compliance requirements in the cloud, they are dependent on a variety of critical factors such as:

- The laws and regulations that are tied to your organization's and your customers' physical locations (Example: GDPR in the European Union)
- Your regulatory requirements of the industry that you operate in (Example: HIPAA for healthcare and life sciences)
- The type of data you store and process in the cloud (Example PII data)
- The cloud services you use (Example: are the managed cloud offerings that you intend to use for your workloads covered under HIPAA?)

The responses to the above questions dictate which security controls you need to implement for your workloads in the public cloud. A typical compliance journey goes through three stages: assessment, gap remediation, and regular monitoring to check adherence to compliance standards. A comprehensive compliance assessment involves a detailed review of all your mandatory regulatory obligations and how your organization is currently putting it to practice. Once you have a clear understanding of your current state, you can begin to identify any gaps between your requirements and your current practices. The next step of remediating those gaps involves implementing the latest security controls and updating your existing policies that are outdated. The final stage of the compliance journey is continual monitoring. This step is important to ensure your organization is up-to-date with changing regulations. To adhere to compliance even amidst changing regulations, you should consider automating your cloud infrastructure security policies by incorporating them into your infrastructure as code (IaC) deployments. You could also use a cloud compliance management platform to help you track your compliance posture and identify any gaps and last but not the least, stay up-to-date on the latest regulatory changes.

4. Understand Your Privacy Requirements and Build a Robust Plan to Adhere To Those

Privacy requirements of your organization are dictated by how you acquire, process and store data - both of your internal users and that of your external clients. As the organization grows, building a robust set of security controls to ensure privacy becomes increasingly complex and it might seem like a daunting task to keep up with the changes. However, a methodical and well-thought framework will help you to adhere to the privacy requirements of your organization. Below are several approaches to think about when considering privacy requirements:

- Define ‘Confidential/Sensitive Data’ as it pertains to your organization: For example, this could be PII information such as SSN, home address, email etc. Classifying this data will help you identify what needs to be protected most carefully. Once identified, consider approaches such as tokenizing, obscuring or de-identifying PII data even to folks within your organization
- Lock down access to sensitive data: Use identity and access management controls to implement ‘least privilege’ and limit access to sensitive data. Use tools for audit trails to get granular insights on who in the organization accessed what type of data and use that information to further restrict access if the controls are over provisioned.
- Monitor for phishing attacks: Phishing attacks via email are the most common attack mechanisms for fraud and malware. Ensure you have the necessary protection systems in your email servers to limit the attack servers. SaaS email systems such as Gmail have advanced protection mechanisms against phishing built-in.
- Extend zero trust security in your organization: The traditional approach to cybersecurity is based on the idea of a perimeter. This means that organizations build a perimeter around their networks and then try to keep unauthorized bad actors out. With the rise of remote work and cloud computing, it is no longer possible to simply keep everyone out of the network and protection simply based on a perimeter model is outdated. Zero trust security takes a novel approach to the “keep the bad actors out” problem. In a layered zero trust model, the concept of perimeter ceases to exist and no one is trusted implicitly. This means that every access request needs to be passed at several levels of checks such as device identity, user identity etc. before the request can make its way all the way to the resource that it has seeked access to. For example, you could use Google Cloud’s out of the box BeyondCorp solution that helps enterprises implement zero-trust at-scale.

After you have done the due diligence of doing a thorough analysis of the 4 secure framework considerations as called out above, you can confidently say that you are ready to deploy your workload in the cloud. Depending on what kind of workload you intend to run in the cloud - such as analytics, managed Kubernetes, serverless, databases etc., the next step is to deep-dive into the security features of the specific cloud native services that you are planning on using for your workload. Specifically, the three key areas where you want to focus next are - application/infrastructure security, network security and finally data security (at-rest, in transit and while processing) Last but not the least, consider using a logging and detection tool and a centralized monitoring platform which will help you to quickly view all your threats and vulnerabilities in a single place and take actions on them immediately before you incur a potential attack that can tarnish your organization’s reputation.

About the Author

Jhilam Biswas is an experienced cybersecurity professional with over 9 years of experience in cloud computing and security. She's currently a Customer Engineering Manager at Google Cloud helping strategic digital native clients to deploy and scale securely in the cloud. Before Google, she has worn many security hats in different F500 companies such as Security Solutions Architect at Akamai and Security Engineer at Cisco. She earned her MS Degree from the University of Maryland at College Park with a focus on cloud computing and network security. Jhilam can be reached online at https://www.linkedin.com/in/jhilambiswas/ and at our company website https://cloud.google.com/

Increase in Phishing Threats among Organizations Has Created a Lot of Opportunities for the Cyber Security Industry

By Koyal Ghosh, Senior Writer, Allied Market Reasearch

Growing trend of BYOD and smart assimilation of machine learning, IoT, and AI in several projects have heightened the need for cyber security in more than one way. The cybersecurity bionetwork takes in a number of regional clusters of cyber haven organizations that account for the global market dynamics. In the present market scenario, the sector operates in three discrete mega-clusters namely Israel, SFBA (the San Francisco Bay Area), and Metropolitan Washington, DC.

Israel and the San Francisco Bay Area come up with flourishing startup ecologies with a considerable associated flow of risk capital and are deeply concentrated on products, while Washington showcases a greater proportion of service-based companies.

A number of studies and surveys have been conducted in this domain and it's revealed that one of the prime causes of growing cyber attacks is nothing the dearth of proficient cybersecurity recruits in the majority of sectors. The number of skilled, adept, and expert cybersecurity specialists, especially in Middle-East, Europe, and Asia-Pacific, are moderately low as opposed to the need for security mavens required to control cyber threats for government offices, industrial units, and financial organizations. This is the reason why there's been a sturdy increase in demand for cloud based cyber solutions as well as strong authentication processes, which has been highly beneficial for the cyber security market.

The Covid-19 Pandemic Has Had a Positive Impact on the Market

The outbreak of the Covid-19 pandemic, on the other hand, had made most countries worldwide implement strict precautionary measures. With the academic institutions being shut and people asked to follow stay-at-home dictums, multiple organizations had found certain ways to enable their resources to work from their homes. This, eventually, entailed toward a sturdy rise in the implementation of video communication boards, which in turn has paved the way for an array of opportunities for the key players in the industry.

Moreover, there are also case where ransomware attacks have been seen to wreak havoc on many local as well as public sector agencies. In few cases, the local governments were obligated to announce a state of emergency owing to huge leaks of subtle & delicate data. As for example, in June 2021, one of the prominent names in the meatpacking industry, JBS Foods confirmed that it had paid around eleven million dollars to REvil ransomware threat actors in the wake of a cyberattack that compelled the firm to shut down its production activities at multiple sites across the world. Such incidents have heightened the importance of cyber security even more. Furthermore, the arrival of 5G is projected to accelerate the use of connected expedients in industries already jolting toward Industrial Revolution 4.0. This has supplemented the market growth even more. M2M connections, at the same time, have also been influential in fuelling the market tow. According to Allied Market Research, the global cyber security market is anticipated to showcase a prominent CAGR from 2021 to 2030.

Considerable surge in the number of maneuvers connected to the internet, the cyber sector is quite naturally projected to experience an increase in the incidence of new attacks and threats. The attacks of Petya and WannaCry, which distressed more than one-fifty countries across the world, further exposed

the susceptibility of IoT maneuvers as end-points, thereby, propelling the need for improved security for consumer policies that are highly vulnerable to cyberattacks.

Cybersecurity Solutions Are Now in Huge Demand

Additionally, security academics and scholars working in Palo Alto Networks revealed another Mirai malware variation that targeted new exposures associated with Internet of Things. Investigators and scientists from Unit 42 exposed several threats in the first quarter of 2021 that facilitated vulnerabilities. In this context, the compromised expedients downloaded Mirai trojan and spyware binaries, which incorporated them to a bigger IoT buf capable of executing network spasms on devastating measures. Such liabilities are projected to boost the demand for cybersecurity solutions in several ways.

Impeccably connected vehicles are expected to be the future of the automobile sector. Nonetheless, this connectivity is also anticipated to make them pretty susceptible to cyberattacks.

One of the prominent names in the automobile component sector in India, namely Steelbird International is regarding automotive cybersecurity to map out its next chapter of growth. Started as a two-wheeler sieve manufacturing venture in the year 1964, the company has come a long way to come up as the leader in the automobile sector by taking along lubricants, rubbers, and bearings into its product range.

Conclusion

In the recent years, the concept of Zero Trust has turned out to be quite prevalent among the IT leaders, especially in the turf of cybersecurity. A lot of companies have already started providing solutions pertaining to the Zero Trust model. With such elucidations readily accessible, the term is being utilized so slackly that it often becomes tough for IT professionals to realize what the notion is really about. Zero Trust is pertinent for establishments of all sizes.

To sum up, the global cyber security market is growing at a rapid pace and with its growing demand on board, it’s expected that the market would flourish even more in the next few years.

About the Author

Koyel Ghosh is a blogger with a strong passion and enjoys writing on miscellaneous domains, as she believes it lets her explore a wide variety of niches. She has an innate interest for creativity and enjoys experimenting with different writing styles. A writer who never stops imagining, she has been serving the corporate industry for the last four years. koyel.ghosh@alliedmarketresearch.net

https://www.linkedin.com/in/koyel-ghosh/

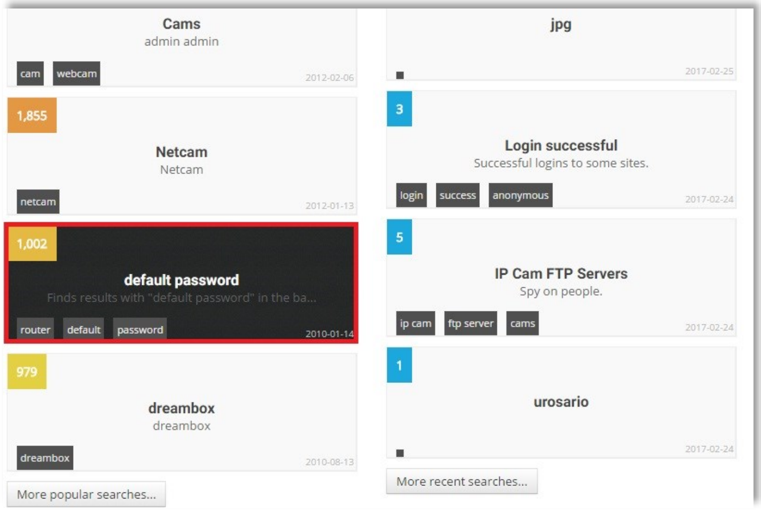
How Hacking of The Internet of Things Works in Practice

By Milica D. Djekic

The Internet of Things (IoT) represents a collection of devices being capable to talk to each other using the internet as a communication channel. As it's obvious – the IoT is a cyber as anything else today. That means such a technology could get vulnerable to hacker's attacks and for such a reason it's important to apply the good procedures and practices in order to prevent your IoT assets from cyber incidents. Through this chapter – we intend to discuss how hacking of the IoT infrastructure works in practice as well as provide some empirical examples how such a campaign could get conducted in a reality.

How we could obtain login details

Before anyone makes a decision to begin the hacker's operation, he should try to think which information he got available as well as which tools he has. In many cases, it's so important to adjust your hacking tool's needs with the information being necessary for conducting a cyber campaign. The role of this learning material's chapter is provide a closer look at some of the hacking techniques as well as a usage of cyber technologies in threatening the IoT resources. For the purpose of a good explanation of this strategy – we would use the Shodan tool that got provided some Default Passwords which could assist you in breaking into someone's system. It's well known that crawlers like Shodan and Censys could offer an opportunity to get anyone's IP address and if there is no or poor authentication – anyone could make a breach or take advantage over weaknesses of that IT infrastructure. In Figure 1, we would want to show step-by-step how a Shodan could serve in obtaining so valuable login information. The illustration is given as follows.



Cams
admin admin
cam webcam 2012-02-06

1,855
Netcam
Netcam
netcam 2012-01-13

1,002
default password
Finds results with "default password" in the ba...
router default password 2010-01-14

979
dreambox
dreambox
dreambox 2010-08-13

More popular searches...

jpg
2017-02-25

3
Login successful
Successful logins to some sites.
login success anonymous 2017-02-24

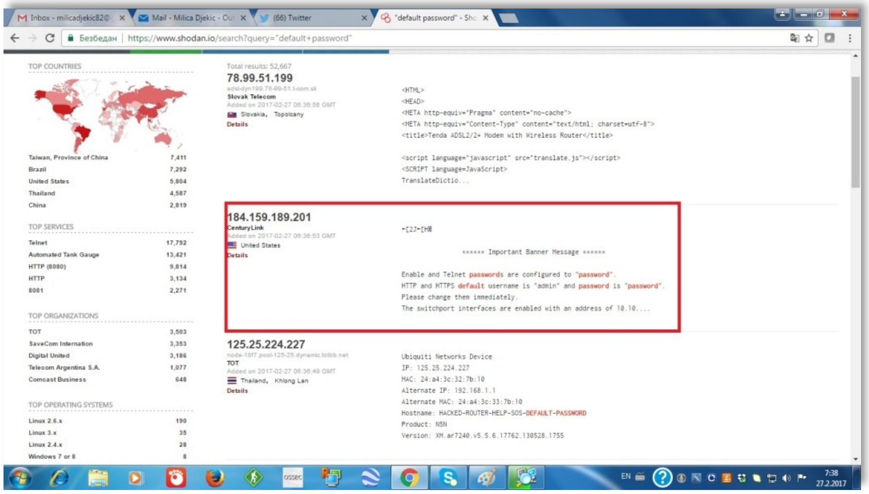
5
IP Cam FTP Servers
Spy on people.
ip cam ftp server cams 2017-02-24

1
urosario
2017-02-24

More recent searches...

Figure 1. The Shodan's default passwords

As it's illustrated in the previous Figure – the Shodan would deal with many different IoT resources and one of the options would be – so called – Default Password. As it's obvious – there would be around 1,000 devices getting its login details available to the rest of a web population. We would always highlight that a primary role of the Shodan is to serve to research's community, but – unluckily – many malicious actors would find their interest to exploit such an asset. Indeed, the Shodan is a powerful tool offering a chance to everyone to test its capacities. Through the Figure 2 – we would illustrate how such a Default Password section could get used for getting the IP details as well as the authentication data. That step is illustrated as follows.



TOP COUNTIES

Taiwan, Province of China	7,411
Brazil	7,292
United States	5,804
Thailand	4,587
China	2,819

TOP SERVICES

Telnet	17,792
Automated Tank Gauge	13,421
HTTP (8080)	9,814
HTTP	3,134
8081	2,271

TOP ORGANIZATIONS

TOT	3,503
SaveCom Internation	3,353
Digital United	3,186
Telecom Argentina S.A.	1,077
Comcast Business	648

TOP OPERATING SYSTEMS

Linux 2.6.x	190
Linux 3.x	35
Linux 2.4.x	28
Windows 7 or 8	8

Total results: 52,667

78.99.51.199
adsl-dyn199.78-99-51.t-com.sk
Slovak Telecom
Added on 2017-02-27 06:36:56 GMT
Slovakia, Topolcany
Details

```
<HTML>
<HEAD>
<META http-equiv="Pragma" content="no-cache">
<META http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>Tenda ADSL2/2+ Modem with Wireless Router</title>

<script language="javascript" src="translate.js"></script>
<SCRIPT language=JavaScript>
TranslateDictio...
```

184.159.189.201
CenturyLink
Added on 2017-02-27 06:36:53 GMT
United States
Details

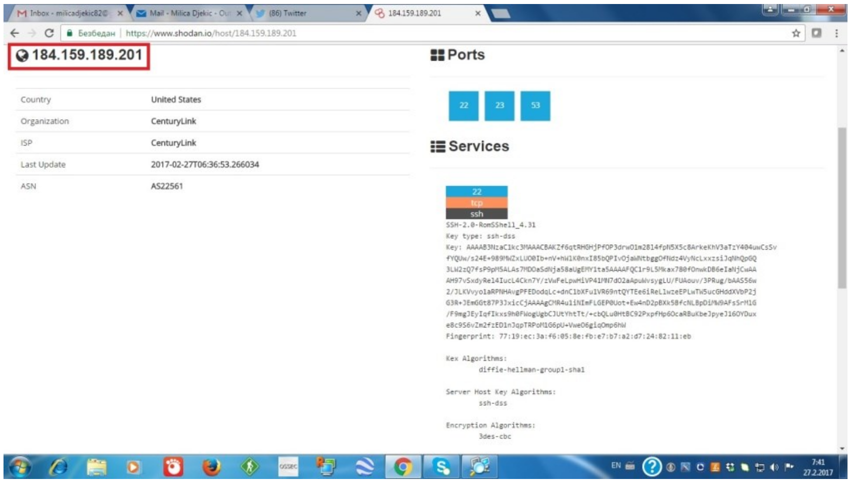
```
←[2J←[H

             ****** Important Banner Message ******

Enable and Telnet passwords are configured to "password".
HTTP and HTTPS default username is "admin" and password is "password".
Please change them immediately.
The switchport interfaces are enabled with an address of 10.10....
```

125.25.224.227
node-18f7.pool-125-25.dynamic.totbb.net
TOT
Added on 2017-02-27 06:36:49 GMT
Thailand, Khlong Lan
Details

```
Ubiquiti Networks Device
IP: 125.25.224.227
MAC: 24:a4:3c:32:7b:10
Alternate IP: 192.168.1.1
Alternate MAC: 24:a4:3c:33:7b:10
Hostname: HACKED-ROUTER-HELP-SOS-DEFAULT-PASSWORD
Product: N5N
Version: XM.ar7240.v5.5.6.17762.130528.1755
```

Figure 2. The Shodan's login details

As it's given through the Figure 2 – we would select some US IP address offering the login details such as username and password to that IoT configuration. The username here would be 'admin' and the password would get 'password'. In addition, through this book's chapter – we would like to deal with some of the widely used hacker's tools that would get analyzed further through this chapter. At this stage – it's significant to know that for a successful hacking – it's necessary to get familiar with someone's IP address as well as his login details. Through the Figure 3, we would illustrate some of this Shodan's results being covered with more details on.



184.159.189.201

Country	United States
Organization	CenturyLink
ISP	CenturyLink
Last Update	2017-02-27T06:36:53.266034
ASN	AS22561

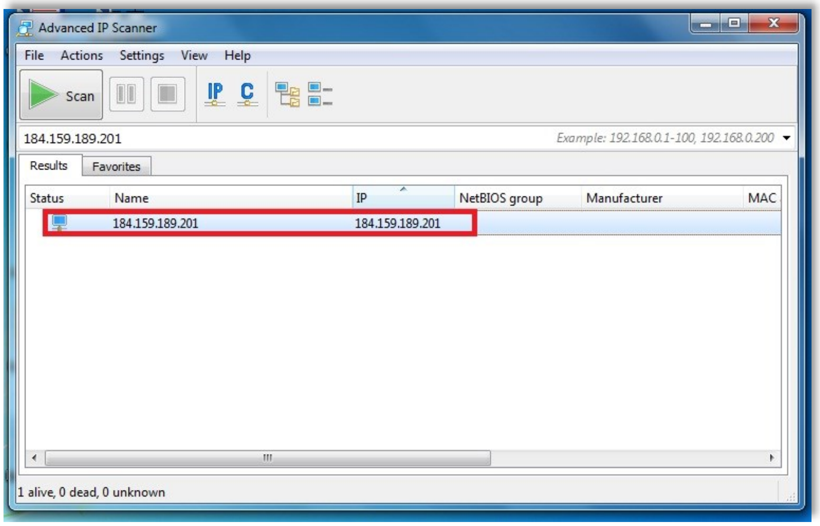
```
SSH-2.0-RomSShell_4.31
Key type: ssh-dss
Key: AAAAB3NzaC1kc3MAAACBAKZf6qtRHGHjPfOP3drwO1m2814fpN5X5c8ArkeKhV3aTzY404uwCsSv
fYQUw/s24E+989MWZxLUO0Ib+nV+hW1K0nxI85bQPIvOjaWNtbggOfNdz4VyNcLxxzsiJqNhQpGQ
3LW2zQ7fsP9pM5ALAs7MDOaSdNja58aUgEMY1taSAAAAFQC1r9L5Mkax780fOnwkDB6eIaNjCwAA
AH97vSxdyRel4IucL4Ckn7Y/zVwFeLpwHiVP41MN7dO2aApuWvsygLU/FUAouv/3PRug/bAAS56w
2/JLKVvyo1aRPNHAvgPFEDodqLc+dnC1bXFu1VR69ntQYTEe6iReL1wzeEPLwTW5ucGHddXVbP2j
G3R+JEmGGt87P3JxicCjAAAAgCMR4u1iNImFLGEP0Uot+Ew4nD2pBXk58fcNLBpDiMW9AFsSrM1G
/F9mgJEyIqfIkxs9h0FWogUgbCJUtYhtTt/+cbQLu0HtBC92PxpfHp6OcaRBuKbeJpyeJ16OYDux
e8c9S6vZm2fzED1nJqpTRPoM1G6pU+VweO6giqOmp6hW
Fingerprint: 77:19:ec:3a:f6:05:8e:fb:e7:b7:a2:d7:24:82:11:eb

Kex Algorithms:
	diffie-hellman-group1-sha1

Server Host Key Algorithms:
	ssh-dss

Encryption Algorithms:
	3des-cbc
```

Figure 3. The Shodan's result details

As it's clear – any researcher could analyze some of the Shodan's results trying to figure out how those results could cope with the real-case scenarios. So, what it's important at this stage are the facts that we got a desired IP address being 184.159.189.201 and some login details being 'admin' for a username and 'password' for password. It's important to mention that unbelievably many IoT assets would use a weak authentication and the hackers would through simple guessing obtain an access to someone's computer or another device being online. Through the coming section of this learning material – we would talk a bit more about some standard hacking tools and try to explain the way of their usage for the system's exploitation. At this stage, we would end up this part of the book's chapter with well-known sentence that following of the best practice could save us greatly from unwanted events.

How hacking works in practice

Some of the best known hacking tools are Advanced IP Scanner and Radmin being used to search the network and take a remote control over the targeted devices. These two applications could get in combination or separately, but we would always advise the users to try to combine the both of them. These tools are free of charge and could get downloaded from the internet. The role of the Advanced IP Scanner is to offer some results about a required IP address as well as attempt to do deeper into a network trying to do some penetration of that infrastructure. On the other hands, the Radmin could get considered as a gadget to the Advanced IP Scanner that could offer us an opportunity to take control over any available device. In Figure 4, we would try to deal with such a tool using the well-known IP address of US IoT asset that we found using the Shodan crawler. This illustration is given as follows.



184.159.189.201

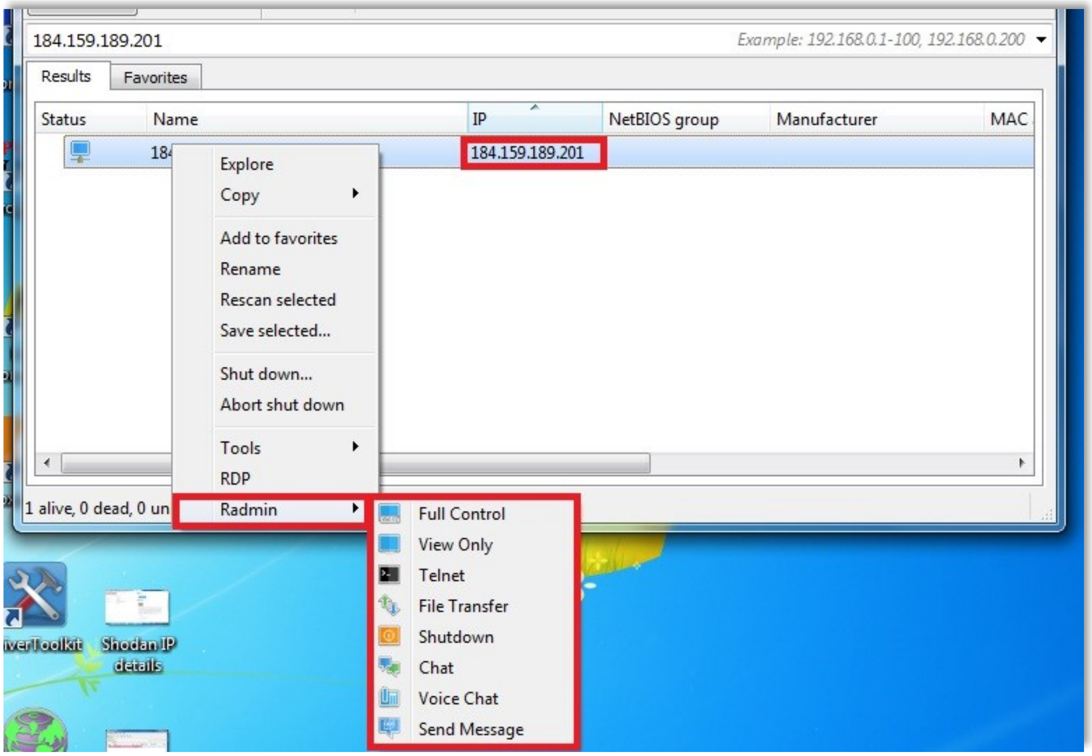
Example: 192.168.0.1-100, 192.168.0.200

Status	Name	IP	NetBIOS group	Manufacturer	MAC
	184.159.189.201	184.159.189.201			

1 alive, 0 dead, 0 unknown

Figure 4. The Advanced IP Scanner with the crawled IP address

As it’s obvious – the Advanced IP Scanner would get the required IP address and make a search trying to identify such a device. We would get an IT asset being visible through this scanning tool. As we suggested – this tool would deal with the remote administration options using the Radmin software. The Figure 5 would illustrate how it works in practice and how it’s possible to hack someone’s IoT asset. Through such an illustration – we would notice that many of scenarios are feasible and also see that making a cyber breach or stealing the confidential information could get a piece of cake to any hacker. In this case, it’s not about the skill because the children would know how to use those tools – it’s more about money which would make someone commit a cybercrime and gets exposed to a risk for a reason that he would leave a trace in a cyberspace anyhow. Such a finding could make an investigation being much easier and increase the chance that such a case would lead to an arrest.



184.159.189.201

Example: 192.168.0.1-100, 192.168.0.200

Status	Name	IP	NetBIOS group	Manufacturer	MAC
	18	184.159.189.201			

1 alive, 0 dead, 0 un

Figure 5. The remote options of an Advanced IP Scanner

As it's illustrated in Figure 5, the Radmin alternative would offer us many possibilities such as full control, view only, shutdown, chat and so on. Choosing one of these options – you would get an opportunity to login to someone's computer. In this case, such a device would be an IoT asset being found through the Shodan's crawler. Finally, all you need is to connect to such a device and apply some of the command being given above. The rest of a job is just a piece of cake!

The ways of cyber prevention

Through this learning material, we would talk a bit more about how these sorts of scenarios could get prevented in a practice. As we would suggest many times – it's so useful to follow the best practice. In case of preventing the device to get accessible through some of the scariest searching tools – it's so helpful to try to block your inbound ports as well as use the strong authentication which would offer you much better protection. Also, it could get convenient if you would change the passwords to your system periodically as well as apply more firewall's options and regularly update your network's devices such as modems and routers. Finally, this chapter would illustrate us how it's possible and we must say – easy – to hack someone's computer, so that's a reason more to invest into your cyber defense either in private life or at the work.

The final talk

Through this chapter – we would see how our IoT asset would get vulnerable to some of the hacker's operations. Unluckily to all of us – many critical infrastructures would belong to IoT capacities and those assets could get attacked so easily. In conclusion, we would want to say that the entire expert's community should work so hard in order to prevent some of these incidents even happen as well as aware people how to help themselves in such a sort of dealing with the threats, risks and challenges.

References:

[1] Djekic, M. D., 2017. The Internet of Things: Concept, Application and Security. LAP LAMBERT Academic Publishing.

[2] Djekic, M. D., 2021. The Digital Technology Insight. Cyber Security Magazine

[3] Djekic, M. D., 2021. Smart Technological Landscape. Cyber Security Magazine

[4] Djekic, M. D., 2021. Biometrics Cyber Security. Cyber Security Magazine

[5] Djekic, M. D., 2020. Detecting an Insider Threat. Cyber Security Magazine

[6] Djekic, M. D., 2021. Communication Streaming Challenges. Cyber Defense Magazine

[7] Djekic, M. D., 2021. Channelling as a Challenge. Cyber Defense Magazine

[8] Djekic, M. D., 2021. Offense Sharing Activities in Criminal Justice Case. Cyber Defense Magazine

[9] Djekic, M. 2019. The Informant Task. Asia-Pacific Security Magazine

[10] Djekic, M. D., 2020. The Importance of Communication in Investigations. International Security Journal

[11] Djekic, M. D. 2019. The Purpose of Neural Networks in Cryptography, Cyber Defense Magazine

[12] Djekic, M. D. 2020. Artificial Intelligence-driven Situational Awareness, Cyber Defense Magazine

[13] Djekic, M. D. 2019. The Perspectives of the 5th Industrial Revolution, Cyber Defense Magazine

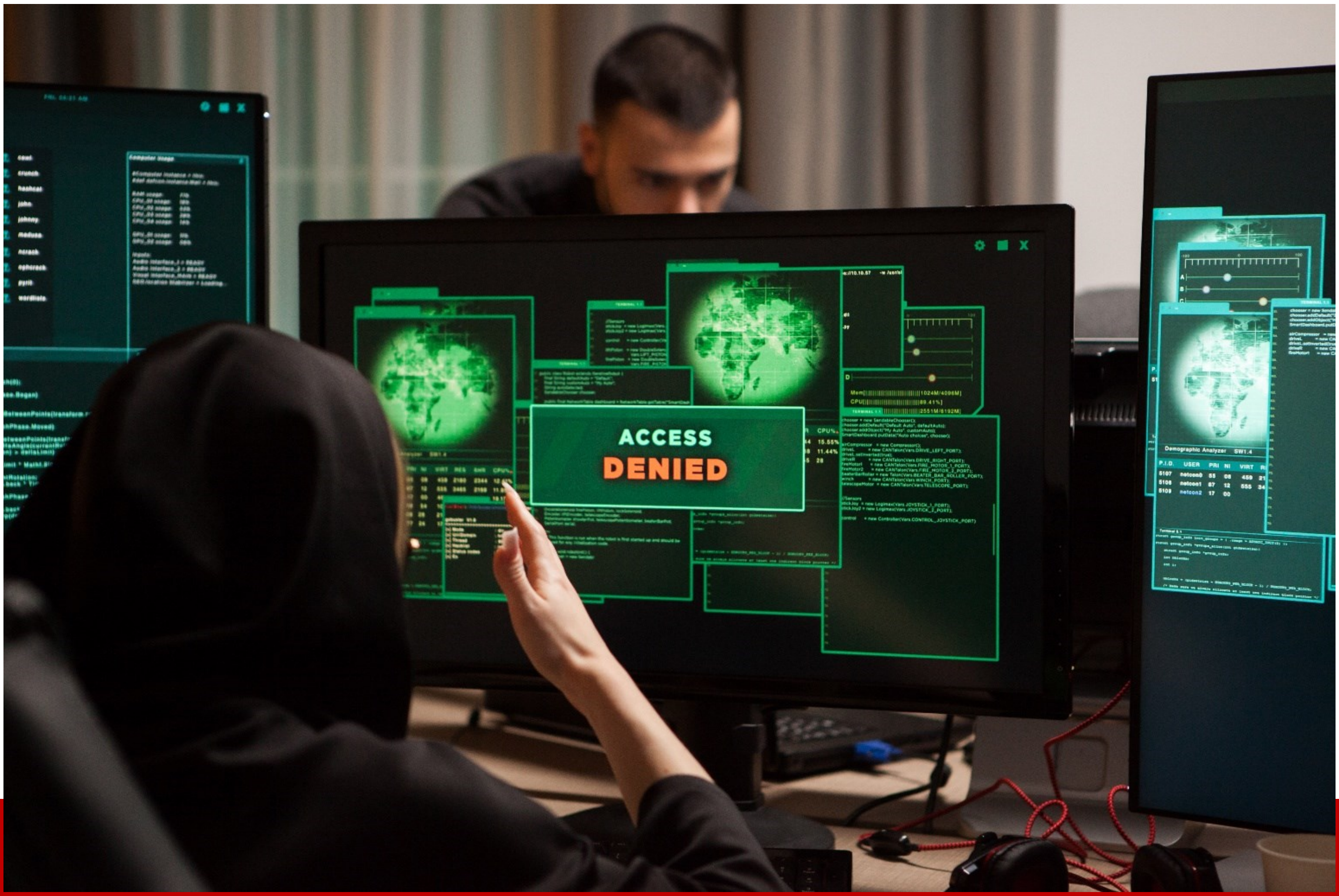
[14] Djekic, M. D. 2019. The Email Security Challenges, Cyber Defense Magazine

[15] Djekic, M. D. 2016. The ESIS Encryption Law, Cyber Defense Magazine

[16] Đekić, M. D., 2021. The Insider's Threats: Operational, Tactical and Strategic Perspective. LAP LAMBERT Academic Publishing.

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.



MOVEit's Ransomware Attack Highlights the State of Cybersecurity

By Ben Smith, Field Chief Technology Officer, NetWitness

Vulnerability is a four-letter word in the world of cybersecurity, as one leading business application vendor learned the hard way in May. The company's managed file transfer (MFT) software, MOVEit, experienced a sizable attack orchestrated by the Russian ransomware group, CL0P.

According to the victimized company, the gap in security had the potential to allow unauthorized users access and privileges to the software, and the supply chain attack against MOVEit impacted many of its own downstream customers, including other companies in the payroll services and identity theft verticals, as well as several government agencies. In recent years, supply chain attacks have become more prevalent as threat actors have evolved to extract even more value from personal data, especially when 80% of companies disrupted by ransomware wound up paying the ransom. This is a profitable exercise, because after all, cybercrime is a business and has its own business models.

The Business of Cybercrime

When you think about cybercrime, you really should think of it like you would any other business. CL0P is best known as a “ransomware-as-a-service” provider, helping other threat actors create and deploy their own ransomware campaigns. The end goal is almost always money, and in MOVEit’s case, CL0P sought an undisclosed amount of money to prevent the distribution of the victim organization’s private data. And like any growing business, CL0P has diversified its offerings to include complementary capabilities such as access to a dedicated botnet as well as direct access to compromised networks as a means to mint future victims (and revenue).

Every action a threat actor like CL0P carries out is intentional, including widely publicizing and threatening the potential disclosure of the sensitive information it now controls through its ransomware capability. The group’s intention is to create additional urgency in the hopes of forcing the affected company to act quickly or suffer further embarrassment or even operational impact as more details are released.

Mitigating Ransomware Attacks

It’s no easy feat to protect a supply chain against determined threat actors who own a growing toolbox of potential weapons, including ransomware. These threat actors may even work harder than vendors to identify and leverage zero-day vulnerabilities, because your data is their payday. In a sense, companies need to take a cue from groups like CL0P and understand how these cybercrime enterprises operate.

Since most attackers rely heavily on their own supply chains, one of the best defenses is to seek, understand, and document potential bottlenecks in these adversarial supply chains - this information represents low-hanging fruit where you (or the managed security provider who protects you) can gain the biggest bang for the buck. For example, how does a typical ransomware attack arrive into a victim’s environment? How does an infected laptop communicate back to the threat actor with its status? How does a threat actor ultimately monetize its efforts? These are all questions that may be addressed with skill sets on your extended team like threat intelligence and incident response, and technology solutions such as network-based threat detection and response. To disrupt this chain, one needs to hone in on the adversary’s business model and use it against them, much as we see in the martial art of jiu-jitsu.

Unfortunately for many companies, the approach after a ransomware attack is to focus on the primary vulnerability, remedy it, and then go back to business as usual. In the case of MOVEit, there were new and previously unannounced vulnerabilities still being announced more than six weeks after the first vulnerability’s public announcement. It’s critical that affected companies remain proactive; where there is one vulnerability, there are frequently others.

While companies should move forward with improved security measures to enhance the documentation, monitoring and protection of their own supply chains, enlisting external help is almost always a suitable option. Not only can these externally-based defenders help respond to or even prevent ransomware attacks, they may also be explicitly involved in the takedown of threat actors. In January 2023, the U.S. Department of Justice announced it had disrupted the actions of the ransomware-as-a-service group Hive, which had targeted more than 1,500 victims. The disruption indicates that these groups aren’t infallible, and with the right defenses and knowledgeable defenders, those adversarial supply chains can be disrupted.

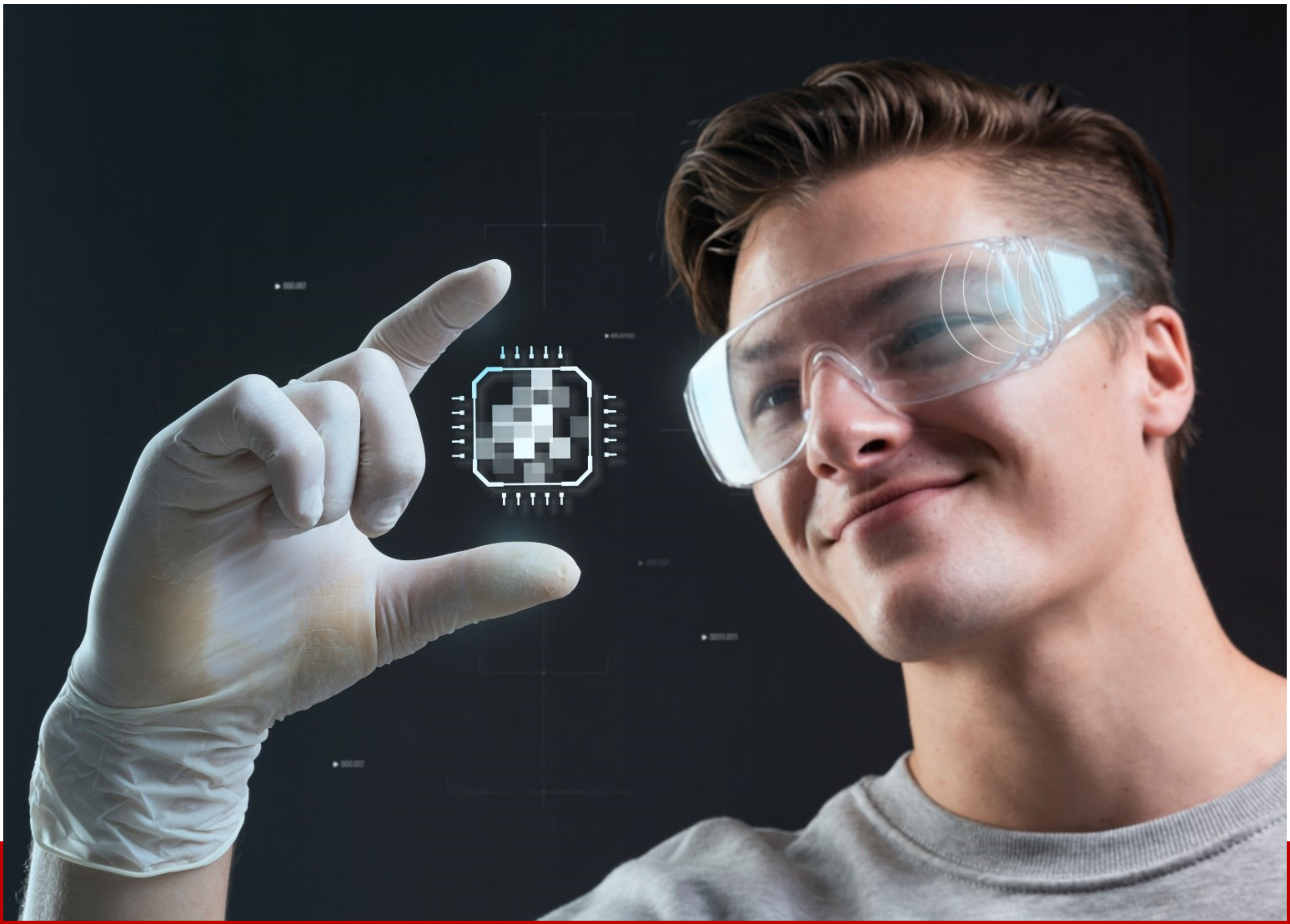
The State of Cybersecurity

Threat actors are constantly active and evolving, and we are all definitely hearing about more and more ransomware attacks today. As security measures become more advanced and third-party defenders help reduce vulnerabilities, one would hope that the volume of these attacks should be dwindling. It's true that bad actors are on the rise, but it's also true that current disclosure requirements may be driving a lot of the activity we see in the news today. An attack which might have been quietly handled completely out of sight of the public and the government a few years ago is much more visible today.

Despite all of these challenges - adversaries working with one another through their supply chains, using evolving tools and techniques in an effort to crack open your own supply chain at a weak point - there is still reason to be optimistic. While preventing these types of attacks is always preferred, mature organizations today recognize that prompt and timely detection of these attacks may be even more important. You want to know where "patient zero" is within your environment, and to be able to take action early in a ransomware attack, before it spreads and spirals out of control. After all, if you can't see what's happening on your network, if you can't see what's happening on your endpoints, you may not see the attack until it's too late. Don't be afraid to ask for help.

About the Author

Ben Smith is Field Chief Technology Officer with NetWitness. He brings more than 25 years' experience in the information security, risk management, networking and telecommunications industries; his prior employers include RSA Security, UUNET, and the US Government, along with several technology startups. Smith holds industry certifications in information security (CCISO, CISSP), risk management (CRISC), and privacy (CIPT); he is an acknowledged contributor to NIST SP 1800-1, -3, and -7 and he chairs the Cybersecurity Canon Project. He is a patent holder, a published contributor of four of the "97 Things Every Information Security Professional Should Know" [O'Reilly, 2021] and previously served as a corporate representative to the National Cybersecurity Center of Excellence (NCCoE). Ben can be reached online at https://www.linkedin.com/in/bnsmth/ and at our company website https://www.netwitness.com/.



Passive Optical Networks: A Game Changer for Now and The Future

By Folden Peterson, Director of the Federal Initiative at Quadrant Four, and John Taglieri, President of Mission Focused Consulting LLC

The Department of Defense (DoD) faces challenges in meeting network requirements due to evolving needs, diverse missions, and coordination with other sectors. However, the current network infrastructure falls short in addressing these challenges. While acquiring more physical infrastructure or optimizing existing resources may seem like viable solutions, they also come with their own set of challenges. As an Army communications battalion commander, I experienced the reliance on human touch, tenacity, and innovation to make the existing technology work for our mission requirements. However, there were concerns about the interoperability of our systems, the durability of our aging equipment, and whether these systems aligned with the DoD Software Modernization Strategy from a resilience, unity, and cyber-survivability standpoint. To ensure that we effectively incorporated these mission facets into practical terms, my team and I consistently conducted planning meetings to project future budgets.

Given these challenges, passive optical networks (PON) technology has emerged as a game-changing opportunity for the DoD to take a lead role in establishing more sustainable networking and achieve its green energy goals. Prioritizing the adoption of PON can lead to the creation of a secure, efficient, and environmentally resilient communications infrastructure. This paper emphasizes the numerous benefits of PON, including cost-effectiveness, improved network infrastructure and services, and support for various applications. By leveraging successful use cases and best practices from both civilian and military sectors, the DoD can maximize outcomes and position itself as a pioneer in sustainable networking.

PON technology, widely utilized by major telecommunications service providers such as Verizon and AT&T, is transforming how data is transmitted over optical fiber networks. While commercial entities have already embraced this technology, the DoD currently lags in leveraging cutting-edge network technologies. Adopting PON can provide significant advantages, as it offers enhanced security, reliability, and cost-effectiveness. It can reduce capital costs by up to 30-50% and operational costs by 50-70%, while also improving network infrastructure, services, trustworthiness, and speed. PON supports various applications like voice, video, wireless access, security, surveillance, building environmental controls, and automation using Power over Ethernet.

PON technology uses a Layer-2 transport medium to deliver converged audiovisual and data services at gigabit speeds over a single strand of fiber to the user's location. Unlike traditional copper-based LAN, transitioning to a PON infrastructure does not require reconfiguration of clients or PCs.

To gain a competitive edge, the DoD should aspire to integrate state-of-the-art commercial network technologies into its networks at the speed of relevance. This requires aligning telecommunications technology goals with environmental sustainability and proficient management of the application portfolio. By adopting PON technology, which is already employed by various industries such as by finance, hospitals, manufacturing, airports, solar farms, hotels, stadiums, schools, and utilities, the DoD can achieve this edge.

By embracing innovative solutions, the DoD can establish a secure and efficient communications infrastructure that is technologically and environmentally sustainable and resilient, positioning itself as a pioneer in the field. This would not only benefit the DoD but also showcase the substantial impact of PON technology in telecommunications. Leveraging successful use cases and best practices from both civilian and military sectors, the DoD can maximize cost-effectiveness and results, driving transformative changes that benefit both sectors.

Embracing PON: Technology for Environmentally Sustainable Military Networking

The DoD seeks to enhance operational efficiency and maintain global dominance in national security, but utilizing sustainable and energy-efficient solutions in the military is also important, so much so that the DoD has spent over $100 million since 2010 on what are known as Energy Resilience and Conservation Investment Program (ERCIP) fund projects.

Aligned with its commitment to environmental sustainability, the DoD has prioritized the adoption of PON technology in its Digital Modernization Strategy publication to reduce energy consumption, minimize waste, and promote eco-friendly alternatives. While some may argue that the reductions in energy consumption and waste from PON installation may not have a significant impact on the environment, using PON technology in the telecommunications mission is beneficial for the environment and enables other energy-saving capabilities like smart grid integration and Supervisory Control and Data Acquisition (SCADA) systems. By reducing our carbon footprint, PON enhances its sustainability contributions.

Enhanced Efficiency: Network Reliability, Operational Savings, and Less Human Touch

PON technologies offer enhanced efficiency, network reliability, operational savings, and less human touch, making them the future of networking resilience. These technologies align with the current administration's green energy goals and require less human intervention by eliminating the need for active electronic components. As a result, PONs are an ideal fit for military networking, delivering significant long-term savings.

The capability of PONs to operate without active electronic components means they are less prone to failure and require less maintenance. This enhanced reliability results in high-speed internet connections of up to 40km, which is significantly further than traditional copper wire connections. Initiatives such as the Rural Digital Opportunity Fund (RDOF) and the Infrastructure Investment and Jobs Act (IIJA) aim to improve broadband infrastructure and access in underserved rural areas in the United States. These initiatives align with the broader concept of promoting Broadband Equity, Access, and Deployment (BEAD) to bridge the digital divide and create economic growth opportunities in rural communities.

The deep fiber design of PON technology offers four times better Ethernet density from a smaller footprint and reduced cabling, which continues to attract cable and telecom cooperatives. As a result, PON is an excellent choice for organizations pursuing sustainability and zero-trust initiatives. Thus, PON is an ideal fit for organizations seeking sustainable and cost-effective networking solutions.

PON for the Military: Reduced Infrastructure, Unmatched Security

PON is superior to traditional alternatives, particularly in military applications. One of its main advantages is that it can connect multiple users using a single optical fiber, thereby eliminating the need for copper cabling and bulky active equipment. This feature makes PON ideal for rapid deployment and mobility, making it perfect for military operations. In addition, PON offers physical layer security, which allows for the implementation of various security measures at different levels, ensuring HIPAA-compliant and PCI-compliant networks, and it has a lifecycle of 10 years or more.

Although some critics claim PONs are vulnerable to cyber-attacks, implementing AES encryption and regularly updating security measures can substantially reduce the risk. PON operators must stay vigilant and continuously enhance security to stay ahead of emerging threats. PON technology provides a secure and low-emission solution by utilizing fiber optic cables to eliminate TEMPEST concerns. It includes extensive security measures, such as Access Control Lists, Broadcast Datagram Rate Limiting, and strong authentication across the physical, data, and user port layers to prevent malicious activities.

PON technology is a versatile communication platform that supports video, voice, and data transmission from a single network. It is also designed to be resistant to electromagnetic interference, a critical advantage in military environments. By adopting PON technology, the Department of Defense can optimize its limited resources and protect critical information from potential adversaries. Therefore, PON technology represents an excellent opportunity for the military to enhance its communication capabilities while also safeguarding its networks.

A Call to Action: Prioritizing PON Adoption

To assume a leadership position in the field of sustainable networking and fulfill its green energy goals, the DoD must continue its focus on prioritizing the adoption of PON technology. It presents an affordable option for increasing equipment lifespan, and it enables the prioritization of future military construction projects through periodization.

To ensure successful implementation, it is necessary to conduct a thorough assessment of PON technology's long-term expenses, scalability, maintenance costs, and compatibility with current systems. Additionally, optimizing the benefits of this technology requires a well-managed application portfolio that utilizes the Six Step Process for Application Rationalization.

Service providers have already widely adopted PON technology, making their local area networks more secure, reliable, and cost-effective. It can save up to 30-50% in capital costs and 50-70% in operational costs while improving network infrastructure, services, reliability, and speed. It also supports various applications like voice, video, wireless access, security, surveillance, building environmental controls, and automation using Power over Ethernet.

By adopting PON technology, the DoD can align its telecommunications technology and environmental sustainability goals and gain a competitive edge. It can position itself as a pioneer in establishing a secure and efficient communications infrastructure that is technologically and environmentally sustainable and resilient. The DoD can also draw upon successful use cases and best business practices in the civilian and military arenas to maximize cost-effectiveness and results, potentially benefiting both sectors.

Having served as an Army communications battalion commander who has seen the technology's effectiveness in an operational environment, I strongly recommend that the DoD prioritize the adoption of PON. Its passive architecture simplifies infrastructure and lowers maintenance costs, while its inherent security benefits will protect sensitive military data. This move will not only enhance operational efficiency but also contribute to climate resilience.

The DoD has a unique opportunity to revolutionize our understanding of sustainable networking by adopting PON technology, so it is crucial to urge the DoD to do so. Once implemented, the use of PON will enable each service component to create a brighter, more sustainable future and lay the groundwork for 2035 and beyond.

About the Authors

Folden Peterson, Director of the Federal Initiative at Quadrant Four, brings over 30 years of U.S. Army experience. His expertise spans digital communications, risk management, and strategic transformation, acquired through service at all levels from tactical to Army and MACOM staffs. His operational, combat deployment, congressional, and legislative liaison experience further enhances his capabilities. He can be reached on the Quadrant Four website, LinkedIn, folden@quadrantfour.com or by phone at 717-753-4148.

John Taglieri, President of Mission Focused Consulting LLC, has 41 years of U.S. Air Force service, 28 years on active duty and 13 years in civil service. He has a wide range of experience in communications, information technology, and cyber. His insight, dedication, and persistence ensured mission accomplishment at the operational, deployed, and base levels and at the Air Staff and MAJCOM staffs. He can be reached on LinkedIn, jrtaglieri@missionfocusedllc.com or by phone at 425-984-4102.

Cybercrime, Cyber Warfare, and Government Attitudes Towards Cybersecurity

By Avishai Avivi, CISO, SafeBreach

The face of cybersecurity is evolving. Cybercrime and its implications have grown into an inescapable fact of our daily lives, affecting everyone from the general consumer to Fortune 500 corporations. Cyberattacks have even begun to creep into the military sphere, with the threat of all-out cyber warfare looming large over conflicts across the globe.

As a result, government attitudes towards cybersecurity have undergone a dramatic change. 2022 saw governments around the world creating—or at least more heavily debating — cybersecurity regulations to help secure enterprises and organizations from evolving cyber threats. The UK, for example, passed the Telecommunications Security Act, which implemented tougher security standards on Internet service providers (ISPs) to minimize breaches that could expose the private data of millions of consumers. And for the first time, the US-based Cybersecurity and Infrastructure Security Agency (CISA) urged enterprises to choose a more proactive approach to defend themselves against cyberattacks, recommending automated continuous validation of security controls to protect against the constantly evolving threat landscape.

With this in mind, it’s worth taking a deeper look at how cybercrime and cyber warfare have impacted government attitudes towards cybersecurity.

What is cyber warfare?

The term “cyber warfare” is itself contentious. There has been much debate surrounding its definition, with some experts even questioning whether we can truly distinguish between cyber warfare and traditional warfare.

However, the RAND Corporation, an American global policy think tank, does give us a reasonable working definition.

“Cyber warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks.”

Considering contemporary society’s near total reliance on computers and information networks, it’s easy to see why governments would want to shore up their defenses against potential cyberattacks, particularly at a time of geopolitical unrest. We have already seen glimpses of the havoc cyberattacks can wreak on a nation’s infrastructure. The most memorable of these perhaps was the Colonial Pipeline incident in 2021, which caused gasoline prices in the US to skyrocket, sparked a wave of panic buying, and resulted in President Joe Biden declaring a state of emergency.

How are government attitudes changing?

As previously noted, the prospect of cyber warfare has brought about important changes in the way governments approach cybersecurity. The US government has long emphasized the importance of collaboration between the private and public sector in protecting critical national infrastructure (CNI). However, the 2023 US National Cybersecurity Strategy puts a new, much stronger emphasis on regulation, expressing the need to:

- Establish cybersecurity regulations to secure critical infrastructure
- Harmonize and streamline new and existing regulations
- Enable regulated entities to afford security

This is in stark contrast to the 2018 strategy that only mentions regulation once in the entire forty page document, and in fact, goes so far as to criticize the idea. The two documents represent far more than the ideological differences of different administrations. They show how the federal government shifted its views on cybersecurity in response to significant, world-changing events.

Roughly two years after the unveiling of the 2018 US Cybersecurity Strategy, COVID-19 swept the globe, irrevocably changing the world as we know it. In March 2020, much of the US was locked down, forcing many employees to work from home. By June, the FBI reported a 75% increase in cybercrime.

Just under a year later, in May 2021, the Colonial Pipeline incident occurred. DarkSide, a cybercriminal group with ties to Russia, launched a ransomware attack on a pipeline system originating in Houston, Texas, that supplies gasoline and jet fuel to much of the Southeastern United States. The attack caused mass fuel shortages, halted flights, and brought about a state of emergency.

In February 2022 the Russian army stormed Ukraine's borders. War had returned to Europe. The invasion provoked widespread condemnation from world leaders and sparked an atmosphere of geopolitical unrest that persists to this day. Moreover, throughout the war, Russia has repeatedly launched cyberattacks on Ukraine to varying effects. Russia also engaged in traditional kinetic attacks to destroy Ukraine's access to the internet.

These events undoubtedly helped influence the U.S. government's attitudes towards cybersecurity. From COVID-19 to the Colonial Pipeline attack to the eruption of war in Europe, it became clear that state-sponsored cyberattacks on US infrastructure were no longer out of the question. The development of more stringent regulations was a natural outcome.

What role should the private sector play?

The prospect of cyber warfare has dragged the private sector into conflicts to an extent that hasn't been seen in the US since the Second World War. Private organizations are now a legitimate target for military campaigns. For nations such as the United States, who have grown unaccustomed to fighting battles - kinetic or otherwise - on their own soil, this is a particularly worrying prospect.

As a result, the private sector has a significant role to play in national security, and this doesn't only apply to organizations that could be considered CNI. Any organization could be targeted by state-backed hackers, for a number of reasons. The nature of modern business supply chains means that any organization could be seen as an attractive target, as they could be the first step on the way to breaching a larger, more critical organization.

In light of this, it's more important than ever for the private sector to take responsibility for their cybersecurity. Their responsibility now goes beyond the protection of their reputation, finances, and customer data, and into the realm of keeping their nation safe. This is absolutely key to understanding why global superpowers such as the US are bringing in more stringent regulation and recommendations, and why automated continuous security validation is so important. Organizations must be able to tell whether or not they are at risk, and tools such as breach and attack simulation (BAS)—which provide a way for organizations to continuously validate the efficacy of their security ecosystem, identify gaps, and take meaningful remedial action - are essential to providing that information.

Could cybersecurity be considered CNI?

We've already touched upon the importance of cybersecurity for CNI, but this begs the question whether cybersecurity could actually be CNI. The Center for the Protection of Critical National Infrastructure (CPNI) defines CNI as:

"National Infrastructure are those facilities, systems, sites, information, people, networks and processes, necessary for a country to function and upon which daily life depends. It also includes some functions, sites and organizations which are not critical to the maintenance of essential services, but which need protection due to the potential danger to the public (civil nuclear and chemical sites for example)."

Considering that all of the industries that would fall inside those parameters rely on cybersecurity to continue operating, then surely cybersecurity, by definition, should also be considered CNI.

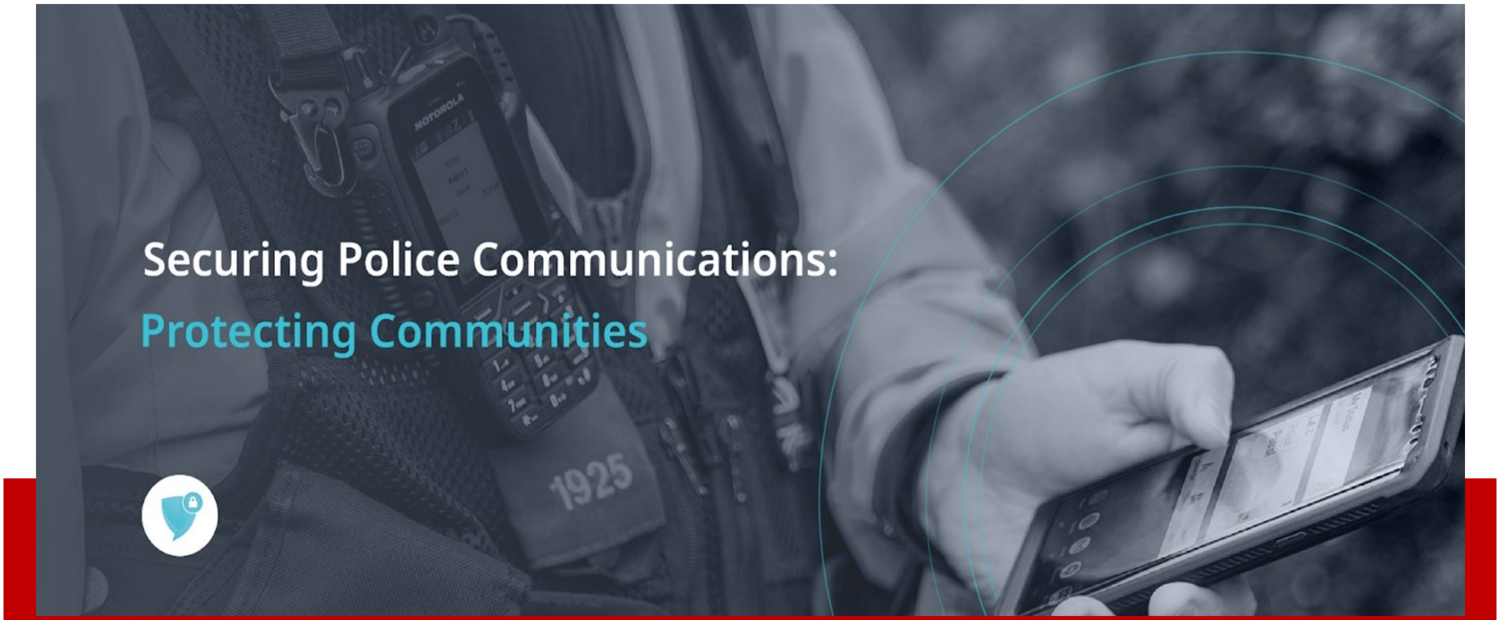
CNI sectors are considered critical because if any failed, a country could cease to function. Moreover, CNI suffers more frequent, diverse, and sophisticated cyberattacks than any other sector; this means that should the cybersecurity sector fail, an entire nation's CNI could fail with it.

In summary, it's clear that the mere prospect of cyber warfare has had a major impact on government attitudes towards cybercrime. While, from a security perspective at least, this change is welcome, it does mean that private organizations will be increasingly pressured to take responsibility for their cybersecurity. Employing security tools, like BAS for example, that provide deep insight into an organization's environment is more important than ever. Whether we like it or not, more stringent cybersecurity regulation is on the horizon, and businesses must be prepared.

About the Author

Avishai Avivi is the Chief Information Security Officer at SafeBreach, the pioneer in Breach Attack and Simulation (BAS.) Avi brings more than 30 years as a senior information security leader with companies such as Wells Fargo, E*Trade, and Experian, where he created and implemented security programs with a focus on best practices and control maturity. Avi's security career started with the Israeli Defense Forces Unit 8200 and has included multiple roles and domains across information security, product R&D, professional services, customer support and strategic leadership. Avi holds a dual MBA from UC Berkeley's Haas School of Business and Columbia University's Business School. He is CISSP, CISM, CRISC, CISA, CIPM and CIPT certified and holds the Stanford University Strategic Decision and Risk Management program certification.

Avi can be reached online at linkedin.com/in/aavivi and at http://www.safebreach.com



Securing Police Communications: Protecting Communities

By Nicole Allen, Senior Marketing Executive at Salt Communications

Probably now more than ever, secure communications are crucial for Policing and the communities they serve.

The ability to successfully communicate with co-workers, superiors, other departments and jurisdictions, and the court systems is essential for law enforcement and police officers if they are to fulfil their duty to "**protect and serve**" the communities they operate within. Having this level of secure communications throughout a police force is vital to investigate crimes sensitively and efficiently, defuse tense situations with all relevant information readily available which will in turn establish a stronger trust within communities.

The challenges Policing face when protecting communities

Police forces must communicate in a clear, succinct and accessible manner in order to be effective. The issue arises when communication becomes broken down due to using multiple different communication channels. Without a clear understanding of what methods of communications are secure and acceptable, officers will use whatever tools are most convenient, often putting crucial information at risk.

The confidential policies, updates, protocols, directives, and initiatives that are given to police officers are constantly changing. Not to mention the memoranda and communications from various departments and leadership that they are receiving, which can be overwhelming and unclear for officers to take in - in addition to being insecure. This may have long-lasting repercussions for an officer's comprehension of specific rules and policies, which may then negatively affect civilians.

By placing a high priority on good communication in policing organisations, you will raise morale, boost job satisfaction, improve feedback, strengthen teamwork, ensure compliance and most importantly communicate securely.

How Policing can build trust with communication

In the sphere of criminal justice, the capacity to safely communicate can make the difference in critical situations. Police officers must be communicating in a safe manner to maintain order, protect citizens and obtain information that can help law enforcement apprehend criminals. Learning to communicate effectively also requires learning how to spot indicators of conflict, avoid and resolve them.

A department's internal communication, including how officers communicate with one another, how leadership communicates with the rank-and-file, and the rules and regulations that govern how the department runs, should be one of its top priorities. If you can get this mastered and deploy an effective system, it will greatly enhance how your department operates within the community. Officers will grasp the policies and instructions from leadership more clearly if there is an effective communication system in place to receive this information. They'll know what to do in particular circumstances and have the technology available to them to make better decisions, which will ultimately be advantageous to both the officers and the community in which they work.

Better equipped officers means a happier community

Not only is what you say and how you say it important, but also the channel in which you say it. As a result, policing personnel must be able to share various pieces of information over a reliable route. While answering a response call, it would be as easy as clicking a few buttons via a broadcast message to push out real-time alerts to all relevant groups of users. It has a central area where memos, evidence on scene, policy updates, and training materials can all be shared and accessed from a laptop, mobile device or one to the other. Ultimately this ensures trust in your community as they know their emergency call is being dealt with quickly and efficiently.

Your officers will have some of the most cutting-edge police communication technology if they can communicate through this one secure platform when out on the ground and back to base.

In order to obtain intelligence and information on current and potential criminal and terrorist activity, the police and security agencies rely heavily on their capacity to communicate in a secure and clear manner at all times. Maintaining public safety and successful policing depend on police forces and the communities they serve developing strong relationships based on mutual trust.

The effectiveness, efficiency, and engagement of communication between officers can be significantly increased by a secure communications platform that supports efficient communication in law enforcement. There will be clearer and simpler internal communication for both policing organisations to share sensitive information, aiding decision making and offering on the ground evidence, improving their ability to serve their communities.

You will always be connected to a resilient, dependable network when you need it most thanks to Salt Communication's expertise in developing and delivering secure, robust communication capabilities. To learn more about protecting your communications for your force, you can read more on our website or sign up for your 30 day free trial.

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 visit Salt Communications.

References:

https://www.ojp.gov/pdffiles/commp.pdf

https://onlinedegrees.sandiego.edu/police-communication-important-today/

https://www.college.police.uk/guidance/vulnerability-related-risks/communication#:~:text=Vulnerability%2Drelated%20risks-,Communication%20%E2%80%93%20guideline%20introduction,including%20any%20experience%20of%20abuse.

About the Author

Nicole Allen, Senior Marketing Executive 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 nicole.allen@saltcommunications.com) and at our company website https://saltcommunications.com/

ISO Certification is the Key to Better Cybersecurity for Business

By Sami Mäkiniemelä, Chief Security Officer, Miradore

Cyberattacks are on the rise. Every month it seems like another major business gets hit, with their data and customers compromised at an ever-growing cost. But more and more it's not just the large, global conglomerates who are at risk — small-to-medium sized businesses (SMBs) are increasingly becoming targets as well. While a recent survey showed two-thirds of organizations with over 1,000 employees were hit by cyberattacks in 2022, SMBs aren't faring much better with a reported 43% of all cyberattacks targeting them. And that number is expected to rise in the coming years.

These attacks not only cause significant disruption to business operations, but they are also affecting the corporate bottom line. Last year, the average cost of a cyberattack in the US hit $9.4M along with all the additional time and effort spent to deal with the damages done. Because of this growing problem, many businesses are actively seeking ways to signal to their potential customers and attackers that they take cybersecurity seriously. One way for organizations of all sizes to show this commitment is to gain ISO 27001 certification.

The International Organization for Standardization (ISO) is a multinational federation of standards organizations from 168 countries around the world. They serve as a forum for members to collaborate in the development and promotion of worldwide standards for technology, scientific testing, and working conditions. These approved standards are then sold by the ISO to global accrediting organizations, issuing certifications to businesses and institutions that apply for them and then ensuring they comply with these standards.

Currently, ISO 27001 is the industry's leading standard for information security management systems. Today, some of the world's largest technology companies have ISO 27001 certification, including Microsoft, Verizon, Apple, Google, Intel, and Amazon. But it's not just for the larger, global conglomerates. ISO 27001 can provide companies of any size with guidance for establishing, implementing, and maintaining their systems to manage risks related to the security of the company's data.

Additionally, ISO 27001 promotes a holistic approach to information security by vetting people, policies, and technology. When an information security management system is implemented according to this standard, it becomes an essential tool for risk management, cyber-resilience, and operational excellence. According to the ISO, implementation of their 27001 standard helps organizations in multiple ways by:

- Reducing vulnerability to the growing threat of cyberattacks, and helping companies respond to evolving security risks
- Ensuring assets such as financial statements, intellectual property, and employee data entrusted to third parties remain undamaged, confidential, and available
- Providing a centrally-managed framework that secures all information in one place, including paper-based, cloud-based, and digital data
- Preparing people, processes, and technology throughout an organization to face technology-based risks and other threats
- Saving money by increasing efficiency and reducing expenses for ineffective cyberdefense technology

The ISO standard also benefits companies by signaling to potential customers that they take cybersecurity seriously. Certification demonstrates that a vendor is committed to constantly investing in the infrastructure, staff, and policies needed to ensure that their customers' data remains safe and secure. This is especially important for businesses that provide IT or technology services to other organizations like MSPs, SaaS vendors, or cloud hosting organizations. Also, clients working in extra sensitive industries like healthcare and defense are often required by law to work with IT vendors who maintain ISO 27001 certification for compliance reasons. That means certification can bolster a company's reputation in these sectors while opening them up to new customers and markets.

Miradore, the mobile device management company I work for, recently received its own ISO 27001 certification. Initially, we did this to show our commitment to strong cybersecurity practices and demonstrate our commitment to protecting our customers. But we had also heard from many potential customers that they wanted to work with us but needed an ISO 27001–certified vendor. Now, by having this certification, we can bring in new business while ensuring that all of our customers are protected by the industry's leading data security practices.

After our experience with this certification, which has had so many positive results, we now recommend that any companies that are serious about cybersecurity, especially those providing IT/tech services to clients, should start pursuing ISO 27001 certification immediately.

As cyberattacks continue to increase in frequency and cost, it’s clear that companies of all sizes need to do everything they can to stay current with cybersecurity best practices. ISO 27001 is one of the best ways for businesses to do this. It ensures internal compliance with industry-standard practices, signals to potential customers and attackers that you take cybersecurity seriously, and broadens an organization’s appeal to new customers and additional markets. Not only does it protect your data and clients, it ultimately protects your bottom line and the very future of your business.

About the Author

Sami Mäkiniemelä is the Chief Security Officer at Miradore, a software company that offers MDM

services. Sami can be reached online via LinkedIn. You can learn more about the benefits of mobile device management on Miradore’s website.

Secure Remote Access is Not a One Size Fits All Vision

Unlocking the puzzle of OT security

By Kevin Kumpf, Cybersecurity Evangelist at Cyolo

Secure Remote Access (SRA) is a term that can be technologically defined in many ways, depending on whom you talk to, from a customer or vendor role and through what "lens" they are looking. No matter what the person's role or perspective though, Secure Remote Access must be safe and secure, but everything else that can encompass Secure Remote Access is truly open for discussion.

What is "Secure" Remote Access

"Secure" Remote Access by technical definition, is a combination of security processes / controls that are designed to prevent unauthorized access to digital resources. Successfully implemented SRA, however, does not just include the technology used to connect a user to a resource or even a resource to a resource. The weakest link in any implementation of SRA is people.

In the recently published "State of Industrial Secure Remote Access (I-SRA)" report which surveyed respondents from the Operational Technology (OT) space, 75% of the respondents overwhelmingly acknowledged that threats to business operations were the biggest concern when dealing with any form of SRA to a resource. Additionally, 67% of respondents felt that Advanced Persistent Threats (APTs) are a growing concern and 72% viewed third-party connections as their biggest risk for any Remote Access.

Now, you may be asking why an OT targeted report is relevant to SRA across any organization and the answer is simple. Many SRA solutions are shared, maintained, managed or controlled in some form by IT resources within an organization. The threat of Ransomware as an example, is not just focused on attacking specific company resources but is focused on being able to disrupt as many business operations as possible to extract financial gain for the threat actors.

Navigating the Scope of Secure Remote Access Components

As for the human component of SRA, 59% of respondents were concerned about even trusted users with direct access to resources. This is where the definition of SRA and trusted users gets murky.

In most organizations, SRA is not just used by third parties but is also used by remote workers, internal users crossing organizational boundaries to connect to resources and a growing segment where SRA and Software Defined Networking (SDN) are being used together as well. This brings us back to the “lens” statement above.

To many organizations or technology vendors, a Virtual Private Network (VPN) is a form of Secure Remote Access, and they are not incorrect in this statement. A VPN is encrypted (secure) and uses a form of 2FA/MFA user / device authentication (ex. token, cert, key, etc.) prior to granting access (safe) but that is where it ends generally. Some can enforce access policies, resource controls, connection time but generally they place you on a jump / bastion host where applications are published to the multiple users.

Things such as session recording, supervised access, shared credential vaulting and function restricting are not available. Lastly this type of connectivity is at the Network layer (the letter N in VPN) not the application layer so if the end device is compromised ransomware and other network layer threat vectors can be attempted successfully.

Another form is the highly discussed and promoted ZTA / ZTNA, which for those of you who do not know is based on NIST SP 800-207 (I highly suggest reading this Special Publication before using the term freely). In this vision of SRA the premise is trusting nothing, hence the Z for Zero. It also practices the principle of continuous validation which means inspecting the session to ensure everything is still safe and secure. This form of SRA also is deeply rooted in policy which means granular control or people, process, and the technology being used within the SRA session.

Unmasking the Weakest Link in Secure Remote Access

The point of this article is not to get into which technology model (and there are others as well) is the best, but to discuss the real underlying problems of any SRA solution and those are proper configuration, oversight, usage and management.

The underlying problems above all are directly related to the weakest link in any SRA implementation and that is the people component. We do not truly trust the end users or devices they are connecting from or to (hence the Zero in ZTA / ZTNA) and for valid reasons. We also cannot trust that internal staff (or external resources managing our SRA implementations) follow published best practices for creating a safe and secure access infrastructure. From the auditor "lens" we all have found open VPN connections, weak passwords, shared user accounts, ineffective policies and just overall poor security hygiene. We also have found a lack of audit trails or that collaboration tool installed on a jump host so a third party can easily get in to do urgent work after hours.

In conclusion, no matter what we define as an SRA solution we all must do a better job from both a vendor and end user perspective in creating a more secure and risk reducing safety posture for SRA implementations overall, which 55% of respondents stated was a concern as well.

About the Author

Kevin Kumpf has more than 20 years of IT security and compliance experience, including over 10 years of cybersecurity, governance and critical infrastructure experience working in the energy, medical, manufacturing, transportation and FedRAMP realms. Kevin's past roles include Director of OT Security (N.A.) for Iberdrola, where he oversaw the security, and regulatory compliance of multiple OpCo's, and Principal Security and Regulatory Lead for interactions with the NY and NE ISO's, NERC, ISAC's as well as state and federal entities. He has also worked internally and as a vendor/consultant at multiple healthcare and manufacturing entities to mitigate the threats they were under in relation to ransomware, insider threats and malware infestation. Today Kevin works as the OT Technical Lead at Cyolo. More information can be found at Cyolo's website here: https://cyolo.io/

Steps for Preparing for a Quantum-Resistant Cryptographic Future

By Timothy Hollebeek, Industry Technology Strategist, DigiCert

The rise of post-quantum cryptography (PQC) is shedding light on the pervasive nature of cryptography in our digital world. Virtually every digital connection relies on cryptographic techniques and public key infrastructures (PKIs) to establish trust. However, the emergence of cryptographically relevant quantum computers (CRQCs) poses a threat to traditional asymmetric algorithms such as RSA and ECC. The solution lies in post-quantum cryptography, which encompasses cryptographic algorithms designed to be resistant to quantum computer attacks.

While CRQCs need to be more powerful and larger than currently available quantum computers, their development is progressing, and organizations must prepare for the eventual transition to post-quantum algorithms. This transition poses a significant challenge, necessitating a complex upgrade of the vast digital infrastructure built over the past few decades. Although organizations have some time to adapt, they need to initiate the process of understanding the implications of this transition.

In the United States, federal agencies have been instructed by the Office of the National Cyber Director (ONCD) to inventory their cryptographic systems in preparation for the shift to quantum-resistant cryptography. The guidelines, outlined in the White House's National Security Memorandum 10, required agencies to submit their prioritized inventories of cryptographic systems by May 4, 2023. However, meeting this deadline has proven to be challenging for some agencies. The complexity of identifying cryptographic systems is not limited to federal agencies alone; it applies to organizations across all sectors. Cryptography's ubiquitous presence makes it difficult to track assets that organizations may not even be aware of.

Although not subject to the May deadline, Enterprises must also identify and proactively manage their cryptographic assets. It is crucial for all organizations to follow a structured approach for transitioning to a post-quantum world. Consider the following steps:

Step 1: Inventory

The first step is to inventory all cryptographic systems, including certificates and algorithms, and prioritize them based on their level of criticality. This process entails understanding the crypto assets within an organization's environment, including the algorithms certificates used, their issuers, expiration dates, the domains they protect, and even the software signed with specific keys. Additionally, organizations must investigate whether their software packages or devices automatically download updates, connect to backend servers, or operate on websites or portals managed by third parties or cloud providers. Establishing these details requires extensive communication with various providers and backend entities.

While identifying an organization’s digital footprint may seem daunting, it is essential in today’s interconnected world. Understanding crypto assets is the key to protecting them effectively.

Step 2: Prioritize

The next step involves prioritizing the replacement of encryption algorithms that generate signatures requiring long-term trust. This includes securing the roots of trust, firmware for long-lived devices, and other critical components. The urgency arises from the fact that encrypted data can be recorded now and decrypted later by operators of future quantum computers, a practice known as “harvest now, decrypt later.” Therefore, any encryption intended for long-term use should be the first priority for replacement.

Step 3: Test

Furthermore, organizations need to explore and test the incorporation of post-quantum cryptography algorithms. The National Institute of Standards and Technology (NIST) has already selected the final algorithms for PQC standardization, but the development of standards, documentation, and secure implementation methods is still underway. It may take up to two years before these algorithms become widespread. However, implementers of cryptographic libraries and security software should start integrating these algorithms into their products now. Organizations can also begin exploring how to incorporate the selected PQC algorithms, as there will be a certain level of effort required to accommodate them.

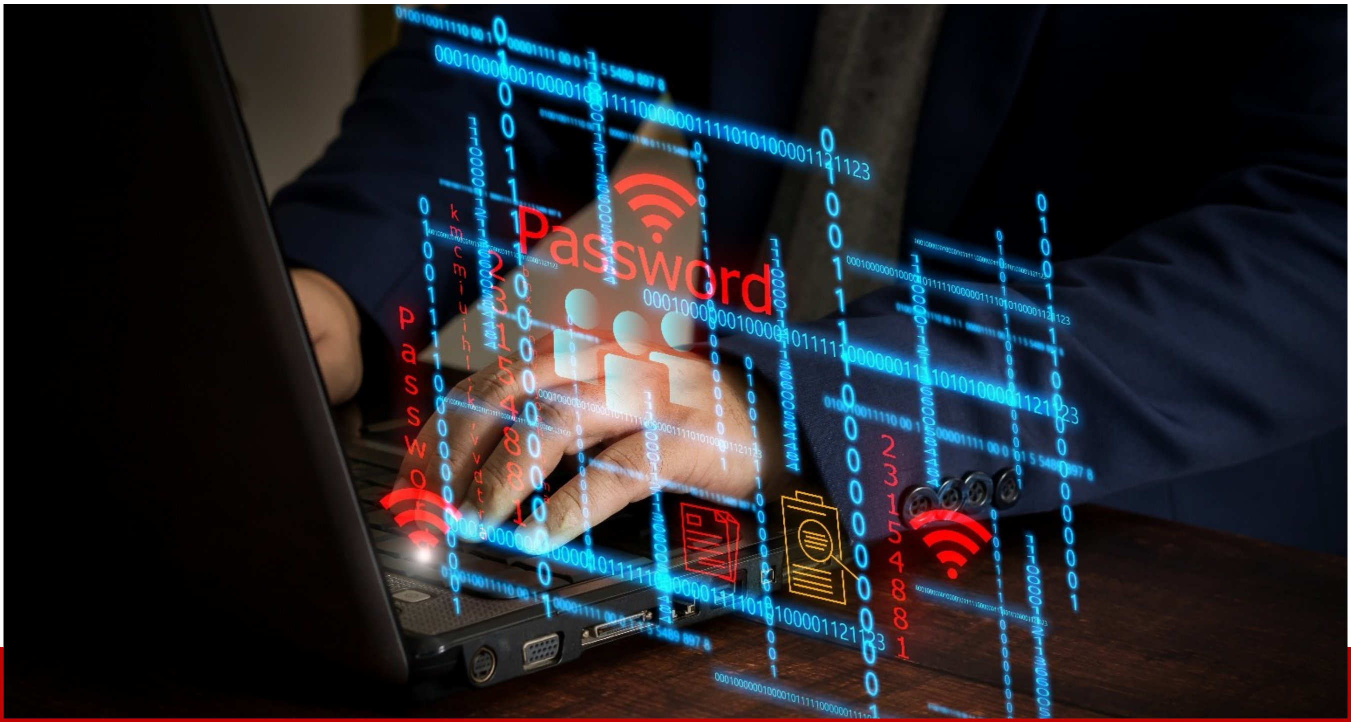
While the deadline for federal agencies to submit their inventories of cryptographic systems has passed, the need for all organizations to identify and manage their crypto assets proactively remains. The transition to quantum-resistant cryptography is a significant undertaking, but by understanding and managing their crypto assets, organizations can lay the groundwork for a secure and trustworthy digital future.

It is crucial to start the process now and stay informed about the developments in post-quantum cryptography to ensure a smooth transition when the time comes.

About the Author

Timothy Hollebeek is the Industry Technology Strategist at DigiCert. He has more than 20 years of computer security experience, including eight years working on innovative security research funded by the Defense Advanced Research Projects Agency. He remains heavily involved as DigiCert's primary representative in multiple industry standards bodies, including the CA/Browser Forum, striving for improved information security practices that work with real-world implementations. A mathematician by trade, Hollebeek spends a lot of time considering security approaches to quantum computing.

Tim can be reached online at (tim.hollebeek@digicert.com) and at our company website http://www.digicert.com/



Tech-Forward Strategies to Effectively Fight Fraud

By Blair Cohen, Founder and President, AuthenticID

Not only has digital transformation completely reshaped the way we conduct business, but it has also introduced an onslaught of fraudulent attacks on both organizations and consumers alike. In fact, more than half (53%) of consumers today have had their identity compromised at some point. As we continue down the path of digital transformation, cyberattacks will only increase in volume and complexity. As a result, identity-proofing will remain a critical piece of the fraud-prevention puzzle.

With the total cost of cybercrime expected to reach $8 trillion this year, there are several next-gen authentication methods business leaders should consider implementing to help protect both their company and their customers from harm.

The Value of Stateless and Biometric Authentication in Fighting Fraud

Stateless authentication – also known as token-based authentication – verifies users through tokens, most frequently a JSON Web Token (JWT), which are used for managing authorization. With this authentication method, information is stored within the token, allowing a user to access what they need without being required to provide their username or password.

Token-based authentication offers another layer of security beyond password and other single-factor authentication methods; giving only administrative users control over the actions needed for verification. As hackers have grown to realize, passwords are often repeated or slightly changed across accounts over time, making them easily accessible and, in some cases, putting multiple accounts at risk.

Adding token-based authentication is an important step in preventing fraud as it ensures that any user must have access to an external account or device that will verify their identity through a uniquely-generated, cryptographically- signed token or code. While this is a smart route to bolster security, this approach can be further strengthened to enable passwordless access through the use of biometric authentication.

New technology has enabled fraudsters to reroute text messages and easily gain access to a person's sensitive information via an account takeover or by remotely accessing their IoT devices. Biometric authentication includes facial, fingerprint, iris, and voice biometric data that can be used to prove someone's identity.

For example, a person's face is instantly compared to and matched with a database of existing users to prevent one user from making multiple accounts. Today, behavioral biometric technology is being used to detect behaviors like keystrokes or touchscreen behavior to *continuously* authenticate a user, leading to even stronger authentication.

Unfortunately, today's fraudsters have the benefit of new technologies like generative AI that make it much easier to spoof someone's biometric information. To effectively deter fraud, organizations need to implement solutions with biometric algorithms that aren't vulnerable to generative AI and injection attacks, in addition to moving away from KBA and SMS authentication methods, which are becoming easier and easier for bad actors to break through in our increasingly digital world.

Next-generation authentication like this provides a winning balance between security and convenience. Deploying future-forward biometric and/or stateless authentication methods will ensure that the person attempting to access an account or perform a transaction actually is who they say they are.

Identity Verification Driven by AI and Machine Learning

Current methods of identity fraud vary from creating fake IDs and passports to the use of more advanced, hard-to-spot deepfake technology. Even the technology available to cybercriminals is advanced enough to create replica ID cards that could fool the most experienced expert. A lot of solutions today only run around ten tests on an identity document, thus requiring manual review from humans, while top-of-the-line solutions using machine learning are able to run hundreds of tests, which decreases user friction while increasing verification accuracy.

Utilizing AI and ML is necessary for accurate and secure ID verification because people can't learn all of the intricacies of identity documents. AI and ML offer a replacement for manual ID verification and can process data much faster than humans, resulting in the ability to quickly spot suspicious patterns, while also making sure visual aspects of the ID are in the right place. This would take much longer for a person to do manually. The technology-driven method is also scalable, which allows for substantial operational expense benefits.

Not only that, but AI and machine learning can also perform facial recognitions, block user actions, detect suspicious logins, and identify faulty transactions. Effective ID verification requires a combination of AI and ML, coupled with best-of-breed facial recognition and liveness detection technology to detect fake identity documents and deepfakes, ensuring authorization is only granted to the correct person.

Zero Trust Security Infrastructure

As we've seen, digital transformation can cause a whirlwind of security issues. Oftentimes, technology and software are released by organizations without a true look into security implications or potential vulnerabilities. Methods that used to be reliable, such as one-time passwords and QR codes, now fall vulnerable to fraudsters. As methods of fraud increase, a Zero Trust approach –- the belief to never trust, always verify – will be critical to keeping bad actors at bay.

A Zero Trust Security framework requires all users to verify their identity before gaining access to valuable information. Even after users are authenticated once, they will need to continue verifying their identity each time they attempt to regain access. Each user and device should be authenticated, meaning ultimate trust in a company's identity proofing strategies will be key.

With a cyber attack happening every 39 seconds, organizations must take a holistic approach to security by combining a number of best practices and technologies in order to effectively fight fraud. As the fraud landscape continues to evolve, companies must stay one step ahead of bad actors. Proactively adapting new technologies as quickly as fraudsters come up with new schemes will be an invaluable line of defense.

About the Author

Blair Cohen is the Founder and President of AuthenticID, a disruptive and transformational identity proofing and fraud prevention technology company. As a dynamic technology entrepreneur with over 30 years of experience, Blair is future-focused and can anticipate industry needs, identify pain points, and then build systems to help organizations improve their bottom line. Prior to turning his focus to solving the biggest challenge on earth, identity, Blair launched several other groundbreaking enterprises and pioneering technology products. Named by One World Identity (OWI) as one of the 100 Most Influential Identity Experts globally, his articles can be found in publications like Fast Company. He frequently speaks at industry conferences focused on identity, risk management, and information security. Blair can be reached on LinkedIn and https://www.authenticid.com/

When it Comes to ZTNA, Buyer Beware

By Denny LeCompete, CEO, Portnox

With traditional perimeter-based defenses proving inadequate thanks to the rise of remote and hybrid work policies, organizations are turning to the concept of zero trust to fortify their security postures. At its core, zero trust centers on the idea that no user or device should be automatically trusted, even when connected to internal networks.

In the initial fury to implement zero trust to combat the security risks posed by dispersed workforces, businesses turned to Zero Trust Network Access (ZTNA) solutions. ZTNA tools exploded onto the scene in the last few years, and the technology was originally pitched as a replacement to virtual private networks (VPNs). The replacement pitch was not without merit. VPN remains ubiquitous, but its broad network-level, encryption-based security is thin and has the potential to expose entire corporate networks to malware, distributed denial of service (DDos), and spoofing attacks.

Instead, ZTNA offered a “never trust, always verify” security approach that requires constant authentication, which spoke to CISOs and their teams looking for a silver bullet to the head-spinning number of new access threats that emerged after the pandemic. And although it’s true – you must start somewhere–the hasty embrace of ZTNA was shortsighted, and has led to further complication, false starts, and budget waste for early adopters.

99 Security Problems, Now ZTNA is 1

While initial ZTNA solutions have undoubtedly marked a notable step forward in addressing remote access security concerns and generally popularizing the concept of zero trust, the technology itself is problematic on several fronts:

Implementation is a Bear

If you've implemented a ZTNA solution, you know it's not a "plug and play" operation. Far from it. Instead, you'll be sidelined by the need to redesign your network architecture from the outset. That may sound dramatic, but it's true. Chances are that your perimeter-based security apparatus can't immediately secure individual applications and verify every access request no matter the network location of the user. So, you're forced to establish an encrypted tunnel between the user and the target application. This means sending traffic externally (likely to a third-party cloud service), and then back to your network to verify the request and authenticate the user.

In short, you've got your work cut out for you from a re-engineering perspective. You also have a greater chance of dealing with latency due to the external traffic routing, which can disrupt productivity. For many, these issues make ZTNA implementation a non-starter, which means it's actually hampering the growth of zero trust adoption.

Physical Networks Are Ignored

Sure, securing access for your remote workforce needs to be a priority – that's not a question. People still work in the office and rely on your organization's physical wired and wireless networks, however. While a balance has largely been struck on hybrid work across most industries, many companies have tamped down on full-time remote work.

This is really just to say that ZTNA misses the mark when it comes to the reach of its zero trust coverage. The same "trust no one, ever" policy needs to be applied to those plugged into the ethernet or connected to the Wi-Fi at the office. Without support for these access layers, companies using ZTNA are forced to adopt another tool (or set of tools) - primarily network access control (NAC) - to define and enforce authentication, authorization, and accounting (AAA) policies for its on-site users. As anyone in IT knows, the more tools you have to manage, the greater the threat surface.

You’re Blind to Endpoint Risk

This is perhaps the most egregious miss for ZTNA. Authentication is great, but as everyone knows, devices are the most used vehicle to compromise enterprise networks and systems. So, if you can’t monitor the risk posture of an endpoint after it connects, you’re out of luck if the device is vulnerable because its anti-virus is out of date, or its firewall is turned off.

Traditional ZTNA does not deliver endpoint risk monitoring or remediation. And since it’s really only focused on applications, it’s not outside the realm of possibility for a device to move laterally across the network after it’s authenticated if the user is sophisticated enough. In this sense, ZTNA can actually make you *more* vulnerable than you even realize. Again, as with the previous problem, this security gap necessitates a solution like NAC, which *can* monitor endpoint risk and remediate devices that fall out of compliance.

Think Bigger, Think Universal Zero Trust

Despite all these problems with ZTNA, there is hope for zero trust, it just requires those considering a move to this security model to expand their mindset. It also means that instead of patching together a portfolio of highly focused security tools like ZTNA or NAC, companies need to invest in unified, cloud-native, and friction-less solutions that can address all key zero trust use cases in a centralized and scalable fashion.

Fortunately, emerging technology is bridging these gaps to deliver “universal zero trust,” which extends zero trust access control to networks, applications and infrastructure for employees, guests and contractors working on-campus and remotely. This is the holy grail of zero trust – where all critical IT assets are covered by a never trust, always verify security model. This is something ZTNA alone cannot do.

About the Author

Denny LeCompete 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/.

Why Compliance Matters When Dealing with AI and Finances

By Saeid Hejazi, Founder, Wally

Artificial intelligence has skyrocketed in popularity in recent months, particularly as the widespread availability and use of AI tools such as ChatGPT have spurred greater interest in technology. Leaders in many businesses and industries — including the financial sector — have seen the potential applications of AI and implemented them in exciting ways.

Nevertheless, it is crucial to adhere to strict compliance and regulatory standards to protect users and their data, especially in a business that deals with sensitive information.

Why compliance standards are important for AI

When people discuss their concerns about artificial intelligence, most people would cite the loss of jobs or the spreading of false information as their primary concerns. However, more people should be concerned about their cybersecurity and privacy being endangered by the use of AI. After all, AI models are able to rapidly process, store, and — perhaps more frighteningly — learn from massive amounts of information. This means that if a hacker can gain access, they have enormous amounts of data available they can then exploit for their own gain.

Compliance standards in the AI industry ensure that AI developers put the right protections in place to minimize or eliminate the risk to the data the algorithm is processing and storing. Some measures that should be standard include a legal obligation not to sell, rent, or share data with third parties, as well as ensuring that all regulatory requirements for data protection are met or exceeded.

What compliance standards are needed for AI

One of the most important considerations when it comes to the use of AI is user consent. From the user's end, it is important to read the terms of use and understand what is being consented to. Meanwhile, from the operator's end, enabling users to understand their consent clearly — such as allowing them to track their consent with intuitive tools and completely delete their data — is necessary not only for accountability, but also for protection to ensure that users are informed of potential risks. This is especially vital for financial companies, whose user data is particularly sensitive.

Companies that implement AI into their practices while handling financial data should also implement stringent cybersecurity standards. The use of bank-level cybersecurity standards can ensure that systems and data are fully encrypted and protected, and any sensitive data stored in the system should have restricted access. Access to this data should only be granted to authorized and verified users with a legitimate reason to view or utilize it.

Additionally, it's important to remember that cybersecurity is about being proactive. Entities employing AI who want to be proactive about protecting their data should pursue penetration and vulnerability testing from a professional service. Through penetration testing, the weaknesses of a program and its cybersecurity measures can be exposed before wrongdoers can ever exploit them, and fixes can be implemented to protect the data.

Still, there are certain types of data that users should avoid inputting into AI programs, and that the entities behind AI programs should avoid collecting and storing, regardless of how strong the system might seem. If an AI program contains user data that is typically valuable to wrongdoers — such as card payment information or usernames and passwords to banking accounts — it is more likely to be targeted for attacks, and therefore far more susceptible to data breaches. After all, the best method to protect against attacks is to prevent the attack from ever happening in the first place.

The truth is that, like any other tool they use, businesses will be held accountable for the risks created by their use of artificial intelligence. That isn't to say that businesses should not implement AI — it is a powerful tool with numerous exciting implications — but it is vital that companies use this technology safely and responsibly. Compliance standards are the best method to ensure that these measures are appropriately met.

About the Author

Saeid Hejazi is the Co-Founder of Wally, a personal finance app that helps people worldwide track and manage their finances. The app is free to download and use, and it connects with 15,000 banks from 70 countries and has been lauded for giving people insights into their finances in a straightforward way.

Saeid graduated from Valley Forge Military Academy and went to study computer science at York University in Canada. After winning a national business plan competition in his senior year, he turned the idea into a startup called Nahel which eventually became the "Amazon of the Middle East" and was later acquired by Aramex in 2013.

Saeid can be reached online at Linkedin and at our company website https://www.wally.me/

EVENTS

CYBER DSA 2023

15 - 17 AUG 2023 | KUALA LUMPUR CONVENTION CENTRE

ADVANCING DIGITALISATION & SECURITY THROUGH COLLABORATION

Have You Registered?

Get ready to connect with the top players in the **cybersecurity industry** at **CyberDSA 2023**

Scan the QR:
***Register** for **FREE Visitor Pass** to Exhibition.*

Scan the QR:
*Ticket for attending **All Access Conference** is now **ON SALE***

Forum & Tracks Schedule:
https://bit.ly/ForumTra cks

www.cyberdsa.com | CyberDSA

SUPPORTED BY:

MINISTRY OF COMMUNICATIONS AND DIGITAL

MALAYSIAN ARMED FORCES

ROYAL MALAYSIA POLICE

STRATEGIC PARTNERS :

DEFENCE CYBER AND ELECTROMAGNETIC DIVISION (MAF)

CyberSecurity MALAYSIA

HELD IN CONJUCTION :

SIBER.SIAGA KUALA LUMPUR | MALAYSIA 2023

MALAYSIA CYBER SECURITY AWARDS

WBF WORLD BLOCKTECH FORUM

ENDORSED BY:

MATRADE

ORGANISER :

AEROSEA EXHIBITIONS SDN BHD
(1315730-A)

IndoSec®

29-30 AUG 2023

AWARDS & GALA DINNER

★ ★ ★

31 AUG 2023
5:00 PM - 9:00 PM

THE RITZ-CARLTON
JAKARTA PACIFIC PLACE

Organised by

TRADEPASS

WORLD CyberCon MIDDLE EAST 2023

MEET ESTEEMED SPEAKERS

Abdullah Alfahaid
CIO, Ajlan & Bros Holding

Abdullah Marghalany
Cybersecurity Chief Officer,
Madinah Health Cluster

Ali Abdulla Alsadadi
Chief Of Information Technology, Ministry of Oil and Environment, Bahrain

Wael Fattouh
Chief Information Security Officer (CISO), Bank Aljazira

Abdullah Alahmade
Chief Information Security Officer & BCM Director, Tamweel Aloula

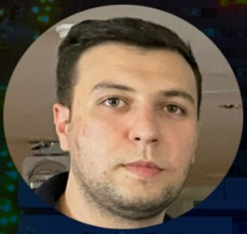
Shenoy Sandeep
Regional Director – META,
Cyble Middle East

Dr. Nasser Alamri
Cybersecurity Executive Director, Institute of Public Administration – IPA – KSA

Eng. Ala Zayadeen
Head of Information Security and Data Privacy,
BinDawood Holding

Jeevan Badigari
Director of Information Security,
DAMAC Properties

Isabelle Meyer
CIO, Zendata Cybersecurity


Ilkin Javadov
Senior Penetration Tester & Ethical Hacker

Augustin Kurian
Editor-In-Chief,
The Cyber Express

Ayad (Ed) Sleiman
Head of Special Projects,
KAUST

Mousab AlSaaydeh
CS Risk Management Consultant,
stc

**AUG 30, 2023,
RIYADH, SAUDI ARABIA**

REGISTER NOW

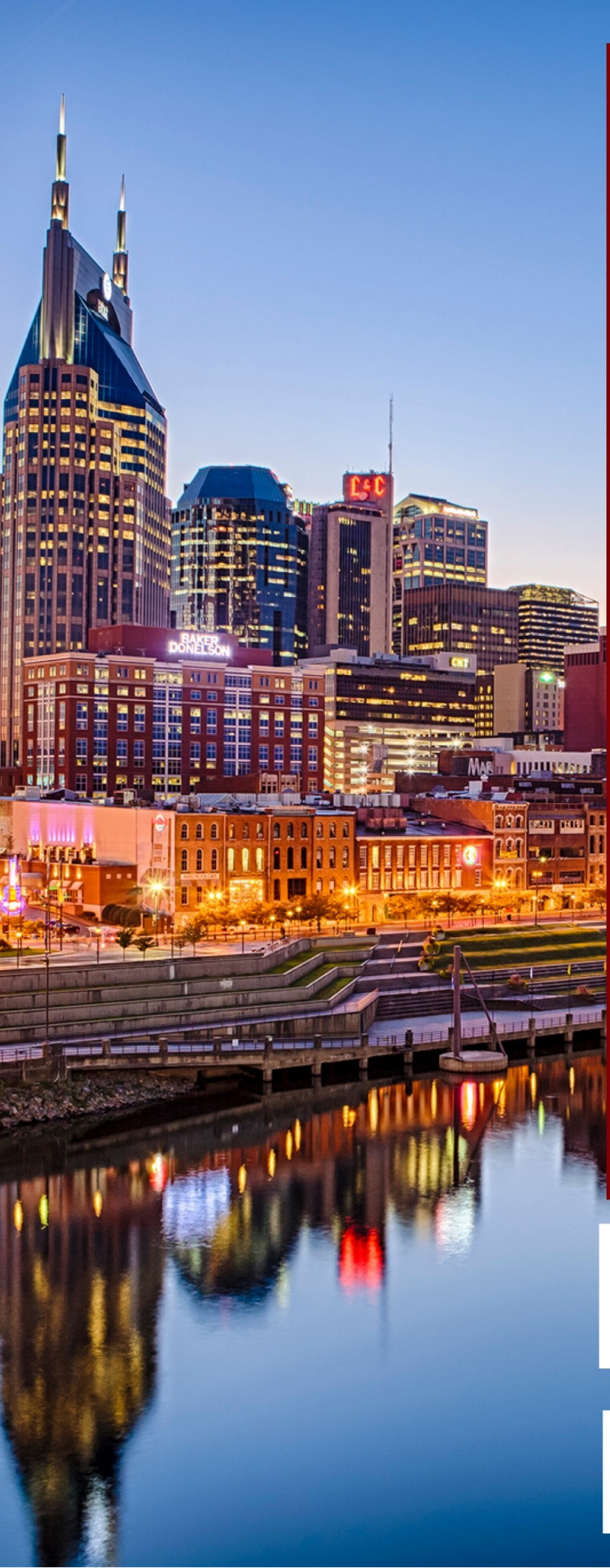
thecyberexPress.com/events

EVENT PARTNERS

CYBLE
potech PATHS OF TECHNOLOGY
ZENDATA
INDEX GLOBAL

MEDIA PARTNERS

CYBER DEFENSE MAGAZINE
INTERNATIONAL BUSINESS MAGAZINE
ACNNEWSWIRE
CIO TECH OUTLOOK
WORLD BUSINESS OUTLOOK
siliconindia
GlobalRisk Community
WIRE19



TECHEX
EUROPE

Co-Located Events:

CYBER SECURITY & CLOUD EXPO
EUROPE

IOT TECH EXPO
EUROPE

BLOCKCHAIN EXPO
EUROPE

AI & BIG DATA EXPO
EUROPE

EDGE COMPUTING EXPO
EUROPE

DIGITAL TRANSFORMATION WEEK

CYBER SECURITY & CLOUD EXPO

EUROPE

26-27 September 2023,
RAI, Amsterdam

The Cyber Security & Cloud Expo will host two days of top-level content and thought leadership discussions around Cyber Security & Cloud, and the impact they are having on industries including government, energy, financial services, healthcare and more.

6 Co-Located Events

8 Conference Tracks

250+ Speakers

150+ Exhibitors

6,000+ Attendees

76% of attendees are **Director Level & above**

Register now for free tickets!

> www.**cybersecuritycloudexpo**.com/northamerica
> enquiries@techexevent.com

in f 🐦

Contact:
> www.**techexevent**.com
> enquiries@techexevent.com

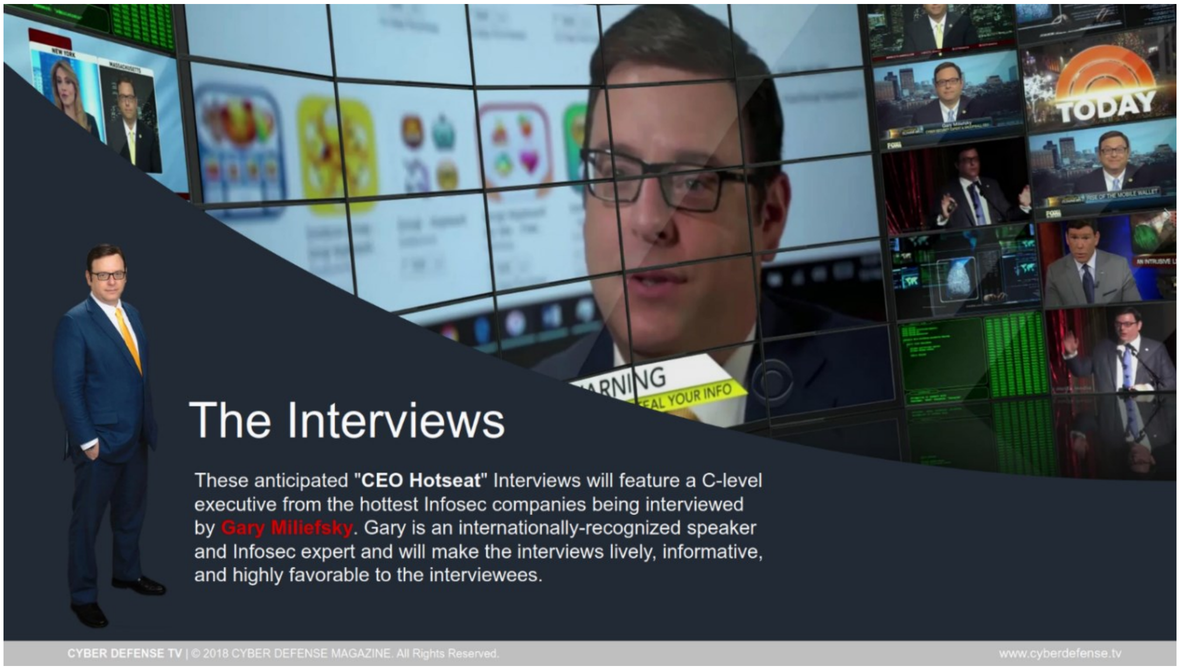
CYBER DEFENSE TV

INFOSEC KNOWLEDGE IS POWER

CyberDefense.TV now has 200 hotseat interviews and growing…

Market leaders, innovators, CEO hot seat interviews and much more.

A division of Cyber Defense Media Group and sister to Cyber Defense Magazine.



The Interviews

These anticipated "**CEO Hotseat**" Interviews will feature a C-level executive from the hottest Infosec companies being interviewed by Gary Miliefsky. Gary is an internationally-recognized speaker and Infosec expert and will make the interviews lively, informative, and highly favorable to the interviewees.

CYBER DEFENSE TV | © 2018 CYBER DEFENSE MAGAZINE. All Rights Reserved.

www.cyberdefense.tv

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.

Copyright (C) 2023, Cyber Defense Magazine, a division of CYBER DEFENSE MEDIA GROUP (STEVEN G. SAMUELS LLC. d/b/a) 276 Fifth Avenue, Suite 704, New York, NY 10001, Toll Free (USA): 1-833-844-9468 d/b/a CyberDefenseAwards.com, CyberDefenseConferences.com, CyberDefenseMagazine.com, CyberDefenseNewswire.com, CyberDefenseProfessionals.com, CyberDefenseRadio.com,and CyberDefenseTV.com, is a Limited Liability Corporation (LLC) originally incorporated in the United States of America. Our Tax ID (EIN) is: 45-4188465, Cyber Defense Magazine® is a registered trademark of Cyber Defense Media Group. EIN: 454-18-8465, DUNS# 078358935. All rights reserved worldwide.
marketing@cyberdefensemagazine.com

Because of the dynamic nature of the Internet, any Web addresses or links contained in this newsletter may have changed since publication and may no longer be valid. The views expressed in this work are solely those of the author and do not necessarily reflect the views of the publisher, and the publisher hereby disclaims any responsibility for them. Send us great content and we'll post it in the magazine for free, subject to editorial approval and layout. Email us at marketing@cyberdefensemagazine.com

Cyber Defense Magazine

276 Fifth Avenue, Suite 704, New York, NY 1000

EIN: 454-18-8465, DUNS# 078358935.

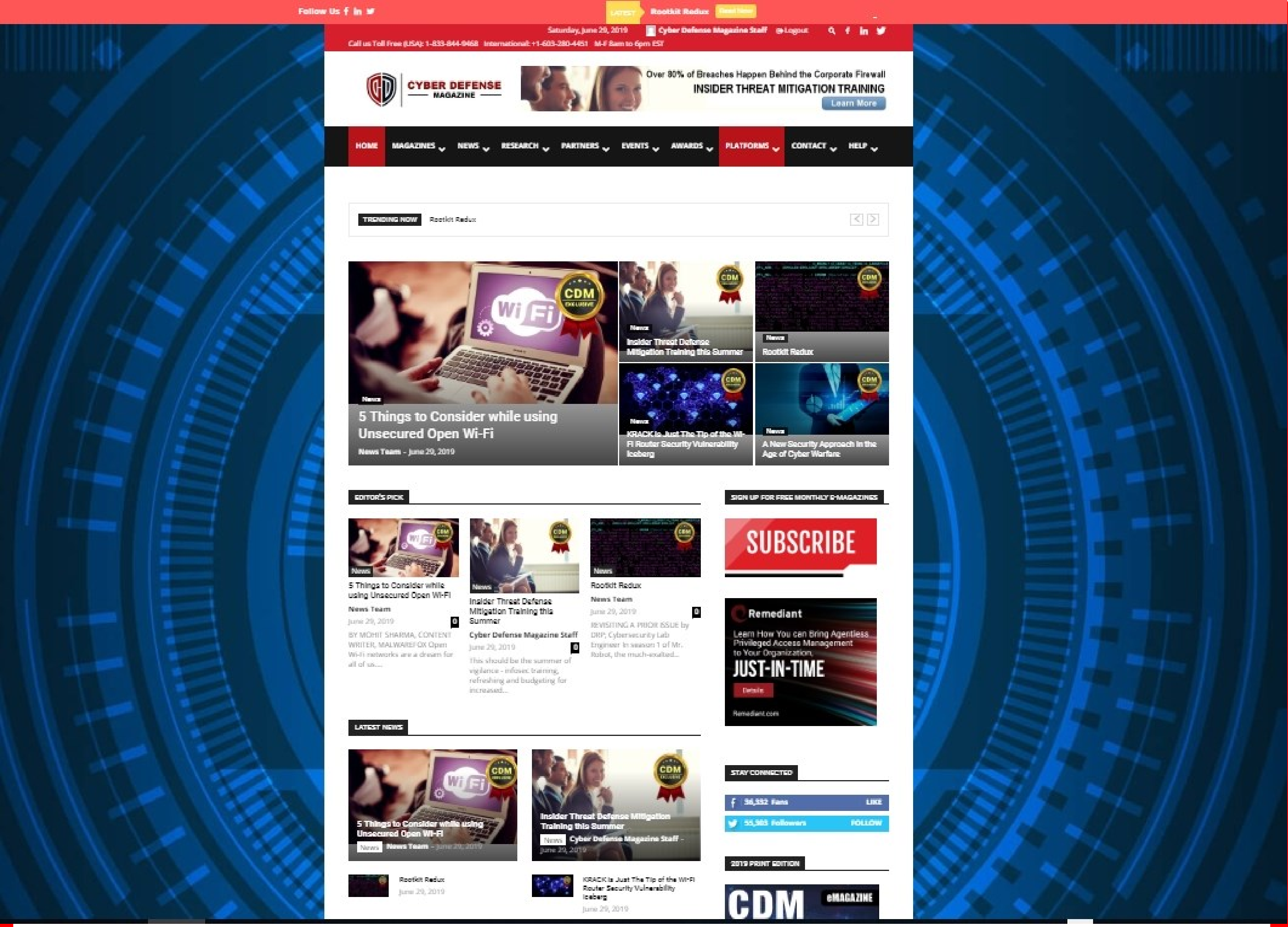
All rights reserved worldwide.

marketing@cyberdefensemagazine.com

www.cyberdefensemagazine.com

NEW YORK (US HQ), LONDON (UK/EU), HONG KONG (ASIA)

Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 08/01/2023



Saturday, June 29, 2019 Cyber Defense Magazine Staff Logout

Call us Toll Free (USA): 1-833-844-9468 International: +1-603-280-4451 M-F 8am to 6pm EST

Over 80% of Breaches Happen Behind the Corporate Firewall

INSIDER THREAT MITIGATION TRAINING

TRENDING NOW Rootkit Radux

News

5 Things to Consider while using Unsecured Open Wi-Fi

News Team - June 29, 2019

News

Insider Threat Defense Mitigation Training this Summer

News

Rootkit Radux

News

KRACK Is Just The Tip of the Wi-Fi Router Security Vulnerability Iceberg

News

A New Security Approach in the Age of Cyber Warfare

EDITOR'S PICK

News

5 Things to Consider while using Unsecured Open Wi-Fi

News Team

June 29, 2019 0

BY MOHIT SHARMA, CONTENT WRITER, MALWAREFOX Open Wi-Fi networks are a dream for all of us....

News

Insider Threat Defense Mitigation Training this Summer

Cyber Defense Magazine Staff

June 29, 2019 0

This should be the summer of vigilance - infosec training, refreshing and budgeting for increased...

News

Rootkit Radux

News Team

June 29, 2019 0

REVISITING A PRIOR ISSUE by DRP, Cybersecurity Lab Engineer In season 1 of Mr. Robot, the much-exalted...

SIGN UP FOR FREE MONTHLY E-MAGAZINES

Remediant

Learn How You can Bring Agentless Privileged Access Management to Your Organization,

JUST-IN-TIME

Remediant.com

LATEST NEWS

5 Things to Consider while using Unsecured Open Wi-Fi

News News Team - June 29, 2019

Insider Threat Defense Mitigation Training this Summer

News Cyber Defense Magazine Staff - June 29, 2019

Rootkit Radux

June 29, 2019

KRACK Is Just The Tip of the Wi-Fi Router Security Vulnerability Iceberg

June 29, 2019

STAY CONNECTED

36,332 Fans LIKE

55,385 Followers FOLLOW

2019 PRINT EDITION

Books by our Publisher: https://www.amazon.com/Cryptoconomy-Bitcoins-Blockchains-Bad-Guys-ebook/dp/B07KPNS9NH (with others coming soon...)

11 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 have another amazing platform coming soon.

CDM
CYBER DEFENSE MAGAZINE
THE PREMIER SOURCE FOR IT SECURITY INFORMATION
eMAGAZINE
www.cyberdefensemagazine.com

"Cyber Defense Magazine is free online every month. I guarantee you will learn something new you can use to help you improve your InfoSec skills."
Gary S. Miliefsky, Publisher & Cybersecurity Expert

* with help from writers
and friends all over the Globe.