CYBER DEFENSE MAGAZINE

eMAGAZINE

SEPTEMBER 2023

In This Edition

MORE INSIDE!

`

CONTENTS

@MILIEFSKY

From the

Publisher…

TOP INFOSEC INNOVATOR
CYBER DEFENSE MAGAZINE
2023

Dear Friends,

This September, the view from the Publisher's desk reflects what might be called a mixed metaphor: even though we have our feet planted firmly on the ground, we enjoy the benefit of a 30,000-foot view of the cybersecurity industry. In publishing Cyber Defense Magazine, in coordination with the other functions of Cyber Defense Media Group, we can see both granular detail and high-altitude perspective on the challenges and responses to the most pressing issues.

One of the most prominent results of this capability is our view of the intersection of Zero Trust Architecture (ZTA) and Artificial Intelligence (AI). On one hand, there is the implicit incompatibility of the two concepts; on the other, they represent a nearly codependent relationship between two powerful forces.

It is incumbent upon our base of CISOs and other cybersecurity professionals to delve into, understand, and implement the most effective means of harmonizing artificial intelligence and machine learning with zero trust practices and human vulnerabilities.

To that end, Cyber Defense Media Group provides a variety of platforms for the exchange of information and education of both professionals and other interested decision-makers. These facilities include articles in the monthly magazine, CyberDefense TV interviews, and recognition of outstanding professionals through our 11th Annual Awards program at https://www.cisoconference.com.

With appreciation for 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

PUBLISHER
Gary S. Miliefsky, CISSP®

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

11 YEARS ★★★★★ ANNIVERSARY

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 September 2023 Issue

From the Editor-in-Chief

Continuing the Cyber Defense Magazine trend of keeping up with the most pressing issues in cybersecurity as well as broadening our base of readers, we are pleased to publish this September issue.

We believe that we have been successful in reaching an effective balance between deeply technical articles and accessible explanations of such challenges as AI-aided phishing attacks. In this way we can strengthen our value proposition to both cybersecurity professionals and to the non-technical executives of organizations which employ them.

As in recent issues, we continue to recognize the spread of cyber threats and the required responses to overcome them. While we place a sharp focus on the future of AI, there is no room for anyone to become less vigilant in assuring that all of the more traditional measures are implemented 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

RSAConference™2024

San Francisco | MAY 06-09 | Moscone Center

Stronger Together

See for yourself why we are **Stronger Together.**

RSA Conference 2024 is your opportunity to join the global cybersecurity community for a rich experience filled with cutting-edge insights and skill-building activities.

From MAY 06-09 , you'll get the chance to:

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

Learn more and register at rsaconference.com/cyberdefense23

#RSAC

FOLLOW US

NIGHTDRAGON

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

-David DeWalt

Managing Director and Founder NightDragon Security

ADVISE

WE DELIVER SOUND ADVICE AS YOUR FINANCIAL PARTNERS

INVEST

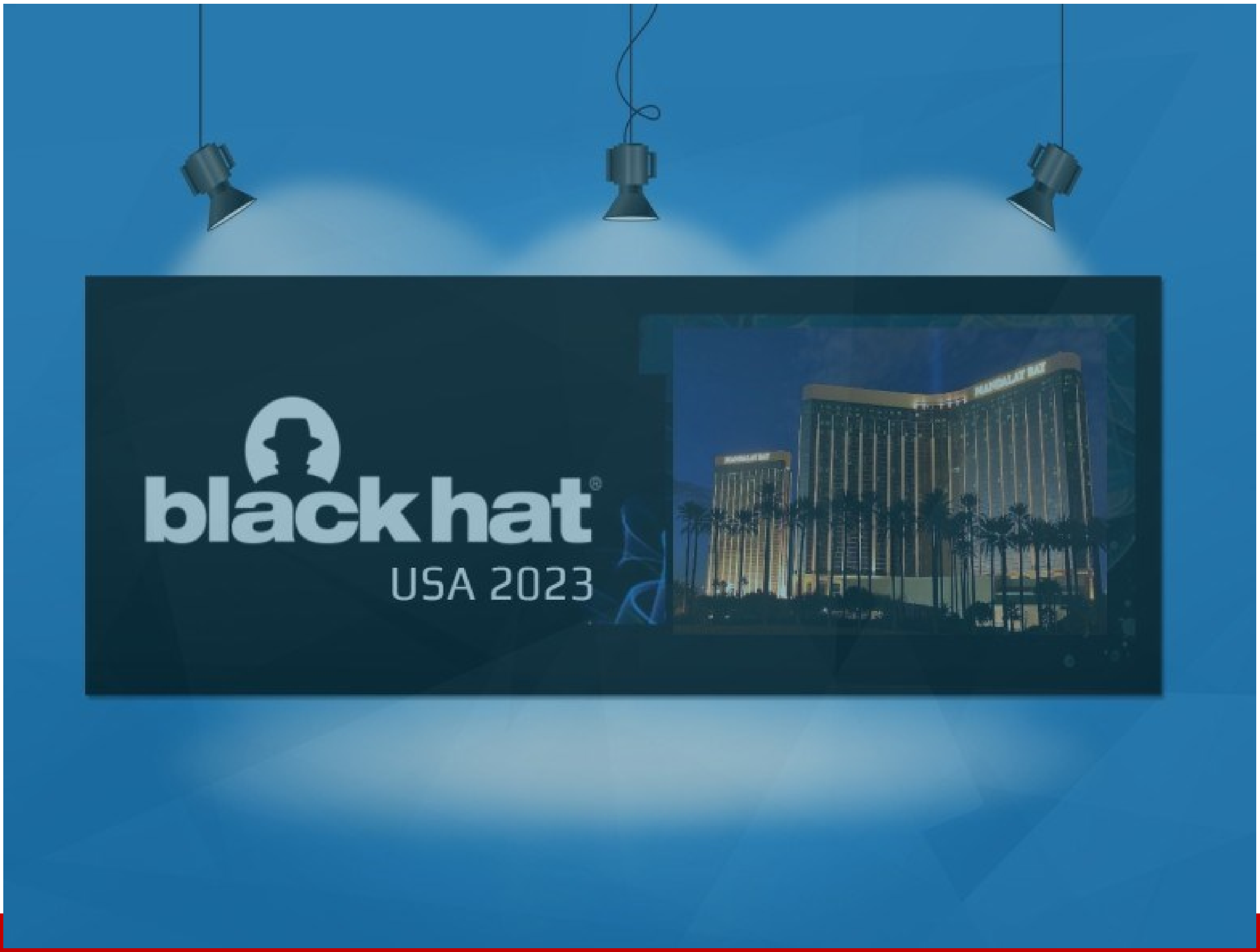
WE ARE FLEXIBLE INVESTORS ACROSS ALL STAGES OF GROWTH TO PRE-IPO

ACCELERATE

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

www.nightdragon.com

ARTICLES



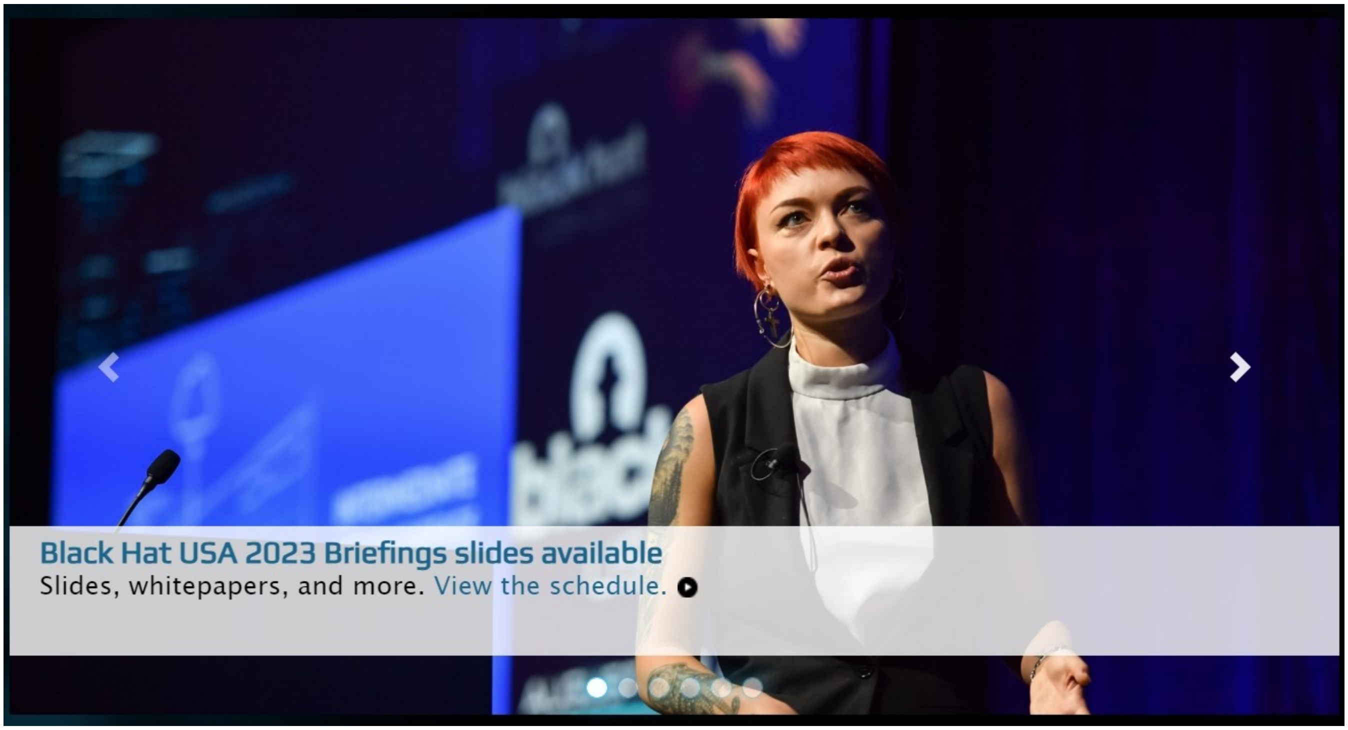
Publisher's Trip Report: Black Hat USA 2023

By Gary Miliefsky, Publisher & Author

I had the pleasure of attending Black Hat USA 2023 this year as well as Squadcon, while some of our reporters attended Defcon as well.

I met so many innovative cybersecurity companies at Black Hat this year, that I could not fit them all in one article, so I'm doing 1 to 2 page spotlights on each of them on the homepage of the magazine's website https://www.cyberdefensemagazine.com.

Black Hat, the producer of the cybersecurity industry's most established and in-depth security events, shared with me, the successful completion of the in-person component of Black Hat USA 2023. The event welcomed more than 22,750 unique attendees, with 19,750 joining in-person at the Mandalay Bay Convention Center in Las Vegas, while more than 3,000 registered for On-Demand Access to the event.



Black Hat USA 2023 Briefings slides available

Slides, whitepapers, and more. View the schedule.

Security professionals from 127 countries registered to attend the event and experience firsthand the latest in research, development, and trends in Information Security (InfoSec), through 92 deeply technical hands-on Trainings and 98 Briefings presenting the latest research and vulnerability disclosures.

“We look forward to Black Hat USA every year and the opportunity to connect in person with our community, Partners, and Sponsors,” said Steve Wylie, Vice President, Cybersecurity Market Group at Informa Tech. “We appreciate everyone who makes the journey to Las Vegas each August to attend Black Hat USA, and it is our hope that all attendees leave the event feeling energized from making new connections and from learning actionable information and best practices from the greatest minds in the security industry.”

Show highlights for 2023 included:

- **Keynotes:** The three Keynotes this year included Maria Markstedter, Founder of Azeria Labs; Jen Easterly, Director of the Cybersecurity and Infrastructure Security Agency (CISA), and Victor Zhora, Deputy Chairman of Ukraine’s State Service of Special Communication and Information Protection; and Kemba Walden, Acting National Cyber Director in the Office of the National Cyber Director, and Jason Healey, Senior Research Scholar at Columbia University’s School for International and Public Affairs. All Keynotes featured in-depth discussions into the current state of the cybersecurity landscape.
- **Omdia Analyst Summit:** The third annual Omdia Analyst Summit featured the industry’s leading cybersecurity analysts, focused on the theme, “Maximum Attention, Minimum Budget.” The Omdia team surfaced valuable insights from its latest Cybersecurity Decision Maker survey, alongside the latest cybersecurity trends, market updates, observations, projections, and insights through a series of presentations, panels, and fireside chats.

- **Business Hall:** This year's Business Hall welcomed more than 440 of the industry's leading information security solution providers, showcasing their latest products and technologies to attendees on-site, both on and off the Business Hall floor. The Business Hall also featured focused areas for attendee, vendor, and community engagement through Arsenal, Sponsored Sessions, the Community Lounge, Community Program, Meet & Greet sessions, and the Meetup Lounge.
- **Startup Spotlight Competition:** The Black Hat Startup Spotlight Competition is a video pitch contest for cybersecurity startup companies interested in presenting their products and solutions in front of a live audience at Black Hat USA. During Black Hat USA 2023, the top four finalists each had the opportunity to pitch the benefits of their respective products and/or solutions to the panel of judges, and then answer follow-up questions from the judges in real time. Additionally, all finalists were invited to exhibit at Black Hat USA 2023 and received a 10-minute scheduled speaking slot and 30-minute call with an Omdia Cybersecurity Analyst. Once all finalists presented and the judges deliberated, the 2022 winner, Phylum, officially announced Mobb as the winner for 2023.
- **Scholarships:** As a way to introduce the next generation of security professionals to the Black Hat community, Black Hat awarded a total of 306 complimentary Black Hat USA 2023 Briefings passes. Black Hat holds its own annual Student and Veteran Scholarship programs, partnering with a variety of associations on additional scholarship opportunities.
- **Network Operations Center (NOC):** As a key component of Black Hat USA, the Black Hat Network Operations Center (NOC) provided a high security, high availability network in an intensely demanding environment. Each year, the hand-selected NOC team meets before Black Hat USA to incorporate the latest infrastructure and security solutions into a workable network design. Black Hat attendees may then visit the NOC for a glimpse into this state-of-the-art network.

Top Partners and Sponsors of Black Hat USA 2023 include:

Titanium Sponsors: CrowdStrike, Darktrace, KnowBe4, Qualys, and SentinelOne; Diamond Sponsors: Armis, BlackBerry, Cisco, IBM, Palo Alto Networks, Sophos, Tenable, Trellix, Trend Micro, and VMware Carbon Black; Global Partners: Adaptive Shield, Akamai, Appdome, ARCON, Armis, Binalyze, Bugcrowd, Contrast Security, Corellium, CYBER RANGES, DataDome, INE, KnowBe4, Kondukto, ManageEngine, Snyk, Sonar, Swimlane, Synopsys, Veracode, and wolfSSL; Sustaining Partners: Akamai, Armis, Axonius, Cisco, Claroty, CrowdStrike, IBM, Kandji, KnowBe4, Lacework, ManageEngine, Microsoft, Mimecast, Pentera, ServiceNow, Snyk, Sysdig, VMware Carbon Black, Wiz, and XM Cyber.

For more information on Black Hat events, please visit https://www.blackhat.com.

About Black Hat

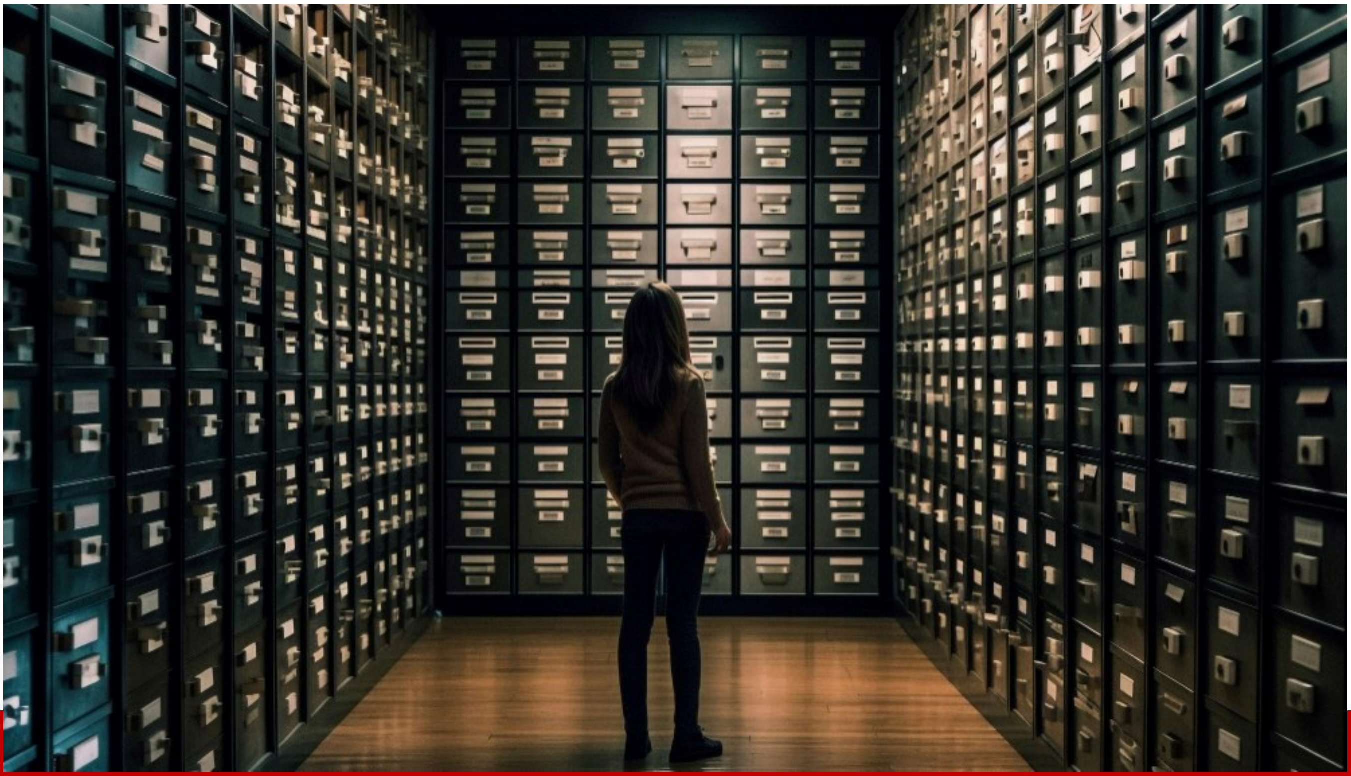
For over 25 years, Black Hat has provided attendees with the very latest in information security research, development, and trends. These high-profile global events and trainings are driven by the needs of the security community, striving to bring together the best minds in the industry. Black Hat inspires professionals at all career levels, encouraging growth and collaboration among academia, world-class researchers, and leaders in the public and private sectors. Black Hat Briefings and Trainings are held annually in the United States, Canada, Europe, Middle East and Africa, and Asia. More information is available at: blackhat.com. Black Hat is brought to you by Informa Tech.

About Informa Tech

Informa Tech is a market leading provider of integrated research, media, training, and events to the global Technology community. We're an international business of more than 600 colleagues, operating in more than 20 markets. Our aim is to inspire the Technology community to design, build, and run a better digital world through research, media, training, and event brands that inform, educate, and connect. Over 7,000 professionals subscribe to our research, with 225,000 delegates attending our events and over 18,000 students participating in our training programmes each year, and nearly 4 million people visiting our digital communities each month. For more information, please visit www.informatech.com.

About the Publisher

Gary Miliefsky, Publisher & Author. Gary Miliefsky is an internationally recognized cybersecurity expert, bestselling author and keynote speaker. He is a Founding Member of the US Department of Homeland Security, served on the National Information Security Group and served on the OVAL advisory board of MITRE responsible for the CVE Program. He founded and is the Publisher of Cyber Defense Magazine since 2012. Visit Gary online at: https://www.cyberdefensemagazine.com/



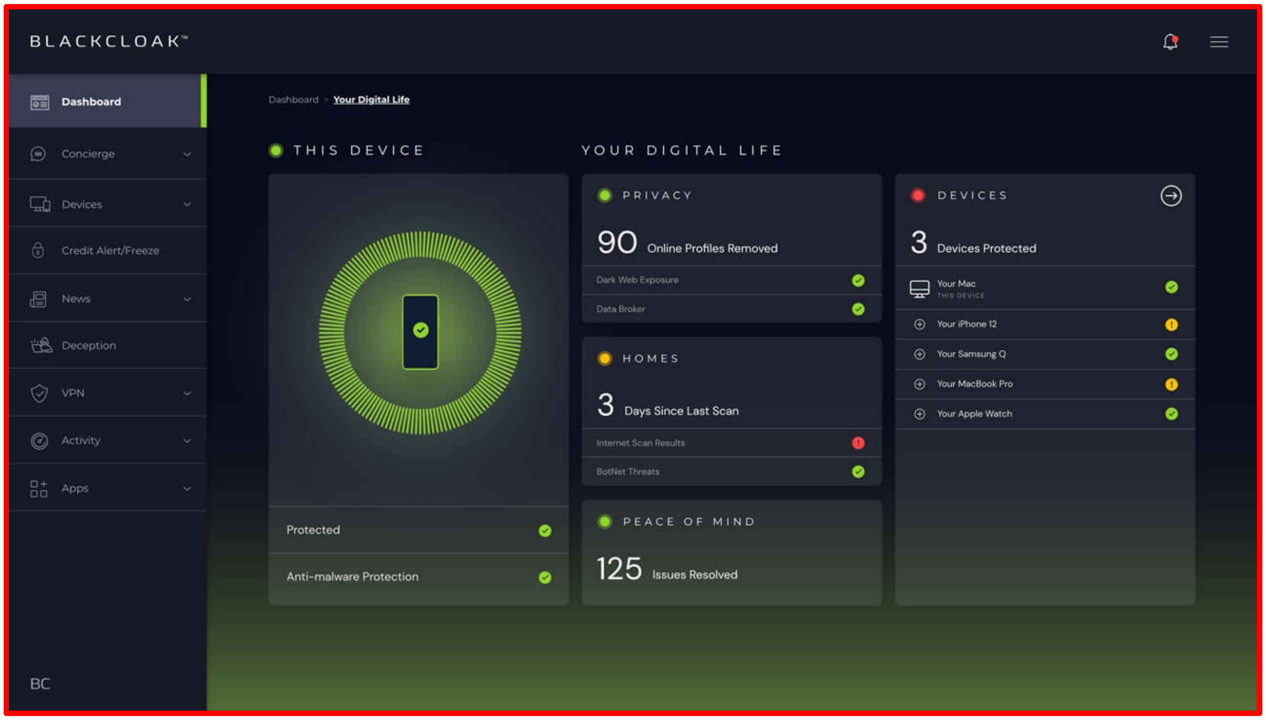
Defending Beyond 9-to-5: BlackCloak's Fortress for Executives' Digital Sanctuaries

By Annabelle Klosterman, Cybersecurity Reporter, Cyber Defense Magazine

Overwhelming would be an understatement while walking through the 2023 BlackHat USA’s business hall. They featured over 440 of the industry’s leading information security solution providers. However - one stood out among all the others. That is BlackCloak. During an insightful conversation with Chris Pierson, the CEO and Founder, I learned about BlackCloak's unique offering – digital executive protection for companies. Unlike most cybersecurity solutions that focus on the usual 9am-5pm business hours, BlackCloak extends its security coverage to the often neglected 5pm-9am personal side. The company's unique approach to cybersecurity, focusing on the personal side of digital lives, has positioned it at the forefront of safeguarding executives, their families, and their valuable data.

A Shifting Landscape of Cybersecurity Challenges

The world of cybersecurity is in constant flux, with cybercriminals continuously refining their tactics to breach the seemingly impenetrable barriers put in place by security professionals. With the advent of sophisticated social engineering techniques, attacks on executives have escalated, targeting the softer entry points represented by their personal digital lives. Conventional security measures, designed to protect corporate networks during business hours, often fall short when it comes to fortifying the extended perimeter of executives' private lives.



BlackCloak Platform Dashboard

BlackCloak recognizes this shift in the threat landscape and has developed a revolutionary solution to counteract it. While many cybersecurity solutions focus on business hours, BlackCloak provides a comprehensive platform that offers digital executive protection beyond the traditional workday. Partnering with CISOs, security teams, and C-suite executives, the company's award-winning Concierge Cybersecurity & Privacy™ Platform bridges the gap between professional and private digital lives.

Addressing the Vulnerabilities

BlackCloak's platform addresses vulnerabilities that have been increasingly exploited by cybercriminals. The Ponemon Institute's report on Understanding the Serious Risks of Executives' Personal Cybersecurity & Digital Lives underscores the severity of the issue. Cyberattacks against executives can lead to the theft of sensitive financial data, loss of business partners, intellectual property theft, and even improper access to the executive's home network. The risk is real: criminals are attacking the digital assets and lives of executives and their families. The two most common cyberattacks are doxxing (57% of respondents) and malware infections on personal or family devices (56% of respondents).

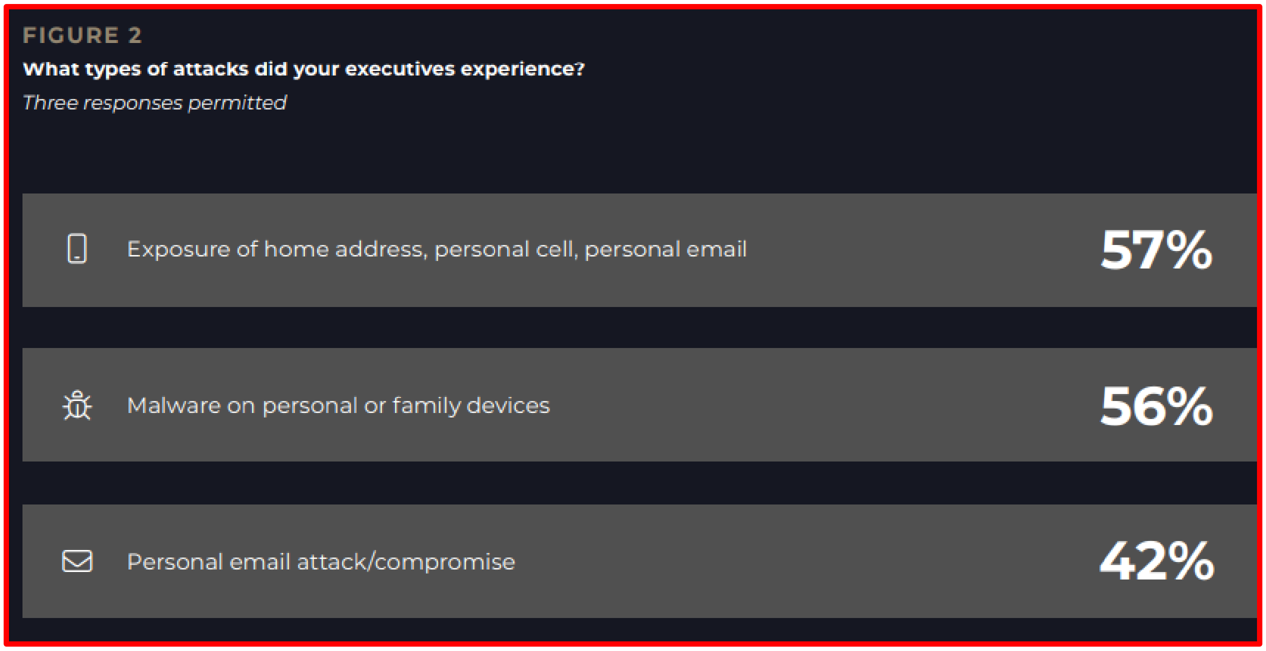


FIGURE 2

What types of attacks did your executives experience?

Three responses permitted

Exposure of home address, personal cell, personal email	57%
Malware on personal or family devices	56%
Personal email attack/compromise	42%

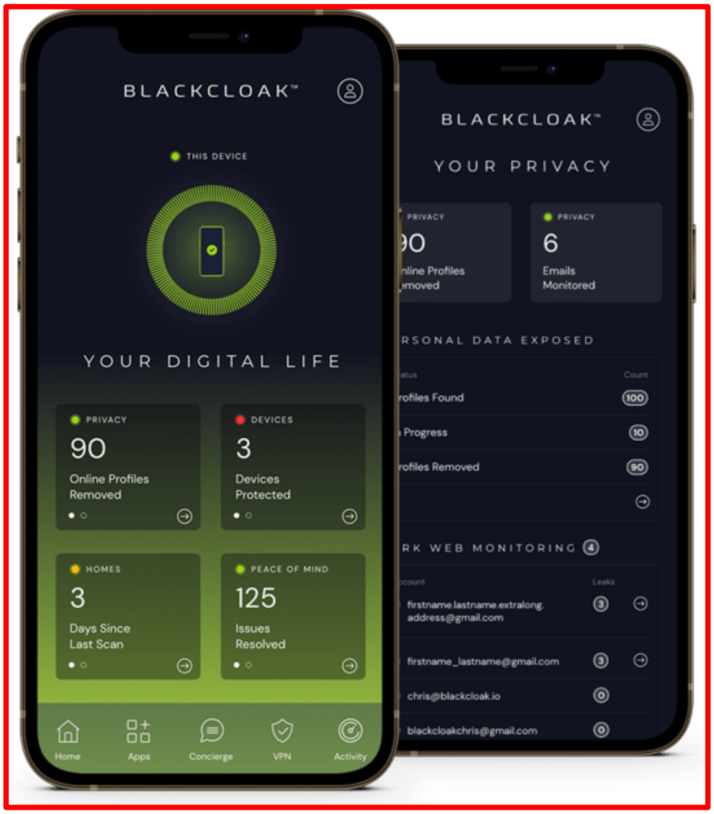
Figure 2 from the Ponemon Institute report

Notably, the human element remains a critical attack vector, and executives are often the preferred targets due to their high-profile status. Cybercriminals have shifted their attention from corporate networks to the softer targets of executives' home networks, where weak passwords and lax security measures are more prevalent. High-profile incidents such as the 2022 data breaches at Twilio and Uber serve as stark reminders of the potential consequences of inadequately securing personal digital assets.

Cybercriminals were able to gain access to sensitive company information at Twilio through a sophisticated social engineering approach that involved phishing texts designed to bypass the two-factor authentication (2FA) they used to protect their system. Similarly, bad actors were able to breach Uber's systems with a social engineering text attack in 2022. However, it is not enough to defend against social engineering attacks — last year, criminals were able to enter Lastpass's secure servers by remotely accessing an engineer's home computer through exploiting a weakness in a third-party software package.

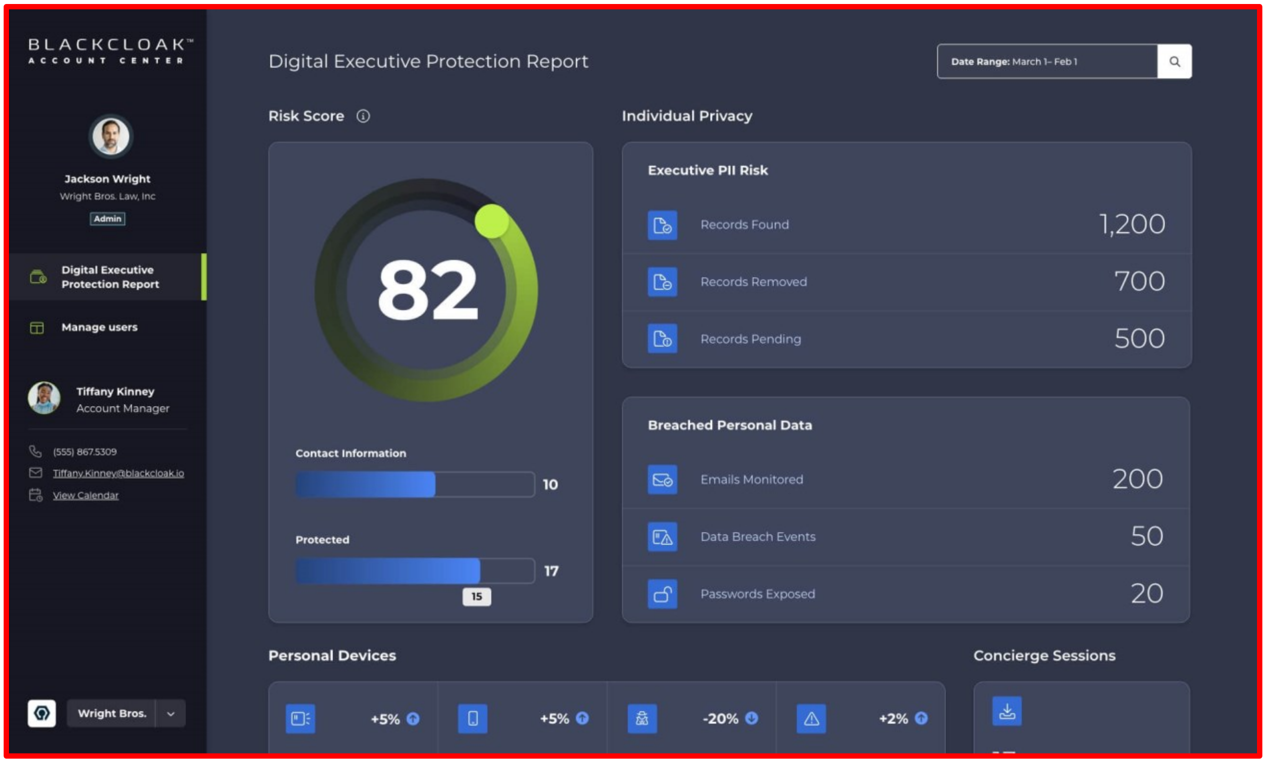
The BlackCloak Solution

BlackCloak has not only identified these vulnerabilities but has also developed a holistic solution to counteract them. They created a service that provides the solution. Digital executive protection from BlackCloak is a powerful, holistic approach to securing the private digital lives and assets of C-Suite executives and other high profile individuals such as board members, senior and executive leadership teams and other key personnel and their families from threats such as cyberattack, impersonation, harassment, and identity theft.



BlackCloak App

BlackCloak’s award-winning Concierge Cybersecurity & Privacy™ Platform combines sleek mobile and desktop applications with white glove concierge service. This unique approach allows executives and their families to maintain privacy and peace of mind, while benefiting from the same level of protection that they would experience inside the traditional perimeter of an organization’s network. The end goal is to provide users with secure, seamless protection that allows for the frictionless transition between private and professional digital lives.



BLACKCLOAK™ ACCOUNT CENTER

Jackson Wright
Wright Bros. Law, Inc
Admin

Digital Executive Protection Report

Manage users

Tiffany Kinney
Account Manager

(555) 867.5309
Tiffany.Kinney@blackcloak.io
View Calendar

Wright Bros.

Digital Executive Protection Report

Date Range: March 1– Feb 1

Risk Score

82

Contact Information: 10

Protected: 17 (15)

Individual Privacy

Executive PII Risk

Records Found	1,200
Records Removed	700
Records Pending	500

Breached Personal Data

Emails Monitored	200
Data Breach Events	50
Passwords Exposed	20

Personal Devices

+5% | +5% | -20% | +2%

Concierge Sessions

BlackCloak CISO Dashboard

Dr. Chris Pierson, Founder & CEO of BlackCloak, emphasizes the urgency of this paradigm shift in cybersecurity. "Cybercriminals have changed their tactics of attack and are looking outside the castle walls for executives and their families as a means to target them, cause real harm, and penetrate the company through a home network. The emergence of this change has been swift, the calls from CISOs more panicked, and the solution for holistic Digital Executive Protection never more clear. The home is the new battleground for corporate security." comments Pierson.

The Time Is Now

In a rapidly evolving digital landscape where cyber threats transcend traditional boundaries, BlackCloak's pioneering approach to cybersecurity offers a beacon of hope. By focusing on the protection of executives' personal digital lives, the company addresses vulnerabilities that have long been overlooked by conventional security measures. They strive to empower executives to safeguard their families, digital assets, and personal well-being, while ensuring the continuity of secure and seamless professional engagements.

As cybercriminals adapt their tactics, the need for proactive, holistic cybersecurity solutions has never been more critical. BlackCloak's dedication to securing the private digital lives of executives signifies a pivotal step towards achieving this goal, ensuring that the battleground of corporate security extends into the homes of those who lead organizations into the digital future.

About the Author

Annabelle Klosterman is a Cybersecurity Reporter for Cyber Defense Magazine (CDM) and CDM's first Women in Cybersecurity scholarship awardee. She is the Technology Manager at First Farmers & Merchants Bank and the Co-Founder/Program Director of the Cyber Community Club. She obtained her Bachelors of Cyber Operations in 2022 and Master's of Cyber Defense in 2023 at Dakota State University. Her areas of focus are offensive and defensive security, governance, risk and management, security consulting, program management, and cybersecurity training/outreach.

Throughout the years, Annabelle has competed in numerous competitions and placed nationally at the Collegiate Cyber Defense Competition in 2022 and 2023 and was a national finalist in CyberPatriot in 2019 and 2020. Additionally, she earned 1st place in the 2022 Idaho National Laboratory CyberCore CTF, and Women in Cybersecurity (WiCyS) CTF in 2021 and 2022. She holds SANS certifications in Cybersecurity Technologies (GFACT), Cloud Security (GCLD), and Incident Handling (GCIH).

Annabelle has spoken on cybersecurity and career topics at various events and organizations including US Cyber Games, RSA Conference, Secure360, Texas Cyber Summit, BSidesSATX, South Dakota InfraGard, Civil Air Patrol, and more. Annabelle's goal is to be in a position that changes the way people view and handle security, for their protection and safety, and the benefit of everyone. Annabelle can be reached online at https://www.linkedin.com/in/annabelleklosterman and at her website https://www.annabelleklosterman.com/

Cybersecurity Implications of AI

A Guide to Staying Secure

By Sercan Okur, VP of Engineering, NextRay AI

Introduction to the Cybersecurity Implications of Artificial Intelligence

Artificial Intelligence is revolutionizing various industries, bringing about incredible advancements in healthcare, transportation, and more. However, along with these revolutionary advancements come significant cybersecurity risks that must be addressed.

Data Privacy: AI models rely on vast amounts of data for training purposes. If not handled properly, this data could become vulnerable to breaches, leading to the exposure of sensitive information such as personal medical records or financial data.

Adversarial Attacks: Sophisticated attackers can manipulate AI models by making subtle changes to the input data. This may result in incorrect decisions or predictions, posing a threat to the accuracy and reliability of AI systems.

Bias and Discrimination: Biased data used to train AI models can result in biased outcomes, leading to unfair or discriminatory decisions. Imagine being unjustly denied a loan due to biased algorithms - it's a clear violation of fairness and equality.

Automated Attacks: AI-powered cyber-attacks have the potential to automate and scale traditional hacking techniques, making them more efficient and devastating. Imagine an AI system turned against its owner, launching automated attacks with unprecedented speed and precision.

Understanding the Cybersecurity Risks of Artificial Intelligence

Artificial Intelligence brings about unique cybersecurity challenges that cannot be overlooked. With the increasing adoption of AI across various industries, it is crucial to understand and address these risks to ensure the security and trustworthiness of AI-driven systems. By staying informed and proactive, we can take control of our AI-driven future while mitigating the associated cybersecurity risks.

The Role of Data Privacy in AI Security

Data privacy plays a vital role in ensuring AI security. AI models rely heavily on vast amounts of data, and if this data is not properly protected, it can lead to serious breaches and privacy violations. Sensitive information, such as personal medical records or financial data, falling into the wrong hands can have severe consequences.

Implementing strong data governance measures, including encryption, access controls, and regular monitoring, is crucial to protecting the privacy and integrity of AI data. Regular security testing of AI systems can also help detect vulnerabilities and ensure timely remediation, minimizing the risk of data breaches.

Adversarial Attacks: A New AI Security Challenge

One of the major cybersecurity risks posed by artificial intelligence is adversarial attacks. Sophisticated attackers can manipulate AI models by making subtle changes to the input data. This can lead to incorrect decisions or predictions, potentially causing significant harm. Imagine your self-driving car being tricked into misinterpreting a stop sign, or a medical AI device making erroneous and harmful predictions due to manipulated input data.

To mitigate adversarial attacks, it is essential to conduct regular algorithm audits to identify and address biases or vulnerabilities in the AI models. Additionally, collaboration with cybersecurity experts can provide valuable insights and guidance in developing robust defense mechanisms against adversarial attacks.

Addressing Bias and Discrimination in AI Models

Another significant cybersecurity risk associated with AI is bias and discrimination. If AI models are trained on biased data, they can perpetuate and amplify existing biases, leading to unfair or discriminatory outcomes. To mitigate this risk, it is crucial to implement bias detection and mitigation strategies. Auditing AI models for bias, and implementing unbiased algorithms will help ensure fair decision-making. Collaborating with experts in ethics and diversity can also provide valuable perspectives on identifying and mitigating biases within AI systems.

The Threat of Automated Attacks in AI Systems

Artificial intelligence-powered cyber attacks pose a new and concerning threat in the world of cybersecurity. These attacks can automate and scale traditional hacking techniques, making them more efficient and potentially more damaging. Imagine an AI system turned against its owner, autonomously launching cyber attacks on critical infrastructure or stealing sensitive information. To control and mitigate the risks of automated attacks in AI systems, companies developing AI should prioritize security audits. By regularly assessing the security measures in place through techniques such as penetration testing and vulnerability assessments, potential vulnerabilities can be identified and addressed before they are exploited.

Mitigation Strategies for AI Cybersecurity Risks

To mitigate the cybersecurity risks posed by artificial intelligence, implementing the following strategies is crucial:

1. Implement Strong Data Governance: Protecting the data used in AI models is essential for maintaining privacy and integrity. Encryption, access controls, and regular monitoring should be implemented to ensure that sensitive data is secure.

2. Regular Security Testing: Regularly testing AI systems for vulnerabilities can help identify potential security risks early on and allow for timely remediation.

3. Bias Detection and Mitigation: Auditing AI models for bias and implementing unbiased algorithms can help ensure fair decision-making and mitigate the risks of discriminatory outcomes.

4. Collaboration with Experts: Working with cybersecurity experts can provide valuable insights into potential risks and the latest mitigation strategies.

5. Data Audits: Companies developing AI should conduct data audits to ensure that the data used in AI models is secured and compliant with regulations, protecting sensitive information from falling into the wrong hands.

6. Algorithm Audits: Examining AI algorithms for biases and potential vulnerabilities is crucial in ensuring the fairness and security of AI systems.

7. Compliance Audits: Verifying compliance with laws and regulations related to AI, such as GDPR, can help ensure that AI systems are developed and deployed in a manner that aligns with legal and ethical standards.

8. Security Audits: Regularly assessing the security measures in place, including penetration testing and vulnerability assessments, can help identify and address potential vulnerabilities in AI systems and mitigate the risks of cyberattacks.

By implementing these strategies, companies can proactively address the cybersecurity implications of artificial intelligence and ensure that their AI systems are secure, trustworthy, and resilient to cyber threats. Artificial Intelligence offers remarkable potential, but it also presents new and unique cybersecurity challenges that must be addressed. To address the potential risks and ensure the secure implementation of artificial intelligence, companies must take a comprehensive approach. This includes implementing strong data governance practices to protect sensitive information, regularly testing AI systems for vulnerabilities, detecting and mitigating bias in algorithms, collaborating with cybersecurity experts, and conducting various audits to ensure compliance and security.

In conclusion, the risks posed by artificial intelligence to cybersecurity are significant and require proactive measures to mitigate. Companies must prioritize data privacy, protect against adversarial attacks, address bias and discrimination, and defend against automated attacks. By implementing strong data governance practices, regularly testing AI systems for vulnerabilities, detecting and mitigating bias in algorithms, collaborating with cybersecurity experts, and conducting various audits, companies can take control of their AI-driven future and ensure the security and trust that society expects and deserves. To fully harness the power of AI while maintaining cybersecurity, organizations must regularly conduct algorithmic audits to identify and mitigate bias in data.

They should also prioritize compliance audits to ensure adherence to laws and regulations such as GDPR. By implementing these measures, companies can demonstrate their commitment to maintaining data privacy, fairness, and security in the development and deployment of AI systems. Overall, companies must stay informed and proactive in addressing the cybersecurity implications of artificial intelligence.

By prioritizing cybersecurity measures in AI development, companies can not only protect their systems and data but also contribute to the broader effort of creating a secure digital ecosystem.

About the Author

Sercan Okur is a highly skilled professional with a strong focus on cybersecurity and artificial intelligence. With a wealth of experience in the information technology sector, Sercan has developed a deep understanding of the complex interplay between cybersecurity and AI, striving to stay at the forefront of emerging trends and advancements. His expertise in these areas has enabled him to tackle challenging projects, implement innovative solutions, and contribute to the growth of the cybersecurity industry. As a thought leader and dedicated expert, Sercan actively engages with the professional community on platforms such as LinkedIn, sharing his insights and knowledge in cybersecurity and AI, while fostering collaboration and staying connected with fellow industry experts. Sercan can be reached online on https://www.linkedin.com/in/sercanokur/.

Generative AI: The Vanguard of Cyber Defense

How Generative AI Strengthens Digital Fortresses

By Dean Frankhauser, CEO, PromptPal

In today's digital-first world, where technology continues to integrate deeper into the fabric of our lives, ensuring cyber resilience is paramount. As the battle between cybercriminals and defenders intensifies, a new contender is emerging on the horizon—Generative AI. This innovative technological breakthrough has the potential to redefine the paradigm of cyber defense. Let's delve into the dynamics of Generative AI and its transformative role in cyber defense.

1. The Genesis of Generative AI

Generative AI, an offshoot of machine learning, holds the promise of creating content from scratch. Unlike traditional systems that respond based on a predefined set of rules, these advanced models learn from data, often vast amounts of it. Their capability to generate text, images, and even videos has garnered significant attention across various industries.

The introduction of models such as GPT-4 has unlocked unprecedented possibilities. One might ponder, "How is it relevant to cyber defense?" The answer lies in the adaptability and predictive prowess of these models. By simulating complex cyber-attack scenarios, Generative AI is not merely a passive player but a proactive strategist in the world of cyber defense.

2. Virtual Warriors: Generative AI's Role in Automated Red Teaming

Red Teaming, a concept borrowed from military war games, entails simulating cyberattacks on one's infrastructure to test its vulnerabilities. With the incorporation of Generative AI, the complexity and unpredictability of these simulated attacks have skyrocketed.

Imagine having an AI system that plays the devil's advocate—a 'virtual hacker' if you will. This AI doesn't sleep, doesn't rest, and evolves with every attempt, ensuring that cyber defenses are always a step ahead. With generative models at the helm, the depth and breadth of penetration testing have witnessed an astronomical rise, offering a more holistic view of potential vulnerabilities.

3. Navigating the Storm: Mitigating AI-Driven Phishing Attempts

Generative AI's proficiency isn't limited to defense. There are concerns about its potential misuse, particularly in phishing attacks. Crafting bespoke emails that appear strikingly genuine is now within the realm of possibility, thanks to these advanced models.

However, every challenge presents an opportunity. As Generative AI evolves, so do defense mechanisms against AI-generated threats. The utilization of AI-driven algorithms to discern subtle nuances that differentiate a genuine email from an AI-crafted one is proving invaluable. This constant game of cat and mouse between attackers and defenders is fostering rapid innovation in defense strategies.

4. GANs: A Double-Edged Sword in Cybersecurity

Generative Adversarial Networks (GANs), a subset of generative AI, has garnered significant buzz in recent years. Comprising two neural networks - the generator and the discriminator - GANs can replicate data with astounding precision. In the context of cybersecurity, this ability can be a boon or a bane.

While GANs can simulate cyber threats with increased sophistication, there's a silver lining. Their presence has birthed novel intrusion detection mechanisms that leverage the very principles of GANs for data integrity checks. This duality, where the same technology can be the threat and the savior, underscores the importance of understanding and adapting to new advancements.

5. Forecasting the Unknown: Predictive Threat Intelligence

Generative AI transcends reactive strategies, marking its territory in the predictive realm. By analyzing past cyber incidents, these models can craft potential future threat scenarios. This forward-looking approach empowers organizations to preemptively identify vulnerabilities and fortify their defenses.

Additionally, by referencing AI prompts, organizations can customize and fine-tune their threat intelligence, ensuring a more tailored defense strategy. For instance, platforms like PromptPal offer insights into leveraging AI prompts for diverse applications, adding another layer of precision to AI-driven threat forecasting.

6. The Ethical Implications: Treading with Caution

As Generative AI's capabilities continue to expand, so too do the ethical dilemmas surrounding its use. The power to simulate nearly indistinguishable cyber-attacks or create convincing phishing emails is not without its perils. There's a palpable fear that these tools, in the wrong hands, could inflict substantial damage.

Yet, like any tool, the distinction between beneficial and malevolent usage lies in the intent of the wielder. The broader tech community must engage in continuous dialogue about setting clear ethical boundaries. Regulatory frameworks, combined with best practice sharing among professionals, can ensure the responsible evolution and application of Generative AI.

7. A Glimpse into Training: The Backbone of Potent AI

At the heart of every proficient Generative AI system lies rigorous training on vast datasets. These datasets, often comprising details of countless cyber incidents, attacks, and tactics, fine-tune AI models to the zenith of their capabilities.

Yet, there's an inherent challenge: the sensitive nature of the data. As these AI models imbibe information from real-world cyber incidents, ensuring the confidentiality and integrity of such data becomes paramount. Ensuring data anonymization and adopting stringent data handling protocols are critical to both the success and ethical deployment of these models.

8. The Interconnected Web: Linking AI Capabilities

The potency of Generative AI isn't just in its standalone capabilities. Its true power lies in its amalgamation with other AI-driven tools. For instance, integrating AI-generated threat predictions with real-time intrusion detection systems can exponentially enhance threat detection capabilities.

Relevant platforms, like NIST's National Vulnerability Database, provide valuable insights into existing vulnerabilities and can be harmonized with Generative AI's predictions to form a comprehensive defense matrix.

9. A Quantum Leap: The Future Intersection of AI and Quantum Computing

The world stands at the cusp of a quantum revolution. Quantum computing, with its ability to process information at previously unthinkable speeds, might soon become a significant player in the cyber defense arena. The convergence of Generative AI and quantum capabilities could revolutionize cyber defense strategies, offering unparalleled speed and prediction accuracy.

However, it's a double-edged sword. Quantum computing also holds the potential to break several existing encryption methods. Striking a balance and staying ahead in this game will be the next challenge for technology professionals.

10. Best Practices: Staying Ahead of the Curve

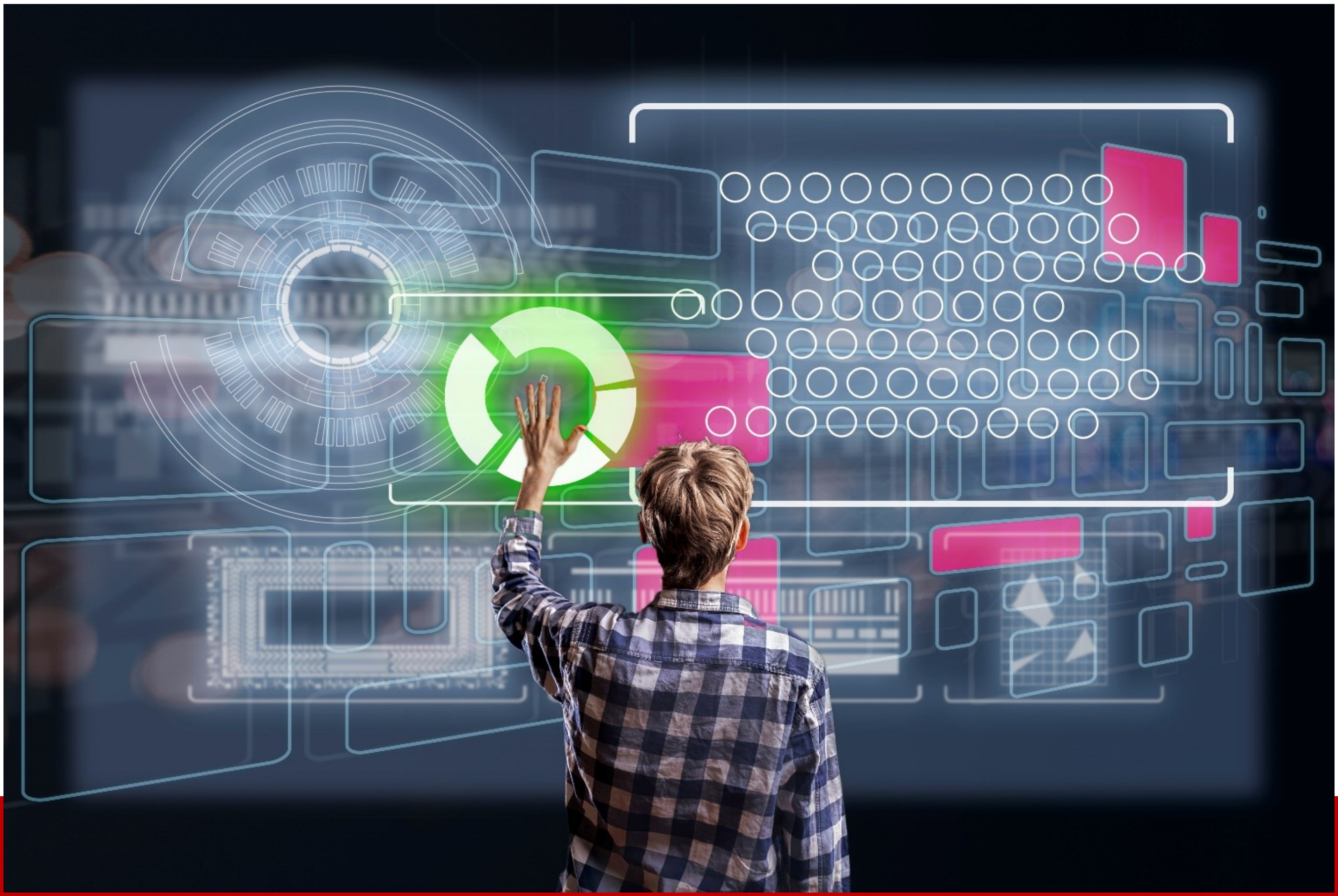
For technology professionals, staying updated with the rapid advancements in Generative AI and cybersecurity is crucial. Participating in webinars, attending conferences like Black Hat, and engaging in forums can provide valuable insights. Additionally, continuous training and certification, like those offered by ISC2, ensure that professionals are equipped with the latest knowledge and skills.

In Conclusion

The dance between Generative AI and cyber defense is intricate, constantly evolving, and profoundly impactful. As technology continues to advance, the line between attacker and defender blurs, necessitating an ever-adaptable defense strategy. By understanding the potential of Generative AI, harnessing its capabilities judiciously, and remaining vigilant to its potential misuses, technology professionals can not only defend but also thrive in this digital era. The challenge is formidable, but with the right tools and mindset, it is one that can undoubtedly be met.

About the Author

Dean, the visionary CEO & Founder at PromptPal, has an impressive portfolio as the mastermind behind Blu.Ventures, a startup studio cultivating innovations in blue ocean industries. With notable ventures like Bitcompare, Movingto, and AITW under his belt. Dean can be reached online at our company website https://www.promptpal.net/



The Rising Role of Artificial Intelligence in The Cybersecurity Market

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

In an era of digital transformation, where organizations rely heavily on technology and data to drive their operations, the need for robust cybersecurity measures has become paramount. With cyber threats evolving in complexity and frequency, traditional security solutions are no longer sufficient to protect sensitive information and critical systems. The fusion of AI and cybersecurity is reshaping the way organizations defend against cyberattacks, detect vulnerabilities, and respond to breaches. This article explores the dynamic AI in cybersecurity market, highlighting its growth, benefits, challenges, and future prospects.

AI in Cybersecurity: A Transformative Partnership

The integration of AI into cybersecurity strategies has brought about a paradigm shift in how threats are identified and countered. Unlike conventional methods that rely on rule-based systems, AI-driven cybersecurity employs advanced algorithms, machine learning, and predictive analytics to detect patterns and anomalies within vast amounts of data. This ability to analyze and process data at unprecedented speeds provides security professionals with a competitive advantage in the cat-and-mouse game with cyber criminals.

Market Growth and Landscape

The AI in cybersecurity market has experienced exponential growth in recent years, reflecting its increasing importance and effectiveness. According to a report by Market Research Future, the global AI in cybersecurity market is projected to reach a value of USD 96.3 billion by 2032, growing at a Compound Annual Growth Rate (CAGR) of 22.50% during the forecast period 2023 to 2030. This growth is driven by several factors, including the rising frequency of cyberattacks, the proliferation of IoT devices, and the adoption of cloud computing.

Considering the said published report by market research future, the AI in cybersecurity market is said to have sheer dominance by the North American region followed by Asia-Pacific and Europe, where the North American region accounted for about USD 7.3 billion in the year 2022 and projecting to grow with a rapid pace.

Leading tech giants and cybersecurity firms are investing heavily in AI-powered solutions to fortify their defence mechanisms. Companies like IBM, Palo Alto Networks, and Cisco have integrated AI-driven capabilities into their security offerings, providing customers with enhanced threat detection, incident response, and real-time monitoring. Additionally, startups focused exclusively on AI in cybersecurity are emerging, bringing innovative solutions that cater to specific security challenges.

Benefits of AI in Cybersecurity

The combination of AI and cybersecurity offers a multitude of benefits that are reshaping the industry:

1. **Advanced Threat Detection**: AI algorithms can quickly identify and analyze patterns indicative of potential threats, enabling security teams to proactively address vulnerabilities before they are exploited.
2. **Real-time Monitoring:** AI-driven solutions offer continuous monitoring of network traffic, applications, and user behaviour, enabling swift detection of suspicious activities and rapid response.
3. **Automated Incident Response:** AI streamlines incident response processes by automating routine tasks, allowing security teams to focus on strategic decision-making and critical tasks during a breach.

4. **Behavioural Analysis:** AI can create baselines of normal user behaviour, detecting deviations that could indicate unauthorized access or insider threats.
5. **Reduced False Positives:** AI algorithms refine their detection capabilities over time, reducing false positive rates and minimizing the impact of alert fatigue on security teams.

Challenges and Considerations

While AI holds immense promise in bolstering cybersecurity defences, it is not without challenges:

1. **Adversarial Attacks:** Cybercriminals are also leveraging AI to create more sophisticated attacks that can evade traditional defences, thereby necessitating the development of AI-driven countermeasures.
2. **Data Privacy Concerns:** The use of AI requires substantial amounts of data, raising concerns about data privacy and compliance with regulations like GDPR.
3. **Skill Gap:** The rapid evolution of AI technology has created a shortage of skilled professionals capable of developing, implementing, and managing AI-powered security systems.
4. **Bias and Fairness:** AI algorithms can inherit biases present in training data, potentially leading to discriminatory or unfair decisions in threat detection.
5. **Complexity:** Integrating AI into existing cybersecurity infrastructures can be complex and require careful planning to ensure seamless operation and maximum efficacy.

Future Prospects

AI in the cybersecurity market is poised for continued growth and innovation. Several trends are likely to shape its trajectory in the coming years:

1. **AI-Powered Threat Hunting:** AI-driven threat hunting will become a fundamental component of cybersecurity strategies, allowing organizations to proactively seek out and neutralize potential threats.
2. **Zero Trust Architecture:** AI will play a pivotal role in enforcing the principles of Zero Trust, where continuous authentication and verification are essential components of cybersecurity.
3. **Human-Machine Collaboration:** AI will not replace human analysts but will work alongside them, offering insights, automating repetitive tasks, and enabling faster decision-making.
4. **Explainable AI:** As the importance of AI ethics and transparency grows, the development of explainable AI models will become crucial to understanding how AI-driven decisions are made.

The AI in cybersecurity market is witnessing unprecedented growth and transformation, redefining how organizations safeguard their digital assets. With its ability to detect threats, analyze data, and automate responses, AI is an indispensable ally in the ongoing battle against cybercrime. As the market continues to evolve, businesses must navigate the challenges and embrace the opportunities that AI presents to stay one step ahead of cyber adversaries. By harnessing the power of AI-driven cybersecurity solutions, organizations can build a resilient defence against the ever-evolving threat landscape.

According to Market Research Future's latest research report on AI in Cybersecurity Market, By Type (Network Security, Endpoint Security, Application Security, and Cloud Security), By Offering (Hardware, Software, and Services), By Technology (Machine Learning, Natural Language Processing (NLP), and Context-aware Computing)

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
Market Research Future (Part of Wantstats Research and Media Private Limited)
99 Hudson Street, 5Th Floor
New York, NY 10013
United States of America
+1 628 258 0071 (US)
Website: https://www.marketresearchfuture.com

A New Ai Arms Race

By Alex Fink, CEO of the Otherweb

The internet has seen its share of arms races in recent decades. The advent of viruses resulted in an ongoing battle between those who make viruses and those who make antiviruses. The increase in spam made our email accounts unusable without spam filters. The proliferation of annoying ads made ad blockers necessary to maintain any semblance of sanity while browsing the web.\

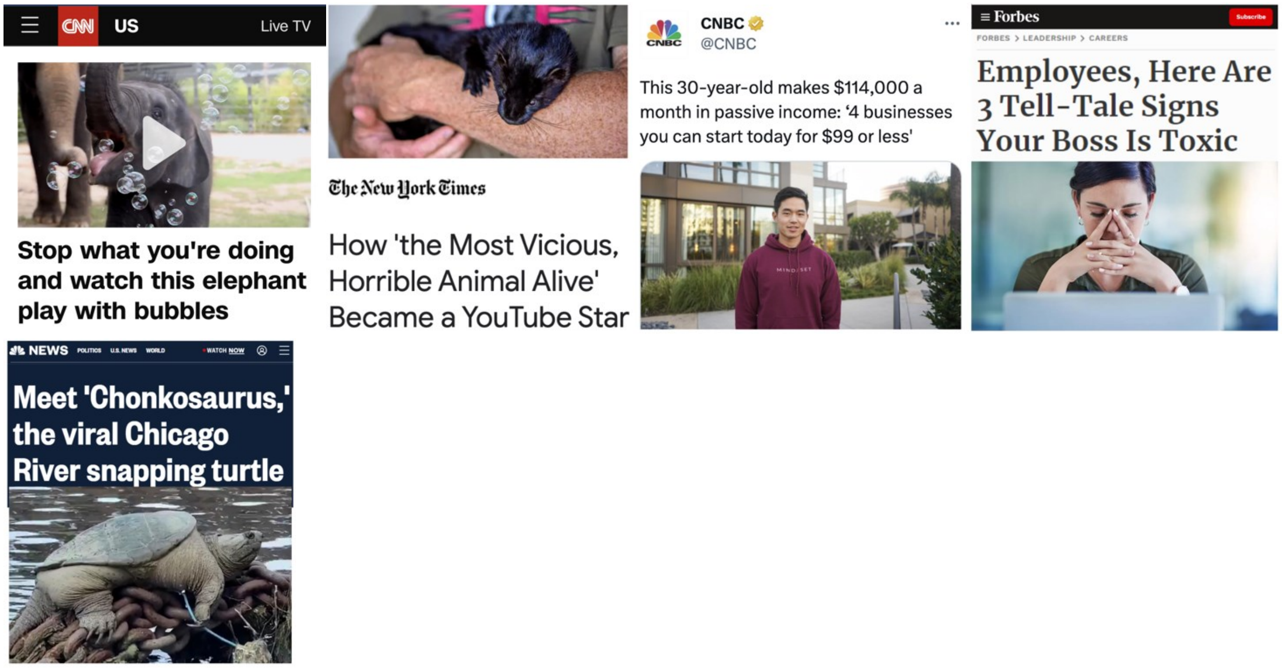
What is the most likely scenario, then, with regards to the recent breakthroughs in AI technology - namely the large language models (LLMs) that most people know as ChatGPT or Bard?

Predictions vary from the catastrophic to the utopian. And to be sure, both scenarios are possible. But I would suggest that the most predictable outcome is substantially more mundane than either of these options.

The inevitability of junk

The power of large language models lies in their ability to generate text that resembles what could only have been produced by humans before. For the time being, their output can rarely be classified as original or brilliant; more often than not, it is derivative and superficial. But therein lies the rub - most of the content that humans produce is derivative and superficial, too.

Here's an assortment of headlines from some of the best publishers of online content, to illustrate my point:



Stop what you're doing and watch this elephant play with bubbles

How 'the Most Vicious, Horrible Animal Alive' Became a YouTube Star

This 30-year-old makes $114,000 a month in passive income: '4 businesses you can start today for $99 or less'

Employees, Here Are 3 Tell-Tale Signs Your Boss Is Toxic

Meet 'Chonkosaurus,' the viral Chicago River snapping turtle

(screenshots taken by the author from cnn.com, nytimes.com, twitter.com, forbes.com and nbcnews.com)

We've already seen how, over the past 20 years, respectable outlets have gone from old-school journalism to elephants blowing bubbles. What do we expect to happen if the production of such bubbles takes 1/10th of the time it previously took? Or perhaps 1/100th?

As a general rule, lower cost results in higher quantity. And so, just as the increase in spam made our emails unusable without spam filters, the use of LLMs in online writing will make the entire internet unusable without junk filters.

AI vs AI

If we continue to follow the spam analogy, we might suspect that filtering junk is - in the general sense - an unsolvable problem. Every filter we create, no matter how perfect it is at a particular moment in time, will inevitably be circumvented by new tools and techniques.

Nevertheless, filtering will likely be necessary to discern any kind of signal in an ocean of noise. What tools might we use to try and compete with the various AI techniques that junk producers might employ?

This part of my prediction is less certain, but I still feel confident-enough to make it publicly: the only filtering technology that can adapt to AI-based content generation must itself be AI-based. Rule-based systems require humans to articulate the solution after the problem has already been articulated; but with generative AI, it's often impossible to articulate why things were done a certain way. The model learns, and the thing it has learned cannot be exported in legible form.

And thus, we have a problem that keeps morphing and cannot be legibly-defined. The only toolkit with any hope of solving it is machine learning.

Low-hanging fruit

As with other kinds of filters, we are likely to encounter a pareto distribution whereby a small number of filters results in a large fraction of the filtering. The vast majority of bad content - whether created by humans or by large language models - could likely be filtered by relatively-simple systems that focus on form, style, and other simple patterns. Each additional improvement in the filters will result in diminishing returns, i.e. more and more effort will be required to improve the filtering capacity by a few percentage points.

It might make sense, then, to focus our initial attention on the low-hanging fruit. Things that are obviously bad (like the examples I provided above) should obviously be filtered out. Complex disinformation campaigns orchestrated by content-creators with a large expenditure of resources might need to be handled later, when the bottom 90% are already taken care of.

Generalizing to other spheres

In all likelihood, writers are not unique in their capacity for derivative and superficial work. As generative AI models become better, their use could likely be generalized to audio, images, videos, and other forms of content that is created exclusively by humans today.

It's neither the end of the world nor utopia. Rather, we are entering an age of broken mirrors where most content will be fake, junk, or fake junk - and we must develop new tools to find needles in these haystacks of bad information.

There’s an obvious necessity, which typically means a market.

And the market for content filters will likely be proportional in size to the market for generated content.

About the Author

Alex Fink is the Founder and CEO of the Otherweb, a Public Benefit Corporation that helps people read news and commentary, listen to podcasts and search the web without paywalls, clickbait, ads, autoplaying videos, affiliate links, or any other junk. The Otherweb is available as an app (ios and android), a website, a newsletter, or a standalone browser extension.

FOR MORE INFORMATION VISIT: www.otherweb.com

Border Crossing: A New Battle Over Governments Extending Information Mandates Beyond National Security to National Interest

By George T. Tziahanas, AGC and VP of Compliance, Archive360

It might seem counterintuitive that in a distributed digital world, the location of data is increasingly important. However, based on current trends, national borders are indeed establishing a presence in cyberspace.

Governments have long sought to control national security-related information (such as classified data), but since the dawn of the Internet Age, they didn't concern themselves too much with non-classified data sharing—or if they did, the targets were typically quite narrow. The adoption of cloud solutions, initially deployed and used without much concern over boarders, just drove the point home.

But all that is changing: Over the last few years, countries have reconsidered their hands-off approach, and now are extending their reach into areas more aligned with their national interest. These include concerns around citizens' privacy, critical transportation or energy infrastructure, financial markets, and non-classified government information. They clearly want to mitigate cyber and other risks, and guard against a broader impact to their economies and population.

This type of data sovereignty laws has either been adopted or proposed in many regions. China, Germany, France (proposed), the Kingdom of Saudi Arabia and Dubai are good examples—they share characteristics such as categorization schemes to define the types of information subject to sovereignty, access controls, and conditions under which cloud offerings are used.

The United States has not adopted a specific data sovereignty statute (apart from export restrictions already in place), but the government has introduced a regulation for Confidential Unclassified Information (CUI). The purpose is to "standardize the way the executive branch handles information that requires protection under laws, regulations, or government-wide policies, but that does not qualify as classified.''

As the purpose noted, the intent was to standardize how federal agencies handle CUI, but it also encompasses those contracting or working with the government. CUI obligations for third parties are enforced based on contractual provisions, now required for anybody handling or managing CUI (or associated systems). This may also include state or local agencies doing business with the federal government or involved in data sharing relationships.

The CUI regulation, like the data sovereignty statutes described above, is based on a broad set of categorized information. It defines areas such as critical infrastructure, financial, immigration, intelligence, export control and transportation. Each of these broader categories is further divided into sub-categories that further defines the types of information subject to controls.

All CUI is subject to a marking requirement, which outlines whether the information is subject to "basic" or "specified" restrictions/controls. All CUI (including "basic") must be protected consistent with standards and policies such as FIPS 199, FIPS 200, and NIST SP-800-53. These are quite familiar within both government agencies and many private sector entities. Additional control requirements may be specified ("specified CUI"), along with other restrictions such as prohibition of sharing with non-citizens, contractors, or outside specific controlled environments. The objective behind all these standards is ultimately to protect this information from unauthorized access, or disclosure.

While some federal agencies and contractors are already negotiating CUI, many entities will likely learn about it only when an update to a contract is requested, or flow-downs from a prime contractor pushes this to smaller organizations. Meanwhile, global corporations will soon have to deal with international digital borders.

But just as these are digital problems, there are digital solutions. There are technologies already available to help manage the data categorization, along with requisite access control and security requirements. It might help to consider government-controlled cloud environments, since much of this information will outlast many technology contracts.

In sum, CUI is coming, and it will be important. Staying ahead of it—rather than trying to catch up—with technologies now on the market will offer a major advantage.

Full a complete list, See https://www.archives.gov/cui/registry/category-list

About the Author

George T. Tziahanas, Vice President of Compliance, Archive360

George has extensive experience in complex compliance and information risk challenges. He has worked with numerous financial services corporations to design and deploy petabyte-scale compliant books and records systems, supervision and surveillance, and eDiscovery solutions. George also has deep expertise in developing strategies and roadmaps addressing compliance and data governance requirements. He has specialized in working with emerging and advancing technologies to address real-world problems. He's conducted AI/ML-driven analytics across legal and regulatory use cases, and helped companies adopt new solutions.

George can be reached online at (George.Tziahanas@archive360.com, Twitter @Georgetz2) and at company website www.archive360.com

Quantum Security is National Security

By Andy Manoske, Principal Product Manager of Cryptography and Security Products at HashiCorp

Quantum computers will be one of the defining frontiers in computing over the next century. Utilizing the power of quantum mechanics to provide near-infinite parallelism to “divide and conquer” certain types of problems better than any traditional computer before them, quantum computers will likely herald many breakthroughs in areas such as AI, high finance, medical innovation, and pharmaceutical research due to their unique capabilities.

But they also pose potential threats to national security. The mathematical capabilities that allow quantum computers to search for novel chemical combinations for future cancer drugs and train AI large language models (LLMs) faster than conceivably possible with digital computers, similarly will enable unique types of codebreaking attacks against traditional encryption. Such attacks pose grave threats to the cryptography we use to identify parties on the internet and protect national secrets.

In response, the White House's Office of Science and Technology Policy (OSTP) has worked to support a new version of the National Quantum Initiative Act: H.R.6227. This act, first introduced in 2018, defines the creation of an office to advise lawmakers on critical congressional committees on the impact that quantum computing will have on the United States' economic, political, and military interests.

In the five years since H.R.6227 was introduced, shifts in computing such as the rise of AI in LLMs such as OpenAI's GPT-4 have already heralded economic innovation and disruption. The arrival of stable, powerful quantum computing will be *orders of magnitude more disruptive*. And it is vital that lawmakers understand the risks, and benefits, that this landmark technology will bring.

What is Quantum Computing?

Quantum Computing (or QC) is a technology that leverages properties of quantum mechanics to dramatically improve a computer's ability to solve specific types of problems. Like their traditional digital computing counterpart, QC allows for the creation of machines that can investigate and solve problems through logic. But in certain circumstances, QCs can solve problems that would be impossibly difficult for digital computers to solve — so much so that the universe would likely end before a result was found.

In digital computers, electrons move through circuits of gates that instrument logic and programming to compute a result known as a *bit*. Bits hold two states — either "on" or "off" — that reflect the result of computation. In QC, quantum mechanical processes are used to create quantum logic gates that operate on subatomic particles. The output of these quantum logic gates are qubits — the quantum version of a bit.

Unlike bits, qubits can hold multiple states at once thanks to superposition. Superposition is a principle of quantum mechanics that allows for some interactions to hold multiple states at once. Much like pressing some piano keys results in a sound that is a composition of multiple simultaneous notes, qubits can utilize superposition to hold more fundamental states than their digital counterparts.

If computation is modifying a deck of playing cards and drawing a result, digital computers return a single card. Quantum computers instead return a distribution of the probabilities of drawing every possible card in that deck. Programmers can then use statistics to compute some results infinitely faster than they could with a digital computer. Rather than drawing cards from a deck until you hit the Ace of Spades, a programmer can instantly compute when you would be most likely to draw that ace without touching the deck.

But there are drawbacks to quantum computing. The properties that make quantum computers so good at solving some problems also make them extremely difficult to develop and reliably use. While quantum computers already exist and are providing real value (for example: serving as infinite random number generators) they are comparatively slower than digital computers for most interactions and not powerful enough today to compute some of the novel solutions that enable world-changing disruption.

Major advances in physics and materials science are necessary to build stable quantum computers powerful enough to herald breakthroughs in computing. But given the rapid advance of both fields, computer scientists as a whole believe that the next generation of the field will be dominated by quantum computing.

Quantum codebreaking: a major risk to privacy and national security

Promoting the safe research and development of QC in the United States is vital for the country to remain macroeconomically competitive in the next generation of computing. But there are also major risks that this disruption brings, most notably within national security.

Cryptography is the area most imminently impacted by quantum computing. Nearly half of the encryption powering modern identity verification and the protection of secrets online is vulnerable to attacks that leverage quantum computers' parallelization capabilities.

With a modern computer, a codebreaking attack to search for a 2048-bit RSA private key (such as those used to protect cryptocurrency wallets and encrypt private communication between users and websites) would take longer than the lifetime of our universe. But using a quantum computer and a technique known as Shor's Algorithm, this attack could take minutes.

Shor's Algorithm and other QC codebreaking methods are well known in intelligence and national security circles. They were researched decades ago and are still researched intently by government groups and defense contractors. US federal programs such as NIST's Post Quantum Cryptography (NIST PQC) program have spent the last decade developing new cryptography resistant to known quantum code breaking techniques.

While drafts of this new post-quantum cryptography exist and are undergoing review and implementation in code across the public and private sector, there are no laws or regulations that exist to guide when and how they should be broadly deployed.

It is likely that NIST's FIPS 140, a certification program to verify cryptographic security for military use cases across the US and many NATO countries, will eventually address QC defense. But for the private sector and many non-military government use cases, no such programs or initiatives to migrate to post-quantum cryptography exist.

Lawmakers in the US will likely have to create new rules and regulations to push tech companies (and the internet at large) to migrate quantum-vulnerable cryptography to new post-quantum counterparts.

Failure to do so means that the cryptography used to identify users and protect privacy online is rendered vulnerable to adversaries such as governments and major non-state cybercrime actors.

About the Author

Andrew “Andy” Manoske is the Principal Product Manager of Cryptography and Security Products at HashiCorp. Prior to HashiCorp, he led product management for security and defense technology such as AT&T Cybersecurity Open Threat Exchange (OTX), NetApp Storage Encryption, and Lockheed Martin BlackCloud.

Building A Secure Integrated Collaboration Platform

By Allen Drennan, Principal & Co-Founder, Cordoniq

Integrated collaboration platforms improve and enhance the experiences of hybrid and remote employees. Robust and comprehensive platforms are crucial to remote work environment success.

When collaboration tools can be accessed through a flexible platform, organizations achieve more well-being for their employees while productivity increases. With a well-integrated collaboration platform, teams can access the tools they need without having to toggle between multiple screens or applications.

But there are greater risks and vulnerabilities with the use of multiple communication and collaboration tools and apps. Remote work creates its own security challenges because of expanded attack surfaces and endpoints. Meanwhile, cyber threats are escalating continually, affecting businesses of all sizes. Secure collaboration tools are a must as threats grow. Industries that are being specifically targeted by malicious actors, such as banking, finance and healthcare, require even more secure collaboration tools and platforms.

Increased risks with collaboration tools

Collaboration and communication tools increase the risk of cyber threats from multichannel social engineering and phishing scams. Phishing attacks are escalating and growing more sophisticated. One study shows that in 2022, phishing scams increased by 61% from the previous year. https://www.cnbc.com/2023/01/07/phishing-attacks-are-increasing-and-getting-more-sophisticated.html

Other attacks commonly affect API-based platforms. APIs are a frequent target of hackers and malicious actors due to the data that can be accessed, such as personally identifiable information (PII) or financial details. Some frequent and common API attacks include Distributed Denial of Service (DDoS) attacks, authorization hijacking and man-in-the-middle attacks. Sources of vulnerability include broken or “zombie APIs” that no longer function properly or have flaws.

In addition, when multiple communications tools and channels are enabled, it is easier for hackers to infiltrate systems and data. Some communications tools carry multiple vulnerabilities and threat actors can gain access to confidential data or information.

Security flaws in popular video conferencing tools recently left users and client systems susceptible to threats including malware and malicious code. Because of software flaws or inadequate cybersecurity, video conferencing tools carry risks such as meeting infiltration by unauthorized parties, as well as unauthorized access to data, confidential conversations, or information.

Other risks with video communications tools include advancement of Deepfake technology. The US Department of Homeland Security defines deepfakes as, “an emergent type of threat falling under the greater and more pervasive umbrella of synthetic media, utilize a form of artificial intelligence/machine learning (AI/ML) to create believable, realistic videos, pictures, audio, and text of events which never happened.”

Deepfakes can produce significant threats to business organizations such as false representation of corporate or leadership figures, fraudulent transactions, or extortion.

Furthermore, the use of “shadow apps,” which include unauthorized applications downloaded by employees, increases vulnerabilities throughout the organization and leads to a loss in visibility and control. Risks with shadow IT or apps unauthorized include cybersecurity risks, unauthorized access to data, and compliance risks.

The vulnerabilities in collaboration platforms are a significant issue for companies in sectors that handle sensitive information and data. Cybercriminals continue to target firms in sectors including financial services, higher education, healthcare, manufacturing, governments and state agencies. Malicious actors continue to find selling data on the dark web to be lucrative and will change tactics continuously to stay in business.

Multi-faceted strategy needed to secure integrated platforms.

Securing an integrated collaboration platform requires a robust and collaborative strategy. Several different methodologies must be enabled to effectively mitigate risks and vulnerabilities that involve platforms or other communications or business tools.

To be most effective, this strategy needs buy-in throughout the organization. Security is not only the concern of the CISO and other IT security teams.

Here are several ways to create a secure collaboration platform that can function optimally for your organization:

1. Start with software applications that are secure by design. As per recent CISA guidance, "secure by design, secure by default" refers to software that has security built in from the ground up. Secure by design means that security is an integral part in and throughout all stages of design and software engineering. Security isn't bolted onto the software as an afterthought.
2. Adopt a culture of security in the organization. When an organization adopts a culture of security, it needs to start with leadership. With cybersecurity infrastructure on its way, teams, executives and systems all need to be prepared. All stakeholders from the C-suite to all employees and end users must be involved in the cybersecurity process. The organization must also ensure that employees are educated in practices for cyber hygiene, including Zero Trust, password rules, and accessing only secure networks, endpoints and devices.
3. Ensure that teams have the tools they need. The organization is responsible for making sure employees have the advanced tools, apps, and platforms required to do their jobs effectively. Tools need to be convenient, effective and easy to use. When employees become frustrated because they don't have access to business and collaboration tools, they resort to downloading and using shadow apps that can introduce vulnerabilities and risks. It's critical for organizations to make sure business tools – including AI tools – are verified and secured at all times to protect data, privacy.
4. Enable all software security tools. It's critical to verify that all collaboration software tools have every advanced security and authorization tool enabled. This includes requiring multi-factor authentication, monitoring and limiting access, and using the most advanced encryption protocols available.
5. Establish API security practices. Some primary API security practices include defining API protocols and maintaining a current API inventory with comprehensive documentation. Other secure API practices include requiring multi-factor authentication, using security keys and certificates, and applying Zero Trust methodology. Partnering with API security software is another effective strategy.
6. Look for collaboration solutions that give you control over the privacy and security aspects of your data and how it is retained. Implementations that allow you to control where modules are deployed (private cloud/hybrid) and how and where those solutions store your data, shared content and collaboration recordings is critical.

Establishing and implementing a comprehensive platform security strategy also requires collaboration and cooperation among business units, IT teams and security teams. Platform, application and API security is an essential part of ensuring an organization's entire tech stack is secure and optima

About the Author

Allen Drennan is Principal & Co-Founder of Cordoniq. When he founded Nefsis Corp. in 2005, Allen Drennan introduced a cloud-based, video conferencing online service, cited by Frost and Sullivan as the first of its kind. He achieved this by building engineering teams to create a mobile and desktop solution that successfully blended web and native code into a seamless online service.

Over his career Allen has designed, built and deployed large-scale SaaS solutions for real-time video and collaboration, and created new technology for mobile video user interfaces, messaging, text, voice and video communications. Some of these solutions have been recognized in Gartner's Magic Quadrant and featured in major industry publications over the years, such as eWeek, PC Magazine, USA Today, New York Times, The Wall Street Journal, CyberDefense Magazine and more.

A frequent contributor to open-source projects, Allen also writes about highly technical software engineering topics for iOS, Android, Linux, MacOS and Windows.

Allen went on to found Cordoniq, Inc., bringing together many of the team of senior engineers who created Nefsis and OmniJoin, as well as new talented team members, to create the next generation of truly secure, state-of-the-art video conferencing and collaboration.

Allen can be reached online at https://www.linkedin.com/in/allen-drennan-0359a822/ and at our company website http://www.cordoniq.com/

Delivering Safe Browsing Experiences in A Rising Tide of Web-Based Threats

By Brett Raybould, EMEA Solutions Architect, Menlo Security

According to Google, the average worker now spends three-quarters of their working day using a web browser. This has provided many productivity benefits. Not least, it is enabling employees to work flexibly as per their individual needs – from the office, from home, on the go, or outside of traditional working hours. However, in a cyber sense, it has created concerns.

Within this new working dynamic, adversaries have placed a massive bullseye on the web browser. It has become the new desktop, where many of us spend the bulk of our working day.

We are witnessing a massive shift in the attentions of attackers as they continually refine their techniques, developing novel and innovative ways to target their victims via this new focal channel.

It's a problematic situation that is not being helped by the emergence of ever more powerful tools, including new generative AI platforms. Indeed, the ability of threat actors to find and develop ways to launch ever more sophisticated attacks is ramping up – something that security professionals fear.

In a recent survey of 1,500 IT specialists, Blackberry found that 71% believe that foreign states are likely to already be using ChatGPT for malicious purposes against other nations, for example.

How threat actors are rendering legacy solutions useless

With web browser threats growing in both frequency and sophistication, it is critical that companies embrace the technologies available to help them in the fight. However, this is where many are lacking right now.

Lagging security vendors are continuing to focus on fighting yesterday's war, attempting to shoehorn network security and endpoint tools to keep users safe – a tactic that simply is not working. By leveraging the web browser as the attack vector, threat actors are effectively rendering a decade or so of security technology investments redundant.

Secure web gateways, firewalls, endpoint security and EDR solutions are all unable to observe and therefore respond to actions occurring within the browser.

Take HTML smuggling for example – a commonly used evasive technique that sees a malicious file dynamically constructed within the browser. It's specifically designed to ensure that no resource requests for a remote file can be inspected, leaving content engines unable to identify any risk, and attackers able to bypass legacy network security perimeter controls.

Similar issues are also encountered with 'Good2Bad' websites, where hackers briefly hijack benign websites for malicious purposes before they are flagged as being 'bad' by web categorisation engines.

Legacy tools also have problems in responding to threat actors' use of browser exploits such as phishing kits, crypto-mining code, and JavaScript to impersonate known brand logos as a means of evading detection from static signatures that examine web page source code and HTTP traffic.

Bucking the trend with innovative technologies

Those traditional tools that many firms continue to rely upon simply are not equipped to combat the new cohort of advanced browser-based threats – and threat actors know this, increasing their attack efforts by the day.

It's a trend we've seen consistently evolving over time. Between 2019 and 2021, Menlo Labs tracked a 958% increase in the use of Good2Bad sites. More recently, a 2022 survey of 505 IT decision makers across the US and UK revealed that more than half (55%) of enterprises encounter advanced web threats at least once a month, with almost two-thirds (62%) having had a device compromised by a browser-based attack in the previous 12 months alone.

To be frank, this is somewhat unsurprising given that the very same survey highlighted that 45% of organisations also hadn't added any capabilities to their security stacks over the same period.

Moving forward through 2023 and beyond, this needs to change. Organisations cannot afford to stand still. Just as threat techniques have evolved, so too have the technologies and tools available to combat them – and they must be embraced.

Enter HEAT Shield – a new technology capable of detecting and blocking phishing attacks before they can infiltrate the enterprise network. It uses novel, AI-based techniques – including computer vision combined with URL risk scoring and analysis of the web page elements – to accurately determine in real time if a link being accessed is a phishing site designed to steal the user's credentials.

Elsewhere, HEAT Visibility can be used to perform continual analysis of web traffic, applying AI/ML-powered classifiers that identify the presence of highly evasive attacks. This delivers timely, actionable alerts that enable security teams to significantly reduce mean time to detect (MTTD) and mean time to respond (MTTR) to any highly evasive threats that could be targeting enterprise users.

The availability of such solutions is a positive, and there are other reasons for optimism too. Indeed, Verizon's 2022 Data Breach Investigations Report revealed that 82% of firms are at least considering adopting a zero trust approach to security, with genuine adoption expected to ramp up throughout this year. However, given the growing threat of browser-based attacks, organisations must address the associated vulnerabilities as a priority.

The technologies are there. Now is the time to embrace them – to turn the tide, and deliver a secure, seamless browsing experience for all.

About the Author

Brett Raybould - EMEA Solutions Architect, Menlo Security. Brett is passionate about security and providing solutions to organisations looking to protect their most critical assets. Having worked for over 15 years for various tier 1 vendors who specialise in detection of inbound threats across web and email as well as data loss prevention, Brett joined Menlo Security in 2016 and discovered how isolation provides a new approach to solving the problems that detection-based systems continue to struggle with.

Securing the Future of Data Security Through Transparency: A Glimpse into Quantum Random Number Generators Research & Development

By Denis Mandich, Co-Founder and Chief Technology Officer of Qrypt

Software supply chain security is a major concern in today's digital world. In 2019, bad actors hacked the software compilation process for SolarWinds Orion platform and placed a backdoor inside legitimate Orion software updates. It had a domino effect impacting 18,000 customers and thirty-seven defense companies. SolarWinds was a major lesson learned for all organizations to scrutinize their supply chain and what is inside the hardware and software they purchase. This is especially important when it comes to future technology like artificial intelligence (AI) or quantum, as many organizations will use the buzzword label for marketing and sales without backing up the claims.

For example, in the field of quantum-secure encryption, an attack on the random numbers used to generate secure encryption keys can fundamentally compromise the security of sensitive data and digital identities. It is therefore critical that organizations confirm the security of the quantum random number generator (QRNG) technology coming to market.

The Importance of Random Number Generators

There is an unfortunate and surprising problem regarding quantum random number generators (QRNG) – our entire universe is quantum, and there is some quantum effect in everything, including coin-flipping (which incidentally is not random at all).

Random numbers are fundamental to all digital security and identity and indeed the entire internet. If encryption software requires keys 256-bits long, but the randomness generator we are using is based on classical algorithms, then predictability becomes an issue. Although seemingly producing random numbers, these generators can be reverse-engineered and their output calculated, especially with the increasing sophistication of machine learning and AI. This can compromise our security.

In science, randomness indicates an event that cannot be predicted or known in advance, even with perfect knowledge of the physical system. The outcome is fundamentally unknowable; not simply difficult to guess. Many methods exist for generating random numbers, such as tossing dice or the motion in a lava lamp. However, these seemingly unpredictable methods are not as unbiased as we might think. Modern computers, adept at finding patterns within a sequence to predict outcomes, can compromise these classical and traditional sources of apparent randomness. This is where the power of quantum physics shines – it offers truly random phenomena unlike anything in classical physics. In the quantum world, certain events, like the decay of a radioactive atom, are fundamentally unpredictable. This unpredictability is not due to a lack of knowledge or measurement precision but a unique feature of the quantum realm itself. Scientists can tap into this unpredictability by performing experiments to measure quantum phenomena. These experiments produce a fundamentally unpredictable and truly random result. This inherent quantum randomness is crucial for QRNGs, powerful tools for digital security. As more QRNGs come to market, they promise to offer the only provably unpredictable events known to science, which are essential to fortifying cybersecurity.

Quantum Randomness and its Role in Security

Why are random numbers essential to cybersecurity? They are used to generate encryption keys, secure passwords, and enable secure communications and data privacy. The foundation of all secure technology, invisible as it might be to many users, assumes secure cryptography, and that, in turn, relies on random numbers. Quantum random numbers, due to their inherent unpredictability, play a crucial role in mitigating the risk of attacks that could compromise our digital security infrastructure.

Unfortunately, many products today labeled “quantum” may often be more marketing gimmicks than scientific facts. Caveat emptor—buyers must demand to know what’s inside their hardware and software purchases. Much like the software bill of materials (SBOM), which provides a detailed inventory of software components to promote transparency and security, the industry is correctly trending towards greater visibility in hardware. With QRNGs, you might hear that it is impossible to “prove” randomness. However, here are a few considerations to help navigate this evolving landscape:

1. **Vendor Transparency:** Demand full disclosure about their technology, particularly about the quantum mechanisms they claim to use. Additionally, you should request min-entropy values to help in evaluating claims.

2. **Public Disclosure:** Verify if the vendor's underlying entropy methodology has been openly disclosed for peer review by engineering professionals.

3**. Independent Tests:** Ensure independent tests, like those from the National Institute of Standards and Technology (NIST), were conducted on the RNGs raw output to check for patterns implying the numbers were not randomly generated.

Remember, a collapse in fundamental cryptography via an attack on random numbers crumbles all the security infrastructure built on top of it. SolarWinds was a warning, perhaps even an omen of worse to come. Thus, it is crucial that vendors are held to high standards of transparency to prevent cascading effects.

New research from my team and I at Qrypt and teams at Advanced Quantum Architecture (AQUA) Laboratory, École Polytechnique Fédérale de Lausanne (EPFL), Ruder Boskovic, and Global Foundries discovered a single-photon avalanche diode (SPAD)-based QRNG design, which utilizes the quantum random flip-flop (QRFF) method. This type of integrated circuit on a SPAD array at the 55nm scale was science fiction a few years ago. The ability to detect a single particle of light, a photon, billions of times a second across thousands of pixels on a 2mm chip would have stunned most technologists of the previous generation. Leveraging quantum events like this at these speeds is essential to making security guarantees further up the encryption stack in any network.

Research like this contributes to our understanding of quantum randomness and its applications in digital security. As more QRNGs come to market, it is crucial that we, as consumers and stakeholders in digital security, demand transparency from vendors and stay informed about the latest developments in the rapidly evolving field of quantum.

About the Author

Denis Mandich, Co-Founder and Chief Technology Officer of Qrypt.

As Co-Founder & CTO of Qrypt, Denis drives the technology roadmap and secures the global expertise to achieve the company vision to protect against quantum computing threats. Previously, he served 20 years in the US Intelligence Community, working on singular, innovative technology essential to National Security. Denis is a board member of Quside, advisor to the Quantum Startup Foundry, and NSF-funded Mid-Atlantic Region Quantum Internet. He speaks native-level Croatian and Russian.

Qrypt can be reached online at our company website https://www.qrypt.com/

Anything Is Hackable: Consumers Must Not Be Caught Out

In an age driven by data, cyber-related crimes are on the rise. Business leaders must invest in new strategies designed to keep their customers and their personal data safe from illicit actors.

By Bryan Seely, Keynote Speaker and Cybersecurity Expert

Our world is driven by data. Vulnerabilities are ready to be exploited by bad actors everywhere we look. Hacks targeting world governments are frequently reported and subsequently covered in global media, but what worries me is the growing amount of innocent consumers being affected by data breaches every day. Massive corporations are failing to adapt quickly enough to the changing landscape.

The global big data analytics market was valued at $272bn in 2022 and is expected to reach close to $750bn by the end of the decade. A growing industry will always be met with an increase in rogue actors looking to profit from it illegally, and consumers must be vigilant.

We submit or create personal data sometimes without even knowing it. Storing passwords online and enabling website cookies are just two examples of things we do every day to make our lives easier. Increasing efficiency is often our primary concern without contemplating the security implications of such actions.

There has been a clear up-tick in cybercrime around the world since the turn of the century as more and more devices are connected to the internet. In the US alone, an estimated 53.35 million citizens were in some way impacted by cybercrime in the first half of 2022. In 2021, US nationals lost $6.9bn to cyber-related crimes.

As we saw during the pandemic, many flocked to the world of decentralized finance (DeFi), seeking opportunity as cryptocurrencies took off in value, but also for security.

Blockchain technology promises enhanced levels of security and personal data protection and while in many cases this remains true, clear risks still remain especially as the tech becomes more mainstream.

It does not take much research to understand the growing magnitude of crypto-related cybercrime. Last year, cybercriminals stole over $2.8bn from innocent crypto holders through various hacks and exploits.

During such exploits, user funds are usually compromised but, due to the ways in which online crypto wallets and accounts are usually set up, consumers may not realize that their personal data is also being stolen via sophisticated phishing attacks.

Major governments continue to be incredibly concerned by the uptick in such criminal behavior. Earlier this year, the Biden Administration published a new National Cybersecurity Strategy promising, amongst other things, significant new long-term investment into cybersecurity capabilities.

While measures like this will undoubtedly help consumers, the reality is that criminals will always find novel ways around defense measures.

We know that nothing is ever truly unhackable. Fortunately, technology enables us to design products that prioritize users' personal data. Crucially, the tech should cover both traditional and decentralized finance.

The world's largest and most successful company of all time, Apple, issued a public statement late last year acknowledging 'increasingly sophisticated and complex' threats to user data and personal security. Following this, they announced numerous security updates to products used by hundreds of millions every day.

In the DeFi sphere, popular Web3 company SafeMoon released a new product called Orbital Shield at the beginning of 2023 which utilizes advanced 256-bit encryption to anonymize user data. This software is actively being rolled out throughout the company's product ecosystem meaning that their one million plus wallet users are safe in the knowledge that even in the event of a hack, their data remains secure.

In March, when discussing the need to protect user data, SafeMoon's CEO, John Karony explained how companies are incentivized to collect and store user data. He went on to say that 'securing user data should keep developers up at night' and that 'the very concept of data storage needs to be reimagined altogether'.

As the cyber threat continues to evolve, new products designed to cope with this are needed across industries. Data which includes one's most personal information including date of birth, address, bank account information, relatives and more continues to be at risk from exploitation.

We know that there is no such thing as perfect security, but like locking your car or setting the alarm in your home, there are measures that businesses can take to help secure their users' personal security.

As stated by President Biden in March, cybersecurity 'is essential to the basic functioning of our economy'. Digital connectivity should always be a tool that uplifts and empowers people everywhere, not one used for repression and coercion.

About the Author

Bryan Seely is a world-renowned ethical hacker, cyber security keynote speaker and thought leader who frequently speaks at major global cybersecurity conferences. He is a former US Marine and host of Black Hat MEA podcast who famously became the only person in history to successfully wiretap the US Secret Service and FBI, informing both agencies of his work.

Bryan can be reached online at https://www.bryanseely.com/ and @bryanthemapsguy

How Can We Turn a Hacker’s Toolkit Against Them? The Evolution of a Phishing Email

By Jack Chapman, VP of Threat Intelligence, Egress

Hackers use many tools at each stage of an attack and with the sophistication of attacks escalating rapidly, it’s vital we understand what they have in their arsenal. These tools are often readily available online, both free of charge and to buy, and are easy to use for even non-technical cybercriminals.

Understanding a hacker’s tools and tactics is essential for cyber security practitioners and vendors aiming to build effective defenses and stay one step ahead of a quickly evolving host of cyber threats. For example, while attackers can change the content, graphics, and payloads of a phishing email, the right technology can detect the tell-tale signs in its underlying structure, its context, and delivery mechanism. Email is a high risk threat vector and with 91% of organizations reporting they had security incidents from outbound email and 92% falling victim to phishing, according to the Egress Email Security Risk Report, care is required when using it. At Egress we analyze thousands of phishing emails and investigate ways to reverse engineer repeatable elements against hackers.

In this article, I walk through the various tools that support the first three stages of the cyber kill chain: reconnaissance, weaponization, and delivery. Most importantly, this article will cover ways to defend against these tactics, including best practices on security awareness training, impersonation protection policies, and keeping applications as secure as possible.

What’s in an attacker’s toolkit?

Different tools are used at each stage of the cyber kill chain. Ultimately, if an attack can be detected and prevented at delivery (a phishing email), it will be killed earlier within the kill chain to help keep employees safe.

And by understanding the intricacies of these stages, you too can start to think like a hacker, prepare for the tactics they use, and implement stronger defenses.

Reconnaissance: Locate the target

This is the first stage of the kill chain, where a bad actor sets out their objectives, finds a target and researches them. There are a variety of tools that make it easier for bad actors to search for targets within your organization and assess their likelihood of falling for an attack. These range from Google, marketing contact databases, and social media sites, to email trackers that can show whether a recipient has interacted with an email.

Our 2021 Insider Data Breach survey revealed that 94% of organizations experienced a data breach in the last 12 months. Furthermore, these breaches can leave a company’s data exposed, increasing the risk of phishing threats. In short, it’s time to batten down the hatches.

A bad actor can use a variety of free and paid-for tools to assess a company’s email security system and its defenses. This enables them to understand any existing vulnerabilities that can be exploited and try to craft their attacks to evade detection. This is aided by the phenomenon aptly titled phishing-as-a-service, a growing trend of cybercriminals diversifying and selling their software and/or expertise to lesser-skilled prospective hackers.

Weaponization: Crafting the phish

After reconnaissance, the next step is crafting the phishing email – which can contain a malicious payload, or it can rely on social engineering without any payload.

Phishing kits can be used to create spoofed websites to steal a target’s credentials, steal multi-factor authentication (MFA) tokens, and evade detection from security technology.

The more expensive kits will include tactics to evade detection by cybersecurity technologies, including:

- HTML obfuscation techniques using encryption, encoding, and whitespace
- IP address blocklists to identify and block connections from security vendors attempting to scan the webpage for signs of a threat

- User agent blocking (again to identify and block connections from known security crawlers)
- Use of compromised or legitimate sites for hosting

We often see these attacks spike around key dates, with attackers weaponizing the news cycle. For example, ahead of US Tax Day this year, our threat analysts saw a 164% increase in tax-related phishing emails since February 2023 and a 32% increase versus 2022 levels. Typically, in these attacks, cybercriminals attempt to convince victims that they have a tax refund available or have underpaid their taxes, when in reality, the email contains a malicious link or attachment.

Delivery: The trojan horse

Once a target has been found and an email has been weaponized, the next function of the toolkit is to help an attacker evade both email security and the scrutiny of the human recipient once it's delivered.

Using a compromised email account to send phishing emails makes it less likely they'll be detected by email security solutions. This is called business email compromise, or 'BEC' and it presents a growing problem for organizations of all sizes. BEC causes 37% of cybercrime losses that are reported to the FBI, and over $43bn has been lost due to BEC attacks. But, when a bad actor doesn't have access to a compromised account, they can rely on various tools to get their attack into the organization. These include legitimate email sending tools, such as those used for marketing and communication purposes, burner email addresses, and free webmail accounts. Additionally, impersonation attacks can leverage the organization's own tools (Microsoft Azure AD and Outlook) to add authenticity to an attack.

Preventing the preventable

With the inner workings of the hacker's toolkit exposed, the focus turns to cyber security best practice. By implementing regular security awareness and training (SA&T), organizations go some way to help empower their employees to identify and deal with phishing attempts before an attacker manages to steal valuable data. Additionally, organizations should augment their defenses with an integrated cloud email security solution (ICES). ICES solutions protect organizations from advanced email attacks by analyzing email content for signs of BEC.

With phishing attempts being a near-constant business threat, users engage at the point of risk, empowering them to not only understand why an email has been flagged as dangerous but also identify compromise from a trusted source.

About the Author

Jack is VP Threat Intelligence at Egress, with expertise on the cyber-threat landscape & trends, cyberattack psychology, and designing & developing intelligent cyber security solutions. He joined Egress in June 2021, having previously co-founded a phishing defense platform. He graduated from the University of York in 2015 with a bachelor's degree in computer science.

Jack can be reached online at Jack Chapman | LinkedIn and at our company website www.egress.com

Who are the Wagner PMCs of Russia

Is There a Risk of Cyber Fallout?

By Stan Vitek, Resident Geopolitical Analyst, Cyfirma

Executive Summary

At the end of June, a Russian mercenary organization known as 'Wagner' has mutinied against its state backers in a bid to keep its independence. The rebellion seriously shook the political system in Russia and weakened the position of President Putin, even though the mercenaries ultimately capitulated and accepted a Kremlin offer. The Russian government has outsourced its information operations through a complex web of companies, run by the head of the mutiny; businessman Yevgeny Prigozhin, who has also been responsible for coordinating secret elements of Russian foreign policy in the Middle East or Africa. In the wake of the rebellion, the Russian government is now looking to restructure its psychological operations, reassessing its position in countries where the policy was covertly executed by the mercenaries. There is also the additional risk that mutineers collaborate, forming a new criminal collective.

Introduction – The Emperor Has No Clothes

The end of June witnessed the culmination of a long-running dispute between the Russian army and Yevgeny Prigozhin; a warlord executing Russian foreign policy, who is also a purveyor of information operations against the West and head of a private business empire. The mutiny of his private military company, ‘Wagner’ was triggered when the Russian Ministry of Defense tried to accelerate its control.

Even more shocking than the mutiny itself was the understated reaction of the Russian army, compounding the ease with which the Wagner group mercenaries took Rostov, a city of a million, which included the important Russian headquarters of the Southern Military District. The group then sent a column of several thousand fighters towards Moscow, which stood down on reaching a government settlement.

Who Is Yevgeny Prigozhin?

Yevgeny Prigozhin was born in 1961 into a well-to-do Soviet family. His mother was a doctor, and his father a mining engineer, however from adolescence he was already known to the juvenile courts for burglary and dealing in stolen goods, culminating with the aggravated robbery of a young woman, whom he robbed at knifepoint and nearly strangled to death. In 1981 he was sentenced to a total of 13 years in a penal colony for a plethora of criminal activities.

He left prison 10 years later as the country was slowly beginning to embrace free enterprise, and opened his first hot dog stand, which quickly became a success. From this humble beginning, Prigozhin expanded into a network of supermarkets and eateries, later founding the upscale, “New Island” restaurant in downtown St. Petersburg, frequented by a then-unknown city hall official; named Vladimir Putin.

Despite this, they didn’t meet until later, when Prigozhin and his associates needed an official ‘helping hand’ with their chain of casinos. At that time, gambling businesses were under the oversight of the city official; Putin, and casinos were legally required to take the city as a partner and share revenue. Despite the business booming, the casinos were turning a loss on paper, however, no investigations into corruption were made, despite numerous allegations.

A mere few years later, Prigozhin was hosting state dinners for Vladimir Putin at his establishments, with the presidents of France or the United States attending as guests.

Putin’s Chef

By the time Vladimir Putin had established his authority as president of the country, Prigozhin was expanding into the catering business, with his holding company; “Concord”, bidding for contracts in Moscow (including in the presidential palace, federal administration, and the ministry of defense). According to the Russian media, the value of these contracts reached over $3 billion. However, this is likely to be a conservative estimation. In addition to this, recent investigations revealed that Prigozhin secretly controlled further companies doing business with the state, giving him a near monopoly in catering services for the city of Moscow, as well as many state organizations.

Indeed, a police raid found documents and company stamps belonging to as many as 600 businesses in Prigozhin’s residence, most of them not legally tied to or owned by Concord group, but mostly managed by personnel working for companies, belonging to the holding. The true extent of the Prigozhin empire is thus extremely difficult to trace, and it is currently unknown to what extent these businesses will be shut down, taken over by competitors or left in operation.

The Troll Factory: Kremlin’s Privately Owned Psy-Ops Center

As a part of his lucrative business with the state, Prigozhin elevated his relationship with the Kremlin ten years ago, when he used his catering profits to fund the creation of the now infamous Internet Research Agency, known in the West as The Troll Factory. The agency was then used as a bedrock for Prigozhin’s new business interest – a media group – which is now a sprawling empire, playing an important role, firstly in influencing domestic public opinion (and vilifying the opposition, as ordered by the Kremlin) but also in election meddling in countries, deemed hostile to Kremlin, and undermining social cohesion by promoting pro-Russian narratives, or supplying autocrat support packages. The nature of the operations is a mixed bag of private enterprise and deniable government-ordered information operations.

The two approaches then intersect into so-called autocrat support packages, which are a combination of traditional tools of political marketing services with fake social media activity (used to support the power of various autocrats from Africa and Asia), and the projection of false images of popular support to third country audiences. Foreign countries pay for the services, but the customers are vetted by the Kremlin. On top of that, there is also a significant share of the standard advertising market and the ability to set the news agenda through the key node of the media empire, the RIA FAN news agency.

Wagner Pmc, Or Becoming Modern-Day Wallenstein

A further step of taking on roles typically performed by government – either overtly by the military, or covertly by the secret services – was establishing Wagner PMC, a private military company, operated by Yevgeny Prigozhin on the behest of Kremlin, since 2014. Prior to its establishment, some factions of the Russian military advocated for the use of private military companies to execute government policy in deniable operations. Most of these advocates were from military intelligence, with general Vladimir Alekseyev being the most senior known representative of this school of thought (often mistakenly labeled Gerasimov doctrine).

Recently revealed documents reveal fighters of Wagner PMC were among the first local militia groups that were used by the Russian government in its initial invasion of Ukraine in 2014. They also performed the role of Russian infantry in the Syrian war, where the operation to prop up the regime of Bashar al-Assad was sold to the Russian public as an air-campaign-only type of engagement in which no Russian servicemen were expected to die. It quickly became clear, however, that the Syrian army needed help on the ground: this was outsourced to the Wagner group, who were equipped and logistically supported by the Russian army. Prigozhin thus assumed the role of a modern-day Wallenstein, a warlord operating on the behest of the government, while pursuing his own business interest at the same time.

A similar scheme was then applied in other countries like Libya, and other African nations like the Central African Republic, Mali, and Sudan.

Why Did The Mercenaries Mutiny?

The reason is likely multifactorial, however a cynic might say it was a desperate act of a man who overestimated his position in the system, his relationship with the president, and usefulness for the state, at the same time underestimating the impact of his challenges on key players in the regime (including intended targets like defense minister Sergei Shoigu, and chief of the general staff Valery Gerasimov, both of which are extremely close to Putin).

It could be argued that the conflict between Prigozhin and the highest echelons of the army has been smoldering for years, or at least since 2018, when the Russian army deliberately let the US Air Force wipe out a unit of Wagner's troops, near Syria's Deir ez-Zor. It is alleged that the army's high command resented the competition of overpaid mercenaries, bound by almost no rules, and did not intend to accommodate Wagner, beyond the point of necessity. This inflamed Prigozhin's anger, fueling his personal attacks on the defense minister and the chief of general staff, whom he has consistently attacked as corrupt, inefficient, incompetent, and generally unworthy of their positions. The behind-the-scenes war for the president's favor was ultimately won by the army, rather than by the increasingly unmanageable warlord Prigozhin, who was clearly not content with his multi-billion-dollar business empire.

The catalyst for the mutiny was the recent announcement by the Russian Ministry of Defense that all private military companies and volunteer units would have to sign contracts with the Ministry of Defense, unifying the command structure at the front, under unambiguous military authority. This would mean the end of Wagner group's independence, jeopardy for Prigozhin's billions, and sidelining of his nascent political power.

The aim of the mutiny, therefore, was presumably to force the preservation of Wagner independence, and assert the role of Prigozhin as a powerful warlord with a personal army and ever-flowing revenue. The rebellion was arguably therefore not a question of overthrowing power structures, but an attempt to save this 'enterprise' in the hope that Wagner battlefield merits would be taken into account. As it stands, these merits are likely why Prigozhin has escaped the whole adventure with his life, albeit at the expense of his political power, and questionably greater expense of his business empire.

Some contend that Prigozhin failed to appreciate that this action would become a public challenge to Putin himself, but most would no doubt feel that it is almost unbelievable that such an entrenched beneficiary of the system should have made such a huge error of judgement.

The Cyber Perspective

One of the crucial parts of Prigozhin's power in Russia has been his media empire. This part of the business was officially shut down earlier this month, and other companies from the media group are reported to be closing in the coming week. Analysts speculate, however, that the core information operations and the psy-op part of the media group will be restructured and resurrected.

The Kremlin needs the services provided by Prigozhin's troll factories, and will likely seek to save the capability, under leadership of a different pro-Kremlin oligarch. Analysts speculate that this vacuum could be filled by the banker Yuri Kovalchuk, who owns most of the privately-operated media in the country and is a close friend and ally of Vladimir Putin.

Another question being discussed by analysts is the recent hacking activity, targeting Dozor; a Russian satellite communications company, in which the PMC logo was posted, and hundreds of files were leaked, (some of which link the FSB to Dozor, as well as the passwords of Dozor employees).

The attackers claim that they have damaged satellite terminals and confidential information stored on Dozor's servers, but this has not yet been confirmed. A pro-Ukrainian, 'false flag' operation remains very much a possibility: as Ukrainian cyber auxiliaries and psy-op operators have been using the mutiny to sow retaliatory chaos, increasingly targeting Russian social media, but also radio broadcasts in cyber-enabled information operations, inserting messages exploiting uncertainty caused by the Wagner mutiny.

The hackers were also able to exploit the chaos in the informational space, created by the lack of a coordinated response by the Russian government, inserting messages, stating Russia had declared martial law in response to a large-scale invasion. The operation gained enough traction to draw an official denial from a Kremlin spokesman.

Analysts are not yet sure of the perpetrators of the satellite company hack, however if this operation was conducted by hackers affiliated with Wagner PMC, it is likely that the collective would ignore the offer to sign contracts with the Russian military, offering its services on the black market instead. According to the deal between Wagner and the Kremlin, its base should move to Belarus, where the local government is not likely to put much pressure on the hacking element of the business, opening the possibility for a new powerful criminal hacking group to enter the market after cessation of its work on the behest of the Kremlin.

Conclusion

Although the immediate threat to the Russian regime has been averted, damage has nonetheless been done. The perception of Vladimir Putin's power and his apparent invulnerability has been eroded by the mutiny, and the Russian political system has arguably been weakened in a way that will be difficult for the Kremlin rulers to overcome: For 24 hours the emperor had no clothes, and the Russian people will now always remember that.

The question now is who will run the Kremlin's information operations, what will become of Prigozhin's empire. The situation has no easy solution for the Kremlin because the political model from the 'Thirty Years War' will not be easy for the Kremlin to cut off, without losing its laboriously built credibility in countries, where it operated through Wagner PMC.

It would be safe to assume that Prigozhin is now a Russian persona non grata, but has he become so powerful that the Kremlin will be obliged to let him keep (at least temporarily) part of his business empire, and continue to represent the Kremlin on other continents? This question is just one of the many levels of absurdity of this rebellion, to which only time has the answer for.

About the Author

Resident International Relations Analyst at Cyfirma, working for technology companies in Southeast Asia and the US since graduation from International Security Studies at Charles University in Prague in 2019. He focuses on international relations and security issues, especially on those revolving around West-East axis Stan can be reached online at (stan.vitek@cyfirma.com, https://twitter.com/FogOfWarCZ, etc..) and at our company website https://www.cyfirma.com

How Google Play Store Security May Fail to Protect Users from Stealthy Malware

Incremental Malicious Update Attack (IMUTA)

By Zia Muhammad and Zahid Anwar, Department of Computer Science, NDSU

Android is the leading operating system in the smartphone industry with more than 71% of the global market share. All Android-based smartphones arrive with a preinstalled application called Google Play Store which provides access to over 2.65 billion mobile applications and games. It is a free, powerful, and prominent platform for both mobile users and application developers.

In 2022 alone, more than 110 billion downloads were recorded through the Play Store. Due to such a high download volume, Google deploys a security tool called the Google Play Protect which scans all uploads in an attempt to root out potentially malicious applications dubbed as malware.

But is this tool self-sufficient and resilient to contemporary cyber-attacks? According to a recent research article published in the Journal of Ambient Intelligence and Humanized Computing (JAIHC), a stealthy cyberattack called an Incremental Malicious Update Attack (IMUTA) can use incremental updates to breach privacy and circumvent Google Play vetting policies. The attack works by users' trust in Google Play Store as a safe and authentic source of applications and stealthily collects private user data from the device that allows it to evade detection. This article examines how this attack works, why it is dangerous, and what Google should do to prevent it.

The Incremental Malicious Update Attack (IMUTA)

The researchers that developed the proof-of-concept malware aimed to demonstrate how easy it is to exploit customer trust and Google's policies to circumvent popular voice search applications. The research is published with the title "Circumventing Google Play vetting policies: a stealthy cyberattack that uses incremental updates to breach privacy." This is how it works:

1. Their first step was to upload a benign application called Voice Search to Google Play Store, which allows users to perform everyday actions through voice commands, such as calling someone or looking at the latest news and weather updates. Interesting the application passed Google's review process and was made public.
2. Afterwards, they released a second version of the application, which added some malicious functionality that accessed and used analytics, event logs, performed activity, demographics, and user location tracking. Interestingly Google also accepted this update within a single day.
3. The researchers finally released a third version, which really upped the game.. This version created a connection to a storage in the cloud to store data against each hacked phone. It collected contacts, version numbers, applications being used and manufacture, and model details. In addition, Users' personal data was collected when they opened the application and performed a voice action. Google also accepted this version within a single day.

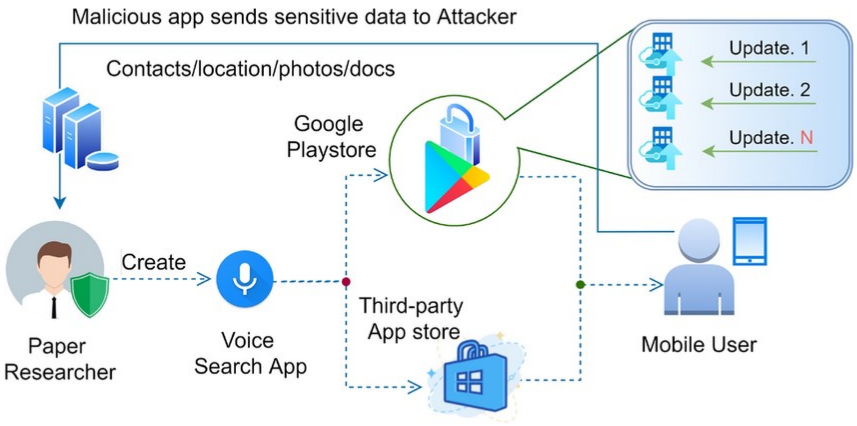


Fig.1: Incremental malicious update attack (IMUTA)

The multi-step approach of the underlined experiment circumvents vetting policies and makes IMUTA successful, a quick overview is provided in Fig.1. Through this attack, researchers were able to collect and exfiltrate private user data to their command-and-control server. The key to their success is incremental malicious updates that apparently builds trust with the server causing no alarms to be raised.

Why this attack is dangerous

This attack is dangerous for several reasons. It evades Google Play Protect security mechanisms by exploiting its relatively lenient trust policies allowing package distribution and feature updates. It exploits users' trust in the Google Play Store, which is a safe and authentic source of applications. Users are unlikely to suspect that an application downloaded from Google Play Store could become malicious through updates. Users may also grant permissions to the application without checking its functionality or content.

It is not certain that these kinds of attacks are just specific to the Google Play store, and this cannot be assumed that other application distribution platforms are immune. According to the researchers, the chosen voice search application is just one example and can be simultaneously replicated in other popular or sensitive applications such as banking, social media, or healthcare applications.

These kinds of attacks are complex, sophisticated, persistent, and remain undetected for an extended period of time. They can be used for various malicious purposes, such as financial gain, political gain, and sabotage. Moreover, the collected data can be used to perform identity theft, fraud, blackmail, phishing, or espionage.

What Google should do to prevent it

There should be a reevaluation of vetting policies in order to improve the security posture of Google Play to protect its users. For instance, a significant portion of such attacks can be blocked by acquiring information on the updated application module from a developer individually and calculating the similarity index based on the code similarity of the earlier version with the new variant. This similarity index will help to spot significant differences and flag suspicious updates.

Moreover, the updated code should be merged directly with the previous version instead of replacing an application entirely. Currently, a new version entirely replaces the older version, which increases the chances of dynamic code loading and reduces the trackability over malicious injections.

In addition, the security mechanism deployed by Google should perform critical analysis of application updates with the same rigor as initial applications, including checking for maliciousness, hidden intents, requested permissions, provided functionality, and comparing the code of published versions of the application and its updates.

Finally, it is essential to educate users about the risks of downloading and updating applications from any source, even from Google Play Store. They should be encouraged to review each application's permissions, functionality, and content before installing or updating it. In order to ensure the security and privacy of users, these measures can be significant steps in preventing stealthy malware attacks like IMUTA and maintain its reputation as a trusted provider of Android applications.

About the Author

Zia Muhammad is a Ph.D. scholar in the Department of Computer Science at North Dakota State University. Zia can be reached online at (zia.muhammad@ndsu.edu and https://www.linkedin.com/in/zianoedar/)

Zahid Anwar is an Associate Professor of Cybersecurity in the NDSU Department of Computer Science and a scholar of the Challey Institute for Global Innovation and Growth. His research focuses on cybersecurity policy and innovative cyber defense. He has authored more than 100 publications in peer-reviewed conferences and journals. He is a CompTIA-certified penetration tester, security+ professional, and an AWS-certified cloud solutions architect. Prior to working in academia, he worked as a software engineer and researcher at IBM T. J. Watson, Intel, Motorola, the National Center for Supercomputing Applications, xFlow research, and CERN. Dr. Anwar received his Ph.D. in computer science from the University of Illinois in 2008.

Rethinking SASE: Why Migrate Cybersecurity from Cloud to Browser

By John "JP" Peterson, Chief Product Officer, High Wire Networks

Cyberthreats are the scourge of our day. Few would argue, but there's little consensus about what to do about it. The vanishing perimeter is to blame. We've now got to protect an ephemeral network edge made up of devices that are not only portable but mobile.

Secure Service Access Edge (SASE) architectures emerged as a cloud-based answer to this problem. In 2019 Gartner, a leading technology research firm, called SASE the "future of network security" because it uses software-defined, dynamically-created, policy-based and cloud-delivered security to lock down access at the ever-expanding network edge.

Vendors and enterprises were quick to jump on the SASE bandwagon to retain centralized control over network security. It's been and continues to be a long and expensive journey because we've been building the car along the way.

Instead of continuing to go down the long and winding SASE road, cybersecurity experts like me believe it's time to go a different route. Rather than put security in the cloud, let's put it in the critical access point – the web browser.

We're not alone in this thinking. Gartner says, "By 2030, enterprise browsers and extensions will be the core platform for delivering workforce productivity and security software on managed and unmanaged devices for a seamless hybrid work experience."

What is Browser-based Security?

Browser-based security comes in two forms:

- **Enterprise browser** – a standalone application with integrated security and centralized policy management that replaces the existing browser
- **Browser extension** – a plugin to an existing browser like Google Chrome or Microsoft Edge that delivers security services

Enterprise browsers and extensions promise a lightweight, low-latency and low-cost way of delivering the functionality of existing security technologies like SASE.

Gartner predicts that enterprise browsing products will compete with and replace some incumbent legacy security tools such as:

- Virtual private networks (VPN)
- Virtual desktop infrastructure (VDI)
- Remote browser isolation (RBI)
- Zero trust network access (ZTNA)
- Cloud access security broker (CASB)
- Secure web gateway (SWG)

Why Is Browser-based Security a Good Idea?

The web browser is the tool used the most at work to access information, social networks and cloud-based productivity apps. As such, it's the tool cybercriminals target the most. Protecting traffic to and from the web browser is paramount.

With a SASE platform, you need to send browser traffic to the cloud, which significantly impacts performance, slowing page load times by tens of seconds compared with milliseconds using secure browser alternatives. On top of suboptimal performance, you must also pay for SASE servers in the cloud, while secure browsers and extensions are low-cost local applications.

Additionally, secure browsers can leverage the distributed computing power of all other browsers/extensions in their network for free rather than paying a SASE provider for high-cost cloud computing.

Secure browsers offer better use of compute resources, reduce latency, improve performance issues and result in a better defense position.

Why Is ‘Bring Your Own Browser’ Security a Better Option?

While both secure browser forms have merit, the browser extension, or “bring your own browser” approach, is the better option for the following reasons:

- It’s easy to adopt. Users continue to use the browser they like.
- It’s easy to deploy. Users are familiar with other browser extensions for quick access to apps they use every day.
- It enables the delivery of the same security services provided over SASE platforms.

Some of the capabilities a secure browser extension can deliver include:

- Antivirus
- Antiphishing
- Data Loss Protection
- Secure Web Gateway
- Firewall
- More

It’s early days for secure browser technology, but the sky is the limit.

What is the Future of Secure Browser Extensions?

A browser security module offers a range of exciting possibilities in the future. It has more capabilities than just a browser extension. Here are a few we’re building into the Overwatch CyberLab SWARM™ Browser Security Module:

Strength in numbers – If all users had secure browser extensions, then all browsers could talk to each other and share information to mount a better defense. So, for example, when one user (“patient zero”) clicks on a phishing link, other users will be automatically protected from doing so. It’s like a hive mind or herd immunity. We SWARM™ together, also known as Secure Web Application Response Module.

Application Proxy – There’s only so much you can do inside the browser. However, if you extend the browser’s capability into the operating system (OS), you have nearly infinite capabilities. To make this happen, we’ve built an OS Communication Proxy™ that bridges the browser to the OS, not unlike middleware.

Embedded URL Inspection™ – Security solutions commonly inspect the main URL for a web page but not the embedded URLs like those for ads, videos and graphics. Many times these URLs lead to sites that are compromised. So, the trusted site may be propagating malicious code through embedded URLs. We inspect them all in real-time.

Known vs. Unknown – The security industry has done a good job of blocklisting known phishing sites but a poor job of detecting unknown phishing sites. Sometimes phishing sites are unknown because they target one person in a spear phishing or whaling campaign. To detect these unknown phishing sites, we've created AI-driven tech that investigates the URL like a human security analyst. Essentially, we've put the human mind in an algorithm to check several variables before the page is allowed to load. If the analysis comes back as high risk, the browser can alert the user, block the site or display it as "read only" so the user cannot enter their personal or financial information.

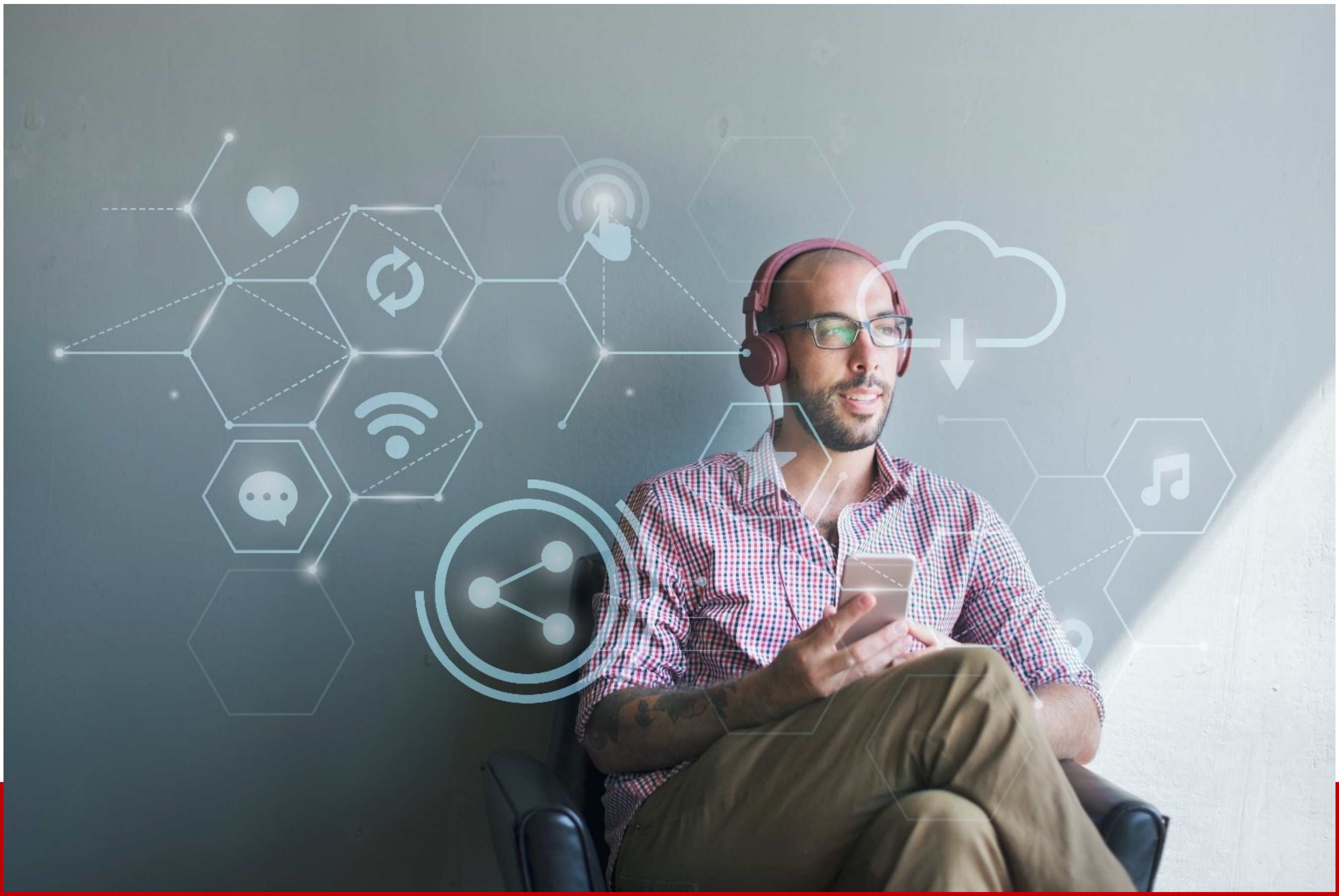
Conclusion

The potential of secure browsers is exciting and promising. Gartner agrees, noting that the browser will become a platform from which enterprises can distribute software, collect intelligence, control access and securely enable remote work.

About the Author

John "JP" Peterson is the Chief Product Officer for High Wire Networks, Inc. (OTCQB: HWNI), a leading global provider of managed cybersecurity and technology enablement. Peterson leads High Wire's Overwatch CyberLab, Inc. and High Wire's product strategy and development. He brings to the position more than 30 years of entrepreneurial and executive experience in product development, sales engineering and technological innovation at leading global technology and cybersecurity companies, including Ericom (Ericsson), Cisco Systems, Fortinet, Barracuda Networks, Juniper Networks, Comodo, U.S. Robotics and 3Com. Peterson has led several tech startups he helped fund and scale through acquisitions and initial public offerings. He is a prolific inventor of leading-edge cybersecurity technology and is named on 13 patents and patent applications that represent major advances for the industry.

"JP" Peterson can be reached online at (john.peterson@highwirenetworks.com and at our company website Managed Network Security and Technology Services - High Wire Networks



Four Years and a Pandemic Later: Have Agencies Become Cloud Smart?

By James Langley, Master Solutions Consultant, Hitachi Vantara Federal

June 2023 marked the four-year anniversary of the release of the final Cloud Smart strategy, which was the government's update to the sweeping Cloud First strategy originally issued in 2011. Cloud First was designed to push Federal agencies to migrate to the cloud. Cloud Smart offered agencies the flexibility to adopt cloud technology according to mission needs.

While four years can feel like a different world from a technological perspective, it is not a lot of time when it comes to effective change in government, especially given the significant disruptions caused by the pandemic since Cloud Smart was issued. Agencies that were working towards Cloud First mandates for eight years may not have been able to fully pivot over the past four years, leaving them unable to realize the full benefits of becoming Cloud Smart.

Cloud First: A Flawed Approach to Cloud Migration

The intent behind Cloud First was to modernize and secure government systems and applications, which were years behind the private sector. However, Cloud First did not include detailed guidelines on how to adopt cloud technology, leaving many agencies to forge their own migration path and creating myriad complex and stop-gap solutions.

As more agencies started the migration process, they began to realize the flaws of the wholesale cloud migration strategy called for in Cloud First.

- **Cloud is expensive.** Agencies assumed that they would gain cost savings by migrating to the cloud because they would no longer need to maintain on-premises data centers. In many cases, they found that cloud was more expensive, especially if they didn't have a cloud data management plan. It is cheap to move data into the cloud, but expensive to get it out, and access or egress fees are an unpredictable cost that many agencies could not plan for effectively. Automatic and self-service provisioning quickly added cloud resources when needed, but didn't always reduce capacity when it wasn't needed, leaving agencies paying for cloud they weren't using. Cloud pricing was also confusing, further complicating the issue. Currently, the government pays billions in taxpayer money for cloud.
- **Security is a concern.** Moving from on-premises data centers to the cloud takes some control over data and application security away from government technology leaders. This can be especially concerning when looking at national security, trade secrets, or personal identifiable information.
- **Legacy applications don't work in the cloud.** Getting existing applications cloud ready was more complicated than expected. Many could not migrate to the cloud – or were prone to bugs or cost overruns if they were placed in the cloud anyway.
- **Cloud migration led to vendor lock-in**. Agencies using the more advanced tools and services of hyperscalers found that they were proprietary, leading to the vendor lock-in they sought to avoid.

Cloud Smart was designed to overcome many of these issues, but agencies still operating with a Cloud First mindset continue to experience many of these problems.

Cloud Is Not a Destination

One of the key lessons learned from Cloud First is that cloud isn't a destination. Not everything should be moved to the cloud, and many things that are moved shouldn't be left there. Agencies should view cloud as an operating model centered around utility and self-service – use and pay for cloud services when, where, and if they are needed. Cloud spending should be balanced with existing infrastructure investments to optimize agency technology budgets – and taxpayer money.

Adopting a Cloud Smart Mindset

Cloud Smart offers specific guidance and recommendations to identify what workloads should – and should not – be migrated to different types of cloud environments – public, private, hybrid, multi, or near cloud.

It lays the framework for government IT modernization because it gives agencies the guidelines and choice for how to upgrade their infrastructures. With the explosion in data collected from the data center to the edge, the push for stronger cybersecurity, and the need to tap into the power of emerging technologies like artificial intelligence, agencies must shift their mindsets. Moving from Cloud First to the holistic Cloud Smart approach to modernize their infrastructures effectively will allow them to innovate new solutions.

The architects of Cloud Smart outlined three fundamental pillars of success for cloud migration: security, procurement, and skills. These pillars are key in helping agencies achieve the Cloud Smart strategy. Agencies need to align the pillars to tools and services that are available today to achieve the goals of the strategy.

Security

Data management is complicated under a Cloud First mindset. Apps built for one cloud environment may not work properly in another part of the environment, leaving them vulnerable to cyberattacks. Accessing data that may live in different places at different times becomes challenging when implementing zero trust. Canceling a hyperscaler contract that is intertwined in a hybrid cloud infrastructure is extremely difficult, leaving agencies at the mercy of that hyperscaler's security policies.

To solve these security issues, agencies can look at near-cloud solutions that include an outsourced physical data center that connects with other cloud providers. Companies that offer near-cloud solutions maintain an agency's data sovereignty while enabling the agency to maintain oversight, management, and security of the hybrid cloud infrastructure.

Near-cloud environments typically use predictive analytics tools to monitor for threats across the hybrid cloud environment, as well as swift mitigation tools to support quick recovery in case of a breach at any place within the hybrid cloud.

Agencies can benefit by looking beyond cloud solutions that are already FedRAMP certified to find products that are FedRAMP compliant. Industry can shoulder the cost burden of certification, so agency choice need not be limited to certified products.

Procurement

Cloud procurement should be approached by looking at workloads, not destinations. That way, agencies are basing cloud procurement on the consumption required to meet the specific needs of each workload rather than a cloud solution to place all workloads. Agencies can realize cost savings on cloud consumption by partnering with organizations that offer X-as-a-service (XaaS) pricing – which includes organizations beyond the hyperscalers – allowing them to pay for any IT solution based on how much they actually need and use.

Agencies still operating under a Cloud First structure may struggle to procure on-premises or edge cloud solutions that can provide the most cost-effective and secure environment for a particular mission's needs. A key step to realizing the benefits of Cloud Smart is for cloud project managers to expand their focus and scope to include consideration of private, hybrid, and near cloud solutions.

Skills

The skills gap in government technology has been a serious factor since Cloud First was issued. That gap continues to grow, especially in a post-pandemic environment.

Taking advantage of automation in any cloud or on-premises environment is one way to overcome the skills gap. Agencies should demand more automation capabilities from industry to support private, hybrid, and near cloud solutions. Wizard-driven or workflow-driven activities should replace manual intervention and tasks.

Looking Ahead

While future innovations are inevitable, agencies must recognize the need to expand their cloud strategies beyond mere migration and actively embrace diverse architectures and solutions, such as private, hybrid, multi, and near cloud. By forging strong partnerships with industry experts, agencies can successfully achieve their ultimate objective of becoming Cloud Smart and effectively serve the American people.

About the Author

James Langley is the Master Solutions Consultant of Hitachi Vantara Federal, a wholly owned subsidiary of Hitachi Vantara, with more than 20 years of experience in the IT industry and a decade as a trusted adviser for federal civilian, defense and intelligence agencies. James can be reached at james.langley@hitachivantarafederal.com or at our company website www.hitachivantarafederal.com

Embracing Zero Trust Architecture: A Critical Best Practice for Cybersecurity in Enterprises

By Walt Szablowski, Founder and Executive Chairman, Eracent

Summary: With the increasing frequency and sophistication of cyberattacks in the digital landscape, and the failure of legacy cybersecurity tools and methods, prioritization by large-scale enterprises of cybersecurity best practices has never been more important. In particular, Zero Trust Architecture (ZTA), has emerged as a favored security framework to the persistent cybersecurity failures. With adoption by the U.S. Government and an increasing number of enterprise corporations, the Zero Trust cyber security architecture attempt to turn around the current failed cybersecurity methods and tools.

Article: After 30 years of Cyber Security failures, and cyberattacks continuing to increase in frequency and scale. The US government has made prioritizing cybersecurity Zero Trust architecture critical for organizations, especially large-scale enterprises where the potential for loss and disruption is enormous.

To mitigate these risks, the U.S. government has ordered the adoption of Zero Trust Architecture, and enterprise organizations are following suit. However, Gartner reports, despite rising support for this framework, only 1 percent of organizations currently have a security program that meets the definition of

Zero Trust, and only 10 percent are predicted to satisfy the full criteria of a Zero Trust program by 2026 (1). With the increasing prevalence and growing cost of cybercrime, it's critical for cybersecurity leadership to quicken the pace of ZTA implementation.

The Impact of Cyber-Risks on Large-Enterprise Organizations

While the magnitude of loss and disruption caused by a cybersecurity breach depends on factors such as the nature and scale of the attack, the industry, and the cybersecurity measures in place, cyberattacks have the power to completely disrupt an organization.

First, the costs associated with cyber attacks can be substantial. The 2021 Cost of a Data Breach Report by IBM Security and Ponemon Institute found that the average total cost of a data breach for a large enterprise was $4.96 million.(2) This includes expenses related to incident response, investigation, notification, legal support, and recovery efforts.

Then there's the indirect financial impact of a cyber attack — such as lost business opportunities, customer churn, and damage to the organization's brand and reputation. A study by Lloyd's of London estimated that cyber attacks cost businesses globally $400 billion per year in terms of lost productivity and reputational damage.(3)

In addition to these financial losses, cyberattacks can result in legal and regulatory consequences, undermine customer confidence and loyalty, and cause operational disruptions that impact productivity and customer service.

In light of these potential catastrophic consequences, it's no wonder large enterprises are prioritizing cybersecurity as a strategic initiative and implementing zero trust best practices to safeguard against cybersecurity threats.

New Approaches to Cybersecurity Threat Management

Some of the most notable technologies and approaches to enhanced protection include:

- The implementation of a Zero Trust Architecture through a managed process. Zero Trust Architecture (ZTA) emphasizes strict access controls and continuous verification to help organizations secure their networks and resources.
- Defining management Policies and process definitions to manage risk.
- Defining and applying risk reduction methodologies.
- Auditing and verifying tools data generation accuracy and scope.
- Artificial Intelligence (AI) and Machine Learning (ML) practices to top of accurate and complete network data to help manage potential cybersecurity threats in real-time and automate security processes.

- User and Entity Behavior Analytics (UEBA) through a managed process to use machine learning algorithms to analyze user behavior patterns and identify deviations that could indicate malicious activity or insider threats, allowing for early detection and response.
- Next-Generation Firewalls (NGFW) applying segmentation and Mini segmentation to go beyond the capabilities of traditional firewalls to provide intrusion prevention, deep packet inspection as required, and application-aware filtering in order to detect and block sophisticated threats and offer more granular control over network communications.
- Endpoint Detection and Response (EDR) solutions focus on detecting and responding to threats at the endpoint level, such as workstations, laptops, and servers.
- Cloud Security Solutions protect cloud environments and data; solutions include cloud access security brokers (CASBs), cloud workload protection platforms (CWPPs), and cloud-native security tools.
- Security Orchestration, Automation, and Response (SOAR) automates and streamlines security operations by integrating various security tools, orchestrating incident response workflows, and automating routine tasks.
- DevSecOps is an approach that integrates security practices into the software development and deployment process

These are just a few of the approaches available to large-scale enterprises for the management of cybersecurity threats. A multilayered managed approach that combines various technologies, ownership and best practices is ideal — Zero Trust Architecture has risen to prominence as a failsafe safeguard from cybersecurity threats.

What Is Zero Trust Architecture?

In response to the evolving cybersecurity landscape and after traditional security approaches have proven to be insufficient, the U.S. Government has ordered the adoption of ZTA as a more proactive and robust security model to counter threats. And enterprise corporations, known for their siloed organizational structures which can inhibit critical communication when managing data across an enterprise network, are quickly jumping on board with this up-and-coming security solution.(4)

What exactly is Zero Trust Architecture? ZTA is a security framework and approach that challenges the traditional perimeter-based security model. It’s based on the simple yet critical principle of "never trust, always verify" and assumes that no user or device should be inherently trusted, and all transactions must be verified whether they’re located inside or outside the network perimeter.

The adoption of Zero Trust Architecture (ZTA) is gaining traction across various industries and large-scale enterprise organizations. Many organizations, including Fortune 500 companies, government agencies, and financial institutions, have recognized the benefits of ZTA and are actively implementing or considering its adoption. A 2021 survey conducted by Pulse Secure found that 60 percent of IT decision-makers across organizations of different sizes and sectors were planning to implement Zero Trust initiatives.(5)

The Future of Cybersecurity

While cybersecurity leaders have their work cut out for them as they work to meet the criteria of a mature Zero Trust framework against an increasingly threatening digital environment, it’s clear they’re on the right track. Given the emphasis on data protection, the evolving threat landscape, and the need for modernized security approaches, it’s no wonder that ZTA has emerged as a favored security framework.

About the Author

Walt Szablowski is the Founder and Executive Chairman of Eracent and serves as Chair of Eracent’s subsidiaries (Eracent SP ZOO, Warsaw, Poland; Eracent Private LTD in Bangalore, India, and Eracent Brazil). Eracent helps its customers meet the challenges of managing IT network assets, software licenses, and cybersecurity in today’s complex and evolving IT environments. Eracent’s enterprise clients save significantly on their annual software spend, reduce their audit and security risks, and establish more efficient asset management processes. Eracent’s client base includes some of the world’s largest corporate and government networks and IT environments. Dozens of Fortune 500 companies rely on Eracent solutions to manage and protect their networks. To learn more, visit http://www.eracent.com/ztrp.

Visibility Isn’t Enough; It’s What You Do with It That Counts

By Christina Richmond, Chief Strategy and Growth Officer, Inspira Enterprise

As cyber risks continue to grow and evolve (here’s looking at you, generative AI) – more and more vulnerabilities are being created, which means cybersecurity professionals must constantly adapt their strategies and tactics. A big part of the security equation involves continuous monitoring and, above all, greater visibility.

Visibility is essentially the elephant in the room. Almost every IT leader today knows they need more of it, but they’re still struggling to obtain a broader view. And what’s more, while visibility is extremely important, it’s not enough. Countless vendors tout their ability to expand organizations’ visibility of their networks, of their systems and of their security tools. But you can’t stop there; it’s what you do with the visibility you've achieved that really matters. The bottom line? This challenge won’t be solved by humans alone.

The constant need for more visibility

To truly get a handle on cybersecurity, you need the ability to see the full picture of your networks, your tools and so on. This will enable you to see where things are broken, where things aren't implemented properly and where your management is accepting risk that probably isn't acceptable. Therefore, you need to harden more of your data and your identities and lock down access. Many times, when companies accept a lot of risk, they aren't taking these steps.

And what's more, despite all the conversations about visibility, it remains a significant problem. Survey after survey finds that organizations are still struggling to get control over their assets. The explosion of endpoints and the growth of a more distributed enterprise are among the many factors contributing to this situation.

You can't protect what you can't see. You must know what you have, and you must see the traffic and the output from all your security tools. But even if you can gain this visibility, it's going to quickly overwhelm your staff – and it's not enough by itself.

Going a step beyond visibility

Gaining more visibility is a double-edged sword. There's the positive side of being able to see more of your network, but the downside is it can quickly lead to alert fatigue amongst your analysts tasked with monitoring it. Having too many alerts is always going to leave you a few paces behind – and it can lead to significant burnout. In fact, SOC analysts statistically have high rates of burnout, driven largely by alert overload. According to the Ponemon Institute, 65% of SOC professionals have considered quitting their jobs due to stress.

There are simply too many alerts for humans alone to handle; it's not realistic anymore to assume they can. To make the most out of expanded visibility you need a better way to monitor it, which is where automation can play a key role. You also need remediation and responsibility capabilities too. Organizations need to take visibility one step further, but they are not going to be able to do it with their human staff. They must add appropriate technologies to partner with people.

This brings up the inevitable question of whether automation is safe or will open up your organization to new risks. A parallel of this scenario is the rise of cloud computing. In the beginning, there was a great deal of concern about security in cloud computing, but now most people think the cloud is more secure. The reality is that automation is quickly becoming a necessity for security and if you don't use it, you won't succeed. Organizations need to get comfortable with automating some remediation and response via security technologies because organizations will not be able to successfully hand these massive tasks off to their humans. Attackers are using automation more and more, so organizations need to fight fire with fire.

A quick caveat, though: you can't automate all remediations across all environments. Start with lower-priority devices, data and networks. Once you've got those working well, see where else automation is feasible.

Best practices for using automation to help go beyond visibility

Gathering threat intelligence isn't enough; it's how the intelligence is correlated that truly makes the difference. Automation and machine learning can assist with ingestion, correlation and resulting output that provides visibility into threats that may have been previously unknown. This analysis must be able to scale to the volume of threats that exist today, which cannot be done manually. With correlation to other data sets, and with detection technologies, a threat can be discovered.

Security orchestration, automation, and response (SOAR) technologies can help prescribe a course of action when an anomaly is discovered. Previously burdened with time-consuming and repetitive duties, SOC teams are freed to resolve problems more quickly. This lowers expenses, increases productivity and fills in coverage gaps.

It's also important to streamline processes so the information that comes from greater visibility is used rather than bogged down in slow processes. Using AI, ML and automation will simplify ingestion, analysis and recommended remediation steps, which will reduce the process slow-down.

Information plus automation

Once you can see all that you need to see across your IT environment, you quickly realize that a humans-only approach to cybersecurity is no longer viable. Taking visibility to the next level isn't going to be done with humans alone; it's simply too big a task. Automation and machine learning are ideal for this scenario. Use the best practices noted above to maximize the value of the information visibility provides and optimize your cybersecurity stance.

About the Author

Christina Richmond is the Chief Strategy and Growth Officer for Inspira Enterprise, a global cybersecurity risk management and digital transformation service provider across the Americas, Asia Pacific, Middle East, India and Africa regions. She is a long-time cybersecurity advisor and recognized luminary in the industry. For nearly a decade, Christina was a well-known industry analyst and led the global security services research practice at IDC.

4 Key Security Challenges to Address with Confidential Computing

Confidential Computing delivers a variety of security benefits and helps deliver a platform for controlled, compliant activation of sensitive data

By Simon Johnson, Senior Principal Engineer at Intel

Over the last decade, businesses have become increasingly reliant on data monetization, especially as workloads have moved to the cloud. But the rise in number and size of data breaches continues to highlight how much the datafication of personal information is being monetized by companies and threat actors alike. As a result, privacy preserving data services are growing in customer demand and increasingly becoming a regulatory requirement. Meeting that demand requires additional layers of protection that can help separate the processing of user data from the platform owner or administrator.

Meeting that challenge has been the driving force for Confidential Computing. At a high level, Confidential Computing protects data in use during processing, with sensitive data isolated in the CPU and encrypted in memory while it's processed. The main premise behind separating user data from platform owner control (whether through a service or on-prem) is that those controlling the platform and those accessing data on the platform being processed are two separate entities.

Confidential Computing delivers a variety of security benefits associated with hardware-based enforcement of data and IP access policies. For example, protecting against un-permissioned data access (even with escalated privileges), containing the "blast radius" of compromised software or unauthorized users, and protecting data and IP deployed at partner or remote sites. But Confidential Computing is also transforming businesses by helping to deliver a platform for controlled, compliant activation of sensitive data. That might include compliant multi-party or inter-department collaboration, privacy-preserving data services, confidential and compliant AI, and more.

In order for this technology to become more pervasive, it must be usable, deployable, and not detrimental to either the data owner's or the platform owner's cost models – all while delivering security value. Finding this balance is what both drives and constrains progress in this field. What are some of the new security challenges the industry faces as we continue to advance in Confidential Computing? Here are four:

- **Post-Quantum Crypto (PQC) Hardening –** The entire computing industry is amid what will be a decade-long transition (or more) to post-quantum safe computing. This transition is where the cryptographic algorithms used in the modern era must change to prevent attacks from quantum computer-based attacks. In some instances, the transition efforts may require that we encrypt data with a change of key length. However, in other cases, new PQC algorithms need to be invented and standardized. There is a lot of working happening in this area.

- **Attestation Complexities –** Part of the element of a Confidential Computing model is understanding the state of the security posture of platforms to which execution is deployed. This process is known as attestation, and it is still in its infancy. Developing and appraising policies to determine actions when platforms are out of update or configuration isn't up to standard is still a developing area. Finding ways of making these processes more understandable, digestible, and automated continue to develop.

  In addition, we have seen many users of Confidential Computing request heterogeneity in the platforms, clouds, and software stacks. This introduces other challenges in making cross-platform, cross-cloud, and cross-trust authority assessments more complex.

- **Side-Channel Attacks –** A side-channel attack, or an attempt to extract secrets from a chip or a system, can happen in any digital system. For example, CPU vulnerabilities (such as Meltdown and Spectre) allowed unauthorized reads of data in running programs and illustrated the challenges of side-channel attacks. While many side-channel attacks are shown in academic or laboratory scenarios, the risks are increased in cloud computing environments that rely on coresident virtual machines. As hardware and software solutions improve to supply mitigations in this space, IT departments can benefit by establishing best practices and mitigations to combat side-channel attacks.

- **Physical Attacks –** A Confidential Computing model emphasizes the separation of platform administrator from user data being operated on it. But as the processing locations become more remote, or platform administration is further subdivided, or third parties become responsible for platform operations, protections from the individual with platform proximity are necessary.

Confidential Computing solutions combines a robust set of hardware features and a rich, vibrant software ecosystem that is in place today and continued growth is expected. The Confidential Computing software ecosystem includes containerized software development kits (SDKs) and shim layers or library operating systems that allow either partial or full applications to be included within the trust boundary. It also includes middleware that allows multiple applications to be brought together securely and orchestrated across an infrastructure provider's network. Finally, the market needs software services for attestation of Confidential Computing instances on a variety of devices so they can be verified at the time of use.

Unfortunately, bad actors will continue to try and exploit cloud security vulnerabilities. Implementing a Confidential Computing ecosystem can help combat these cloud security threats, working not as a one-off CPU feature, but as a larger infrastructure that brings secure computing to the masses. It can help ensure the strongest protections are enacted anytime, anywhere on any computing device, reducing risks and concerns for both suppliers and users. To learn more about Confidential Computing advances, check out OC3 and the Confidential Computing Consortium.

About the Author

Simon Johnson is a Senior Principal Engineer and Confidential Compute Technical Director for the SGX and TDX programs at Intel Corporation. As a confidential computing technical evangelist, Simon engages with partner organizations on how to deliver world-class experiences and identify and accelerate the next generation of hardware capabilities in the confidential computing space. Simon has been in the information security space over 25 years, previously working for the UK Government as an information security specialist developing capabilities and advising a number of national scale projects. He holds a bachelor’s degree in computer science from the University of York, UK.

For more, visit the Intel Corporation company website at https://www.intel.com/.

Guarding Against the Insider Threat: Do Your Employees Pose the Greatest Risk?

By Moty Kanias, VP of Cyber Strategy & Alliances, NanoLock Security

Great businesses understand that their people are their most important assets. But there is another side to that coin. Employees and contractors may also threaten your company by virtue of their access and expertise. Most experts consider three categories of insider threats: preventable mistakes due to simple human error, stolen credentials, and criminal or malicious actors. Issues from the first two categories are much more frequent than those from the third category, but all insider attacks are on the rise.

The 2021 incident in Oldsmar, Florida is evidence of the impact of human error — what was initially thought of as a malicious remote access incident turned out to be an in-house employee accidentally having clicked the wrong buttons.

The 2023 charge against the attack on Discovery Bay Water Treatment facility in Tracy, California, on the other hand, shows us how well-meaning employees or contractors can turn against their employers, instigate attacks, and potentially cause significant damage.

The above examples hint at a much larger problem. In fact, according to the Ponemon Institute, every single company that they surveyed had an insider incident last year.

Companies need to assess if they have given their people too many permissions and not enough safeguards when it comes to cybersecurity policy. This is especially true for industrial and critical infrastructure targets, as well as utilities and energy infrastructures, which have vast networks of connected devices, both new and legacy, and numerous personnel to manage them who need credentials. Here, we'll answer a few questions about how insider attacks threaten our infrastructures.

What makes insiders so dangerous to industrial and manufacturing targets?

All it takes is a single unsecured device or a single worker to make an error or be manipulated. Insider attackers often already know where valuable information is kept, understand how it can be used, and know what's normal (or not normal) to do so that alarms aren't triggered. They also have legitimate credentials, which means they may not need to do much "attacking" at all. This makes them difficult to detect until it is too late, at which point many industrial and manufacturing targets are tempted to concede to certain demands in order to keep operations moving. Stopping operations is a last resort, both because of the financial and reputational ramifications. Insiders understand this and exploit it for leverage.

With the new and increasing abilities of AI in fields of massive content production including text and deep fake voice clones, human manipulation is becoming significantly harder to identify, thereby raising the risks of cyber events to a new level.

Why haven't we heard more about insider attacks?

Though recent research and reporting have shed a light on the rising tide of insider attacks, we historically have not heard much about these sorts of incidents. This is because for the companies who are victimized, these incidents can represent "dirty laundry" that they'd rather not air to the public. There's also often a threat, implicit or implied, that the hack will get worse if authorities are involved, impacting negotiations and decisions on whether to pay a ransom or not and potentially requiring disclosure of sensitive information to the authorities.

Insider attacks can also be easier for people to tune out because these incidents frequently stem from mundane mistakes. Simple human error is a huge source of insider attacks, but news and entertainment typically prefer to show a master hacker in a remote van rather than a technician simply forgetting to log out.

For a high-profile example of an insider manipulation attack using a compromised credential, look no further than the Colonial Pipeline incident. In response to a ransomware attack sourced from an insider breach of their IT network, they shut down operations for their entire pipeline system.

How can we improve reporting?

Organizations are often lax with their implicit trust of employees and partners, as well as the fact that they will be reluctant to report incidents when they occur. A lack of transparency from targets of insider attacks advantages attackers in a number of ways. Firstly, they are more likely to receive (and retain) any sort of ransom payment if authorities are never involved. Secondly, unreported and unpatched vulnerabilities offer an opportunity for hackers to expand their operations under the radar. Only the introduction and enforcement of comprehensive regulations that mandate cyber incident reporting will force organizations to adopt true transparency when they are attacked. In some regions, such as the EU, the NIS2 directive mandates cyber incident reporting, while in other regions it has not yet become mandatory.

What other strategies can we adopt then?

Rather than attempting to patch our way to perfect protection, we can accept that human error will always be a factor and shift focus from access interception to outcome prevention. Assume that breaches will happen. Then what? If we can find a way to better define the level of privileges of our workers, and educate them about the threats, intruders will have a much harder task. Their access becomes much less threatening. A hacker with access but no abilities is a lot less problematic and a lot more fixable than the alternative, especially when they are an insider with privileged knowledge. Zero Trust is the key to defeating insider attacks because it's not insiders that are the problem - it's insider privilege. Manage and monitor that privilege and you can eliminate the attack vector.

About the Author

Moty Kanias, Vice President of Cyber Strategy and Alliances for NanoLock, is a veteran of the Israeli security forces (Col. res) with vast experience in cyber security, counter-intelligence and insiders threats. In his previous position, Moty served as a senior executive in the Israeli Prime Minister's office, managing research of new civil defense & aerospace technologies. Previously, Moty served as the head of counter-intelligence and cyber threats research branch in the IDF and his work was awarded several certificates of excellence.

Moty also served as a division manager in the ministry of Defense Security Authority (D.S.D.E - Directorate of Security of the Defense Establishment), leading a counter-intelligence task force that researched cyber technologies and human vulnerabilities, such as insiders. Moty holds a BA in history and Jewish philosophy from Tel Aviv University.

Moty can be reached online at (motyk@nanolocksec.com) and more information can be found on the company website https://www.nanolocksecurity.com/

National Cyber Security Vulnerabilities in The Changing Security Environment

Implications For the Resilience of The NATO Cyber and Information Space

By Georgi Atanasov, Subject Matter Expert in Bulgarian ministry of defense

In the changed security environment states are seeking to achieve their strategic goals as quickly as possible and with fewer resources. This mindset is gradually gaining popularity among the military and national security decision-makers who would grab every opportunity to achieve more with less. This growing appetite for speed and cost-effectiveness is reflected at a military level, where increasingly the battlefield shifts to cyber and information space as this environment offers unique opportunities to impose cost on adversaries at the speed of light, with impunity and zero casualties.

That is why, NATO must remain vigilant and aware that cyberspace is dangerously insecure and the allies' safety can be jeopardized through this man-made operational domain. The security of the alliance's cyberspace is surprisingly fragile and often it could be compromised as a result of human error. The latter is almost impossible to avoid unless we fully implement artificial intelligence for cyber security at all levels and therefore, we need to begin focusing on building cyber resilience.

Open, democratic societies are much more vulnerable to attack as we offer unrestricted access to cyber and information space. For instance, government employees occupying specific network and system admin positions often take advantage of teleworking and this makes them an attractive target of social engineering attacks which can be a weak spot for National security. The most sensitive sectors are defense, foreign policy, and critical energy infrastructure. In the foreign affairs and defense context, unauthorized access to sensitive information residing on the MoD/MFA computers will compromise sensitive national and NATO/EU information. It will harm the national interest, the interests of our allies, and the collective defense. This otherwise effective health measure increases the opportunities for a state or non-state actor to exploit the information space by deploying fake news, videos, and false statements on the MFA/MoD website instead of the real news and sabotaging our foreign policy posture.

Another even more dangerous scenario would be an attack on our nuclear power plant. This type of attack can occur by using Stuxnet-like malware introduced to the nuclear power plant management system by an infected USB flash drive plugged into a computer in the internal network. If successful, such an attack would threaten our national security and the security of our neighbors. It may also undermine the thrust in nuclear energy in Europe and have economic ramifications.

NATO member states must adapt to the new environment where teleworking will likely become a new normal for government institutions. We need to strike the right balance between being a modern and mature digital society, and actively using cyberspace while safeguarding our national security and the security of our allies. To achieve a durable long-term solution our approach should be comprehensive and address the root causes of the problem.

Although raising cyber awareness of NATO employees and adopting best practices is a solid approach, it is not pursuing lasting results because it does not affect the adversary's motivation to engage in unauthorized use of cyberspace. Thus, a more durable, long-term solution would be to target the adversary's willingness to attack. We can significantly reduce the incentives for malicious exploitation of cyberspace by strengthening our cyber resilience and capacity to recover.

As it grows, cyberspace becomes a more accessible medium for asymmetric malicious attacks against government institutions and critical infrastructure. Thus, it becomes a breeding ground for new threats to allied cyber and information space. COVID 19 caused a boom in teleworking and many government employees started to work remotely from their homes. Although these measures remain efficient against the spread of viral infections, they have an adverse effect in cyberspace by creating opportunities for spreading computer viruses and aiding unauthorized access to government-owned networks. Therefore, teleworking of government employees on certain essential network admin and system administration positions constitutes a significant cyber threat to the security of NATO cyberspace. The most critical domains in this regard are defense, foreign policy, and the energy sector, in which a significant disruption of services could result in major and even catastrophic consequences.

The main methods of gaining unauthorized access to government networks include spear phishing campaigns, malware attacks, compromising systems through social engineering, or manipulation of legitimate user accounts. A cyber breach of our government networks would provide an opportunity for a rogue state or non-state actor to manipulate government websites or send fake messages or even fake videos.

In the defense sector, a civilian or military network/system administrator working from home could become a target of interest for the adversary's intelligence services. With creative social engineering, and the use of a password-cracking tool, for instance, BackTrack 5, any individual working for ill-intended actors may be able to pick up the administrator's credentials and obtain access to sensitive information residing on the government computers. This scenario constitutes a confidentiality breach and will compromise sensitive information – national and NATO/EU and will harm the national interest, the interest of our allies, and the collective defense.

By hacking into the Ministry of Foreign Affairs network, the adversary could compromise the data integrity by deploying fake news, videos, and false statements on the MFA website instead of the real news and sabotage our foreign policy posture. Even worse would be a scenario where the foreign state actor seeks to embroil one ally into a dispute or conflict with its neighbors, partners, and allies in the EU and NATO. They may take advantage of foundational narratives. By manipulating a foreign minister's statement published on the MFA website, and making unfavorable remarks about a neighbor or any other ally in NATO, an attacker could trigger a crisis and significantly harm our bilateral, regional, and even transatlantic relations.

The source of information is of utmost importance to appeal to a larger target audience. In this case, if the source is the Ministry of Defense (MoD) or Ministry of Foreign Affairs (MFA), the false information will be taken at face value. It will then be hard to explain to our citizens that what the institutions announced on their websites has been manipulated. In terms of data availability, the attacker could block any access to the MFA's website by launching a so-called Denial of Service (DoS) attack against the MFA webserver. This attack could use free software known as Low Orbit Ion Cannon (LOIC), which sends millions of requests to the server and renders the server overflown and inaccessible to other users. As the attacker had obtained all the network and system administration privileges, he could also access the server and delete the entire website.

Another even more dangerous scenario would be an attack on a nuclear power plant. The cyber-attack on Iranian nuclear facilities in 2010 was based on malware known as Stuxnet. This malware was so sophisticated that it was called by some authors a "digital ghost." It was reportedly delivered to Iran's nuclear facility via a thumb drive. The malware hijacks the information on the screen and displays that all parameters of the systems are within accepted normal parameters while unbeknown to the operators, it sends random commands to processes. This example demonstrates manipulation and misrepresentation of data which in terms of the CIA (Confidentiality, Integrity, and Availability) triad, constitutes a breach of **data integrity**. The attack demonstrated that even the most heavily protected, air-gapped Supervisory Control and Data Acquisition (SCADA) systems are vulnerable from the inside. An air gap is a security measure that isolates a digital device component or private local area network (LAN) from other devices and networks, including the public internet. An air gap is also known as an air wall and the strategy of using air gaps to protect critical data is also known as security by isolation.

Similarly, nowadays, more than a decade later, if an infected USB flash drive is plugged into a computer belonging to an ally’s nuclear power plant SCADA system, the Stuxnet scenario can happen with its nuclear power plant with a likely more advanced worm. It will jeopardize not only its national security but also the security of its neighbors. It also has the potential to undermine the thrust in nuclear energy in Europe and hurt the European economy. Similar intrusions are also likely to occur in other critical infrastructure sites such as the Metropolitan management systems and Oil refineries on territories of NATO member states.

Although it might seem very far-fetched, these scenarios are highly likely to occur. The threat is genuine as teleworking is currently gaining popularity. It expands the opportunities for unauthorized access to government cyberspace. The more government employees work from home, the more opportunities for malignant individuals or state actors to hack into employees' home networks and obtain their corporate credentials. The threat is complex because it exploits known cyberspace vulnerabilities to exploit cyberspace and the information environment and can have both tangible and intangible reputational damage. It will have internal economic and external political implications, affecting the economy and foreign policy posture.

An attack against a nuclear power plan would be the most dangerous one. The threat associated with it can be classified as critical since "modification or destruction of computers that control physical processes can lead to cascading effects (including collateral effects) in the physical domains." Unauthorized access to the MoD or MFA networks and exfiltration of sensitive national and NATO/EU information can be considered major threats to collective security. Not only does it jeopardize the collective defense of the alliance, but it also crosses over to the information space and degrades a NATO member-state foreign policy posture, undermining the cohesion of NATO and the EU and the transatlantic relations.

Recommended action and way ahead

NATO member states should strive to grow from basic information security and cyber hygiene to a modern mature society capable of withstanding cyber threats across all spheres of life. Therefore, our strategy should focus on investing in developing capacity in information and cyberspace. Our approach should be holistic and comprehensive. It should include hardening the cyber and informational aspects of national security posture while at the same time using strategic communications to counter misinformation.

NATO should seek to implement what is known as “zero trust” architecture in all networks and improve its layered security to ensure cyber resilience and business continuity at all levels. Zero trust is a security approach that assumes that all users, even internal users inside the network are malicious and must be verified.

We must adapt to the new digital environment where teleworking will likely become a new normal for government institutions. At the same time, we need to find the right balance between being a modern and mature digital society actively using cyberspace while safeguarding national security and the security of our allies.

Since the security is only as good as its weakest link, one approach is to address the weakest link in the security architecture - the human factor. To effectively prevent unauthorized access to our government networks, we need to raise cyber awareness of our employees by constant training and adoption of best practices. Our citizens should become aware of social engineering attempts and become more vigilant regarding phishing e-mails. Although this is a solid approach to hardening the security of our networks, the vulnerability will always be there.

A more sustainable, durable, and long-term solution is to invest in strengthening our cyber resilience and capability to recover at all levels. This strategic approach can be achieved by creating more redundancy in our infrastructure. We will affect the adversary's incentive to attack as they realize that their efforts would have no effect. This course of action would significantly reduce the motivations for unauthorized access to the cyber and information space against government institutions. It implies an increased financial burden but addresses the root causes of the problem – the adversary's willingness to attack. Therefore, the benefits will outweigh the potential losses.

The spectrum of cyber threats will continue to widen in the foreseeable future, and more and more government institutions will likely become victims of successful cyber-attacks. As Robert Mueller, FBI Director, 2012 puts it, "There are only two types of companies: those that have been hacked, and those that will be." Therefore, we need to harden our government networks' security at all levels by investing in human skills and more secure infrastructure as well as to adopt a more long-term approach by increasing our cyber resilience against these threats and becoming better prepared.

About the Author

Georgi Atanasov, staff officer in Bulgarian MoD.

He is a graduate of Varna Naval Academy, currently serving as a senior subject matter expert in strategic defense planning, Bulgarian MoD. Georgi is expert in effective use of cyberspace for strategic advantage and national security. Has a significant strategic-level experience in NATO and the EU defense related projects. He is Certified CCNA Security and holds a master degree from the College of information and cyber space, National Defense University in Washington, USA. Georgi can be reached online at LinkedIn: https://www.linkedin.com/in/georgi-atanasov-99329668

Post-Quantum Cryptography: Safeguarding the Digital Future and Bolstering Security in Critical Sectors

By Maila Zahra, Air University Islamabad and Zia Muhammad, North Dakota State University

Post-quantum cryptography aims to develop secure cryptographic algorithms to protect against most quantum attacks. The threats of quantum computers to the current cryptographic system will lead to the development of more secure algorithms schemes to ensure that the communication between channels remains secure and the ability to perform different efficient tasks. The key to sustainable cryptography is to adopt new algorithms that are powerful, resilient, and secure.

Security and Future of Post-Quantum Cryptography

There are a few noticeable questions that arise in our mind, particularly when we think of post-quantum future perspectives. What impact would post-quantum have on departments such as government, finance, and healthcare? How does it impact future security protocols, data protection, and privacy? How will it implement in real-world systems? What happens if a large number of post-quantum computers will use?

Post-quantum cryptography has a significant impact on these departmental elements like the government, as it does depend upon secure communication during the exchange of sensitive data over the channel. Implementing post-quantum cryptography will protect the potential attacks on critical infrastructure. Now a day's, in finance, crypto-currencies such as bitcoins are widely in use, and post-quantum assures the security of these digital currencies. Post-quantum will protect and secure patients' sensitive data, medical devices, and new research in medical fields.

How Post-Quantum Cryptography Works and Why It Matters

Quantum computing has been proven effective to breaks the classical cryptographic components because it can solve factoring problems and break complex algorithms. To defend us against such attacks, post-quantum cryptography came into existence. It utilizes complex mathematical frameworks to resist these quantum attacks and ensure the security of underlined algorithms. It ensures that sensitive information remains protected. Moreover, it strengthens the public and private keys, symmetric encryption, and all models that can be used to mitigate the risk of attacks. post-quantum cryptography has paramount importance, and its significance can not be denied.

In the current interconnected digital world, there is an uncontrolled reliance on technology and the need for online communication and data is key to security and privacy. Researchers are dedicating their efforts to building highly complex mathematical algorithms and key-sharing schemes that can sustain quantum attacks effectively. Build algorithms are tested against various attacks and scenarios to ensure the reliance on both classical and quantum cryptography, ultimately paving the way forward toward development and secure cryptographic solution.

Challenges and Limitations of Post-Quantum Cryptography

Despite the benefits and importance of post-quantum cryptography, there are also some drawbacks and difficulties that require further research and development. Some of the challenges include the complexities of keys, the overhead of key processing, and the underlined legacy infrastructure. These factors can affect the efficiency and performance of post-quantum cryptography, as well as its adoption and implementation in real-world systems.

One of the important aspects of post-quantum cryptography is the deployment in underlined legacy systems and making it compatible with existing protocols. These newly developed post-quantum cryptographic schemes and protocols need compatibility solutions with real-world systems and existing applications. There would be a need to focus on the choice of algorithms, the design of protocols, the evaluation of performance, and the verification of strength.

As with the development of every new technology, there are unintended consequences. For example, in terms of quantum computing, it is a new threat to underlined crypto infrastructure. But this is how we evolve, innovate and come up with more advanced novel solutions. This is how post-quantum cryptography was born to promote security and privacy in the presence of quantum computers. The post-quantum cryptography holds immense potential to safeguard the security of our digital future against any quantum threats. Therefore, there is a need to dedicate efforts to strengthen the current infrastructure with post-quantum cryptography.

About the Author

Maila Zahra is a student of cybersecurity at Air University, Islamabad, Pakistan. She also works for the National Science and Technology Park and actively participates in national-level hackathons. Her research interests include quantum computing, post-quantum cryptography, and various cutting-edge topics in the field of cybersecurity.

Zia Muhammad is a Ph.D. scholar at the Department of Computer Science, North Dakota State University (NDSU). He is a cybersecurity professional, academician, and researcher who has taken professional training and certifications. He has authored several publications in peer-reviewed conferences and journals in the field of cybersecurity. Zia can be reached online at (zia.muhammad@ndsu.edu, https://www.linkedin.com/in/zianoedar/).

With Americans Traveling More Than Ever Before, It’s Time Businesses Increase Their Mobile Security Efforts

If your colleagues are working from the road, follow these five steps to strengthen your mobile cybersecurity initiatives.

By George Tubin, Director of Product Strategy, Cynet

The U.S. travel market is booming. According to the U.S. Travel Association, air travel demand was up 12% in June compared to the same time last year. AAA reported this year’s Fourth of July weekend may have set new records, with 2.1 million more travelers compared to last year’s holiday. Paula Twidale, a senior vice president at AAA, said her organization had never projected travel numbers as high as they predicted for July 4, 2023.

Unfortunately, leisure travel and vacations often pose a serious problem for businesses of all sizes. With 91% of organizations saying mobile devices are critical to their operations, according to a 2022 Verizon report, most work-related emails now are opened on a mobile device.

These stats underscore the increasing need for organizations to prioritize mobile security measures. Employees across organizations, from the most junior-level staff to the C-suite, are conducting business via their mobile devices, checking work emails while sharing an Uber ride, charging company devices at public charging stations in airport terminals or hotel lobbies, or logging into work apps via unsecured Wi-Fi networks that often lack adequate protections.

Why Cybercriminals Target Mobile Devices

In light of these travel trends and employee behaviors, it's no surprise that 30% of zero-day exploits in 2021 targeted mobile phones and tablets—and that nearly half (46%) of small businesses reported a cybersecurity compromise involving a mobile device, according to Verizon's research.

Why do cyberattackers love mobile devices so much? To start, they provide much of the same access as traditional endpoints and often serve as an authentication tool, allowing cybercriminals to more easily infiltrate an entire network through an unsecured smartphone or tablet.

And it's not just travelers putting their business organizations at risk. The cloud data and applications that cybersecurity platforms protect are also left vulnerable if remote workers log into the same systems from an unsecured Wi-Fi connection.

Because hackers realize mobile devices are less likely to be protected, they have shifted their focus to smartphones and tablets as a preferred entry point when orchestrating an attack. Cybercriminals view mobile device vulnerabilities as the low-hanging fruit of cybercrime. Email phishing scams that play out over someone's smartphone, zero-day mobile exploits, and other malicious mobile applications are all becoming more sophisticated. And while traditional mobile device management (MDM) solutions offer protection for managed devices, most fail to detect threats across all endpoints, mobile devices, networks, and cloud environments.

As cybercriminals get more savvy and develop new tools to compromise mobile devices and networks, security leaders must take extra steps and implement additional layers of protection to safeguard their systems.

5 Steps Security Leaders Can Take Now to Protect Mobile Devices

1. Keep mobile devices secure: Regularly update company devices with the latest software patches and security updates. Implement a focused mobile device security app across all employee and contractor devices to protect against mobile device, network, phishing and app attacks before damage can be done. IT and security teams should continuously monitor their organization's mobile devices to ensure the most current applications and security measures are deployed.

2. Prioritize cybersecurity training to boost employee awareness: For smaller businesses that have employees who are more likely to use personal devices for work, it can be difficult to maintain visibility into their mobile usage habits or safeguard endpoints from attacks. That is why employee education on the latest mobile cybersecurity threats are so important. All employees should be instructed on best practices, such as using strong passwords, employing two-factor authentication, and being on alert to report any suspicious emails, texts or other suspect activity so that it doesn't spiral into a full-on cyberattack.

3. Make career training a top priority for you and your team: Educating employees outside of the IT and security department is important, but it's just as important that security professionals stay up to date on the latest cybersecurity threats and attacks, especially when it comes to mobile security. Cybercriminals are rapidly advancing their capabilities and sharing what they know with fellow hackers in underground forums. It's insufficient to simply monitor your business' network and systems, even with advanced security technology. Expert cybersecurity professionals and CISOs must also keep abreast of emerging threats, follow recommended mitigations from industry analysts and national agencies, and even monitor the dark web to preempt cyberattackers' ever-evolving exploitation efforts.

4. Monitor network traffic: At large enterprises, most security teams already monitor their organization's network traffic. But small- and mid-size businesses may lack the personnel to actively analyze all network activity. That's why it's vital to automate detection and response efforts with a security solution that includes mobile protection capabilities. An automated detection and response system that can integrate into your existing cybersecurity tools enables you to have complete visibility and monitor any threat alerts in real-time.

5. Develop and practice a solid Incident Response Plan: Your company's Incident Response Plan is among any security team's most important pieces of documentation. It should serve as a playbook for any cybersecurity threat or attack, defining in detail the actions everyone on your team — as well as the business at large — should take if the corporate network is breached. If employees are conducting business on mobile devices, the plan should outline response protocol for mobile-specific attacks. An Incident Response Plan not only ensures you and your team are prepared, it provides a roadmap to investigate how the attack happened, contain and remediate the threat, and avoid future attacks. It's important to review and rehearse your Incident Response Strategy on a quarterly, or even monthly, basis, so that, should you have to use it, the information is updated and aligns with your most recent security policies and protocols. You can also take advantage of battle-tested templates to customize an effective template for your organization's unique needs.

The future of cybersecurity is centered on a business' ability to protect mobile devices.

Last year, McKinsey reported a 15% increase in cybercrime costs, with 85% of small and midsize enterprises looking to increase security spending in 2023. The research firm listed the increase in "on-demand access to ubiquitous data and information platforms" as the top cybersecurity trend with large-scale implications.

"Mobile platforms, remote work, and other shifts increasingly hinge on high-speed access to ubiquitous and large data sets, exacerbating the likelihood of a breach," according to the report, "Companies are not only gathering more data but also centralizing them, storing them on the cloud, and granting access to an array of people and organizations, including third parties such as suppliers."

Mobile cybersecurity is more crucial now than ever before. To empower employee productivity while staying one step ahead of cybercriminals, businesses need security solutions that enable complete visibility and protection across all endpoints, mobile devices, networks, and cloud environments. By adding an extra-layer of protection to your cybersecurity stack, you gain peace of mind knowing your workforce's mobile devices are protected — in the office, the beach, or wherever your employees may roam.

About the Author

George Tubin is Director of Product Strategy at Cynet and a recognized expert in cybercrime prevention and digital banking and payments security. He was previously Vice President of Marketing at Socure and Senior Research Director with the leading financial services research firm TowerGroup (acquired by Gartner, Inc.) where he delivered thought leadership and insights to leading financial services institutions, technology providers, and consultancies on business strategies, technologies, cybersecurity and Identity and fraud management.

George can be reached online at (https://twitter.com/georgetubin) and at our company website https://www.cynet.com/.

Earthquakes, Cyber Breaches, and Mitigating Disasters through Design

By Archie Agarwal, Founder and CEO of ThreatModeler

The Great Earthquake of San Francisco in 1906 caused unbelievable levels of damage in the city, with over 28,000 buildings destroyed and 500 city blocks reduced to rubble. The event basically wiped large swaths of the city off the map, yet the rebuilding process saw the city continue to prioritize financial considerations over earthquake proofing. This reluctance to acknowledge the likelihood of future earthquakes further exacerbated the damage when the next big earthquake struck in 1989. Although the damage and death toll were less than in 1906, the buildings that were rebuilt with unreinforced masonry and without earthquakes in mind suffered the most harm. This time, San Francisco learned its lesson. The city strengthened its seismic code and made changes that would apply both to structures already standing and new construction.

Similar to the aftermath of the Great Earthquake of San Francisco, cybersecurity is currently undergoing a transformation. With the increasing frequency and sophistication of cyberattacks, organizations must take a proactive approach to stay ahead of the evolving threat landscape.

A Different Kind of Disaster

In the rapidly evolving landscape of cybersecurity, organizations face an escalating array of threats that can jeopardize their valuable assets, sensitive information, and overall reputation. Despite this, many application design teams prioritize functionality and speed of development over security. As a result, security considerations are often treated as an afterthought. This can lead to vulnerabilities that attackers can exploit.

These vulnerabilities can come in many forms, including insecure data storage and transmission and poorly designed third-party integrations. For data storage and transmission, weak encryption practices, inadequate access controls, or using insecure protocols (e.g., HTTP instead of HTTPS) can compromise data confidentiality and integrity. Further, modern applications often integrate with third-party services or APIs that are not thoroughly vetted or securely implemented, which can introduce vulnerabilities, expose sensitive data, and provide an entry point for attackers.

To effectively safeguard against these risks, a comprehensive and proactive cybersecurity strategy is essential.

Secure by Design

When designing buildings in San Francisco today, architects and structural engineers rely on computer-aided design (CAD) and other specialized software to ensure their buildings are structurally sound and able to withstand seismic events. By assessing the structural integrity of buildings and identifying potential weak points before construction, engineers can design reinforcements and implement preventative measures to mitigate risks.

Much as an architect cannot earthquake-proof their building once an earthquake is in progress, it is not enough to be reactive to security threats. Organizations must prioritize security during the design process itself to ensure comprehensive protection. By embracing the secure-by-design approach cybersecurity organizations can lay the foundation for secure, resilient systems that can withstand the challenges posed by malicious actors.

A ‘CAD’ Solution for Cybersecurity

Threat modeling is to cybersecurity what CAD is to building design and earthquake-proofing. Threat modeling emphasizes a secure-by-design approach that identifies security concerns at the initial stages of development to create robust and resilient systems. By providing visibility into an environment's attack surface, threat modeling enables organizations to proactively identify, assess, and mitigate potential security risks.

Threat modeling embodies the same proactive stance against vulnerabilities that architects employ. By identifying potential threats and weaknesses within their systems during the design phase and prioritizing them based on severity and likelihood, organizations can implement the necessary countermeasures to fortify their defenses. This significantly enhances an organization’s cybersecurity posture, reducing the likelihood of successful attacks and minimizing the potential damage they can inflict.

By implementing threat modeling as an ongoing process, organizations are able to prioritize their mitigation strategy and identify the right controls that can be implemented to prevent a disaster. It is no longer a luxury but a critical element of a strong cybersecurity strategy.

Preventing the Great Cyber Breach of 2024

In an era where cyber threats are constantly evolving, relying solely on reactive security measures is inadequate. The imperative for proactive risk assessment and mitigation has never been greater.

Much like CAD drawings provide a blueprint for earthquake-resistant structures, threat modeling in cybersecurity offers a framework for making informed security decisions. By embracing threat modeling and integrating it into their cybersecurity strategy, organizations can bolster their security posture, safeguard valuable assets and information, and protect their reputation. Threat modeling empowers organizations to stay one step ahead, making it a critical element of any comprehensive cybersecurity strategy. Through these secure by design approaches, both seismic preparedness and cybersecurity can continue to anticipate and mitigate risks effectively.

About the Author

Archie Agarwal, Founder and CEO of ThreatModeler. Archie Agarwal is the Founder and CEO of ThreatModeler. Archie has over 20 years of experience in risk and threat analysis. Previously, at WhiteHat Security, as director of education and thought leader he specialized in threat modeling, security training and strategic development. He has also held positions at PayCycle (acquired by Intuit), Citi, HSBC and Cisco. Archie is a Certified Information Systems Security Professional (CISSP) and is SANS GWEB certified. Archie can be reached online through LinkedIn and at our company website https://threatmodeler.com/

Safeguarding Healthcare: A Closer Look at the Major Trends in the Health IT Security Market

The health IT security market is experiencing remarkable growth, driven by the pressing need for robust solutions that protect patient privacy, secure data integrity, and ensure the uninterrupted delivery of critical healthcare services.

By Saloni Walimbe, Assistant Manager-Content, Global Market Insights Inc.

As the healthcare industry continues to embrace digitization and the adoption of advanced technologies, the importance of Health Information Technology (Health IT) security has become paramount. The digitization of sensitive patient data, electronic health records (EHRs), and the interconnectedness of healthcare systems expose the industry to a myriad of cybersecurity threats.

The healthcare sector is a prime target for cybercriminals due to its vast amounts of sensitive patient data and potential financial gains. The incidence of cyber-attacks targeting US hospitals and health systems increased by over two-fold between 2016 and 2021, as per reports from the Journal of the American Medical Association. Ransomware attacks, data breaches, and identity theft are just a few of the concerning threats facing healthcare organizations.

For instance, between February 26 and March 7, 2023, Managed Care of North America (MCNA) experienced a significant breach of healthcare data. During this period, malicious code infiltrated their systems. Subsequent inquiry uncovered that an unauthorized entity had penetrated specific systems and extracted copies of personal data. This attack impacted roughly 8.9 million individuals, including patients, parents, guardians, and guarantors. Incidents such as these have highlighted the urgent need for robust healthcare cybersecurity solutions.

Governments around the world have also tightened regulations concerning patient data protection and privacy. HIPAA (Health Insurance Portability and Accountability Act) in the United States and GDPR (General Data Protection Regulation) in the European Union are two examples of stringent compliance frameworks that healthcare organizations are required to adhere to. Such policies will create a favorable growth environment for the health IT market, which is poised to exhibit over 18.2% CAGR through 2023-2032, according to a research report from Global Market Insights Inc.

3 Key Players Pioneering Change in the Healthcare IT Security Industry

In response to the growing demand for robust healthcare IT security, numerous companies have emerged as major players in the market. These organizations offer innovative solutions designed to address the industry's unique security challenges. Enlisted below are 3 key players and their contributions to health IT security industry development:

GE Healthcare – Skeye Cybersecurity Service

With the proliferation of interconnected devices, the potential for cybersecurity risks grows, and these security incidents can have a profound impact on an organization's efficiency, financial stability, quality of healthcare, and reputation. GE Healthcare is committed to mitigating these risks by furnishing customers with a comprehensive evaluation of the security of their medical devices. This assessment aids in the identification of vulnerabilities, offers recommended action plans, provides guidance for remediation, and outlines strategies for execution. This process promotes collaborative efforts involving customers' clinical engineering, IT, and security teams.

In February 2020, in Chicago, GE Healthcare unveiled a novel service designed to assist hospital groups in their battle against cybersecurity threats. The innovative solution, named Skeye, was designed to harness the expertise of medical device specialists, artificial intelligence, and process management tools. By leveraging a remote security operations center (SOC), Skeye could enhance hospitals' existing capabilities and resources, enabling proactive monitoring and empowering them to swiftly detect, analyze, and respond to cybersecurity threats and incidents in real-time.

Imprivata – Digital Identity Maturity Model & Assessment for Healthcare IT Security

Given the immense value of sensitive patient records and the potentially life-threatening consequences for patient care, healthcare organizations have become prime targets for malicious actors. Many healthcare delivery organizations (HDOs) have identified a lack of thorough assessment of cybersecurity risks as the most significant obstacle to establishing a robust security stance.

Imprivata is dedicated to transforming this landscape by assisting organizations in prioritizing strategies that revolve around securing the user's digital identity and credentials, moving away from the conventional emphasis on network perimeters.

In April 2023, Imprivata introduced the Imprivata Digital Identity Maturity Model and Digital Identity Maturity Assessment. These pioneering tools are designed to elevate the input of clinicians and end-users in shaping the decision-making process concerning a healthcare organization's digital identity strategy. Integrating the clinician's perspective into a digital identity strategy assessment will result in more valuable, efficient, and successful implementations. This, in turn, enhances the collaboration between clinicians and IT teams, ultimately leading to improved outcomes.

Palo Alto Networks – Medical IoT Security

Digital devices are extensively utilized in the healthcare sector, particularly for diagnostics and monitoring, encompassing equipment in ambulances and surgical robots. However, research from Unit 42, Palo Alto Networks' division specializing in threat intelligence and consulting, reveals that nearly 98% of all medical IoT device traffic lacks encryption. Furthermore, 57% of IoT devices face susceptibility to medium or high-severity attacks. This concerning data underscores the allure of security device targeting for cyber attackers, potentially jeopardizing patient data and ultimately putting patient well-being at risk.

In response, Palo Alto Networks announced enhanced features and capabilities in December 2022, tailored to safeguard medical Internet-of-Things (IoT) devices from cyber threats. This initiative takes the form of "Medical IoT Security," a comprehensive Zero Trust security solution specifically designed for the digital healthcare landscape.

Palo Alto Networks' novel Medical IoT Security solution harnesses the power of machine learning to facilitate swift and secure deployment and management of emerging connected technologies within organizations. This solution integrates with existing healthcare information management systems such as AIMS and Epic Systems, streamlining workflows through automation. Users can devise device rules equipped with automated security responses, enabling functions like anomaly monitoring and triggering appropriate countermeasures.

The health IT security market is witnessing remarkable growth, fueled by escalating cybersecurity threats, regulatory compliance pressures, and advancements in healthcare technologies. Key players in the market are delivering innovative solutions to address these challenges, ranging from comprehensive network security to enhanced identity and access management. As the industry continues to evolve, future trends such as AI-driven threat detection and cloud security will play pivotal roles in shaping the future of the healthcare cybersecurity landscape.

About the Author

Saloni Walimbe. An avid reader since childhood, Saloni Walimbe is currently following her passion for content creation by penning down insightful articles relating to global industry trends, business news and market research. With an MBA-Marketing qualification under her belt, she has spent two years as a content writer in the advertising field, before making a switch to the market research domain. Aside from her professional work, she is an ardent animal lover and enjoys movies, music, and books in her spare time.

E-mail Compromise

How to protect business against BEC-attacks

By Sergio Bertoni, The senior analyst at SearchInform

Attacks via email is one of the most beloved cybercriminals' method for compromise of organization's data.

Only during the 2022 the number of Business Email Compromise (BEC) attacks doubled, according to the Computerweekly. What's more, according to the IBM Cost of Data Breach Report 2022, business email compromise and phishing attacks turned out to be the most expensive breaches, resulting in $4.89mln and $4.91mln respectively. According to Research and Markets, the global BEC market is expected to grow from an estimated value of USD 1.1 billion in 2022 to USD 2.8 billion by 2027, at a Compound Annual Growth Rate (CAGR) of 19.4% from 2022 to 2027.

The senior analyst at SearchInform, Sergio Bertoni reveals, why BEC attacks are so popular and how to protect against them.

Cybercriminals' aims and implications for businesses.

A BEC attack is a social engineering attack that is aimed at compromise of a corporate mailbox. Before the attack implementation, intruders gather information about the victim and the company the person works for. It isn't difficult for a cybercriminal to obtain and use the data gathered against the victim and his/her colleagues, since many employees openly publish information about themselves in blogs and on social networks; for instance, they reveal, where do they work and what is their position in the company, where are they going on a vacation, etc. However, data on organization's executives, such as email addresses and business trip dates is even more preferable for intruders. Malicious actors are also extremely interested in details on company's payments and accounts. If intruders have access to such data, it's much easier for them to deceive, for example, a chief accountant and persuade the employee to transfer money to a fake account.

In order to implement an attack an intruder can hack an organization or its contractor's email. After reading the correspondence - simulate the continuation of the correspondence, using the information obtained for their own malicious purposes. But cybercriminals do not always send emails via hacked email, they can register a phishing domain that looks like the original one and continue correspondence via this email. For instance, they can create a mailbox with the @serchincom.com domain instead of @searchincom.com domain. This method of spoofing is called typesquatting, when malicious actors use the company's domain name with an erroneous spelling.

In 2019, with the help of this technique malicious actors managed to steal $1 mln from the Chinese venture fund, which planned investments into the Israeli start-up. Cybercriminals intercepted the correspondence between two companies and sent messages to the fund representatives on behalf of start-up employees and vice versa. In order to implement the attack, intruders used fake domains, which differed from the original ones only by one letter, which was added to the end of the domain name.

Popularity of this type of attacks may be explained with the simplicity and quickness of its implementation. According to the recent survey by Microsoft Security Intelligence, the whole process, starting from the first log to the deleting of the sent message can be performed within 2 hours. It should be mentioned, that intruders manage to gain significant financial benefits or achieve other aims, for instance, obtain access to the infrastructure or confidential data.

Recently, intruders started to implement BEC-attacks in order to steal physical assets (for instance, goods). A *sugar supplier was nearly affected by such an attack. The intruder asked in correspondence to send a truck on the certain address on credit. However, the employee of the sugar supplier company notices that a mistake: an extra letter was added to the sender's email address. The employee got in touch with the representative of the company, on behalf of which the letter was sent, to make sure that the email sender really was the staff member of the company. However, the reply was negative. Thanks to the employee's attentiveness, the cyber criminal didn't manage to steal the product.*

It's crucial to attentively check the sender's email address. What's more, forged emails often contain few mistakes. In case an email is a suspicious one, it's useful to get in touch with a representative of a company, on behalf of which the email was sent and make sure, that their employee really sent the email. But make sure to connect with the representative via legitimate and verified channel, not by replying to the suspicious email. For instance, you can make a call to the head office and find out, whether the email sender really works for the company and if he/she sent the letter.

How else a BEC-attack may look like

In fact, email services aren't the only tool, which intruders use to perform attacks. Not so long ago cybercriminals began using video conference software, for instance, ZOOM, in order to make employees send money or share some confidential information. In such case, intruders usually use deepfake technologies to commit fraud.

For instance, an intruder hacks an executive's email and sends employees an invitation to join a videoconference. During the call the intruder fakes the video and types a message in the chat that there are some problems with the connection or that he/she has problems with the microphone. Then, the intruder adds that he/she wants employees to make a money transfer and explains, where money should be sent to.

Most often, such incidents are detected in the USA, however, it's quite probable that with the further development of the technologies, used for deepfake creation develop and their price decrease, intruders in other countries may also start to actively use such technologies for their malicious aims.

It's possible to prevent BEC-attack. In order to successfully cope with the task, it's required to be acknowledged about the information security rules and stick to the recommendations by information security experts.

Building protection against corporate email compromise

Intruders implement social engineering techniques to perform BEC-attacks and it's important to ensure complex protection against them. One the one hand it's crucial to enhance employees' information security and general computer literacy, on the other hand it's required to implement specific protective solutions and develop specific regulations for staff members which will help to enhance of corporate protection.

Enhancing employees' competencies in information security related issues is a crucial aspect in terms of enhancing corporate safety. If an employee isn't acknowledged about the existing risks, he/she won't recognize a phishing letter at the first attempt, what will result into large financial losses for an organization. However, there is much organizations' employees in charge can do themselves in terms of employees education in information security related issues. For instance:

- Reveal, what are phishing and BEC attacks
- How to distinguish fake email from a real one
- Occasionally imitate attacks, for instance phishing attacks (to check, whether employees understood the theory and are aware of security recommendations).

If your organization lacks experts and resources for developing a training program, there is an option of contracting third party experts. For instance, our company experts have been conducting cyber literacy training for employees of various companies and state institutions for three years yet.

What's more, it may be a useful option to share a few memos with employees. The memos help to mitigate risks, associated with a number of threats (phishing emails, use of unreliable passwords, installation of programs, etc.)

The second step is to deploy tools for protection of email services. Such software ensures protection against external threats, for instance, NGFW helps to block potentially malicious network traffic, antispam software reduces amount of phishing emails, SPF, DKIM and DMARC protocols help to verify whether email senders are legitimate.

Some solutions for mitigation of internal threats can also help to deal with the task. For instance, some time ago we also added the functionality, which detects cases when the domain and the sender's real address differ to our DLP solution.

What's more, it's helpful to develop specific regulations, which will govern how employees should behave in various situation, including potentially dangerous ones.

There is a step change taking place in the amount of BEC attacks. According to ComputerWeekly, the volume of Business Email Compromise (BEC) attacks doubled during the course of 2022. This means, that companies have to ensure advanced protection and thus reduce risks and outcomes of corporate email compromise.

About the Author

Sergio Bertoni, the Leading Analyst at SearchInform which is the global risk management tools developer. Sergio has plenty of hands-on experience in the sphere of information security and has been contributing to the company's success for years. Sergio comments on different infosec topics, including information security trends and new methods of fraud (from simple phishing to deepfakes), provides advice on how to ensure security of communication channels and shares best practices for organizing information security protection of businesses. Sergio can be reached at the company website https://searchinform.com/.

From Network Perimeters to Cloud Access Security Brokers to APIs: The Evolution of DLP Strategies

By Sudeep Padiyar, Senior Director, Product Management at Traceable AI

When Data Loss Prevention (DLP) was conceived as a security concept in the early 2000s, it was largely focused on network perimeters, with efforts towards protecting data in motion across network boundaries. Fast-forward to the present day where the network perimeter has blurred with most applications being deployed in the public cloud and the sensitive data that they access are scattered in several data stores across public and private data centers. In this new landscape, APIs have emerged as the pivotal link for data transfer and business operations, becoming a primary target for hackers. As a result, modern DLP strategies are experiencing a seismic shift, with a renewed emphasis on securing APIs.

Historically, DLP initiatives focused on protecting data traversing these boundaries via web, email, and file transfers. However, the advent of digital transformation, fueled by cloud computing, a mobile workforce, and APIs being the backbone for business, creates a sprawling, decentralized network where sensitive data is frequently in transit, and is accessed from virtually anywhere. This change has dramatically amplified the potential avenues for data loss and breaches resulting in DLP at the API layer being as relevant as Cloud Access Security Brokers (CASB) for SAAS and Data Security Posture Management for IAAS.

Enter APIs: the Invisible Workhorses of the Digital Age

APIs are the bridges enabling software applications to interact, share data, and execute business functions. According to the 2022 Postman State of the API report, organizations are now utilizing an average of 218 APIs – a testament to their increasing pervasiveness and the critical role they play in how applications are consumed. Browsers, mobile apps and API platforms like Postman are now the three most common ways by which modern applications are accessed.

But with this proliferation comes a new set of risks. APIs have become a prime target for hackers due to the vast amount of sensitive data they handle and strong need for authentication and authorization, with several high-profile data breaches in recent years being traced back to API vulnerabilities being exploited by attackers.

This surge in API-related breaches is a clear indicator that API security is no longer an afterthought but a primary requirement in DLP strategies, for several reasons:

1. API-centric data breaches: APIs often expose sensitive data in the payload, many times without the right authentication and authorization controls, making them attractive targets for cybercriminals. Their vulnerability to breaches necessitates robust API security measures. Broken Object Level Authorization (BOLA) and Broken Function Level Authorization (BFLA) being top attack vectors in OWASP API top 10 2023 as well

2. Growth in API development and usage: APIs are becoming increasingly ubiquitous. According to the 2022 Postman State of the API report, organizations have an average of 218 APIs, representing a significant increase from previous years. For example, Netflix reportedly receives billions of API calls every day, underscoring how central APIs have become to their operations. Gartner also chimed in on the growth of APIs, stating 94% of organizations use or are planning to use public APIs provided by third parties; up from 52% in 2019; 90% of organizations use or are planning to use private APIs provided by partners; up from 68% in 2019; and 80% organizations provide or are planning to provide publicly exposed APIs; up from 46% in 2019. With this increased reliance comes a higher number of potential points of failure, making API security a growing priority for most CSO's.

3. APIs have become the universal attack vector: What makes APIs so interesting from a hacker's perspective is that they expand the attack surface across all vectors. They now present the largest attack surface we have ever encountered in the industry. In the past, hackers had to find ways of bypassing existing solutions, such as WAFs, DLP, API Gateways, etc., in order to find data and disrupt systems. Now, they can simply exploit an API, obtain unfettered access to sensitive data, and not even have to exploit the other solutions in the security stack. Hence the

API layer has to be the universal defense layer to prevent attacks and utilize the additional detection logic to do so effectively.

4. Regulatory compliance: Data protection regulations like GDPR, CCPA, and HIPAA have strict rules on data handling. In October of 2022, we also witnessed the FFIEC make updates to its cybersecurity guidelines – and the update included API security. Ensuring API security is a significant step towards regulatory compliance and avoiding hefty fines.

5. Evolution of cyber threats: The cyber threat landscape is rapidly evolving, and bad actors are using increasingly sophisticated methods to exploit vulnerabilities. Credential stuffing, for instance, where attackers automate login requests using stolen credentials, can lead to unauthorized access to APIs. And according to Gartner, last year in 2022, API abuse became the most frequent attack vector for data breaches. Furthermore, they also predict that by next year, 2024, API abuse attacks will double. Account takeover, Bot based attacks and Online Fraud are also being increasingly carried out via API's. The relentless advancement of such threats necessitates a dedicated focus on API security.

As we navigate the new age of data security, securing APIs is more critical than ever. Organizations must prioritize API security in their DLP strategies, not only to guard against data breaches and meet regulatory compliance but also to fortify their defense against the ever-evolving threats posed by cybercrime.

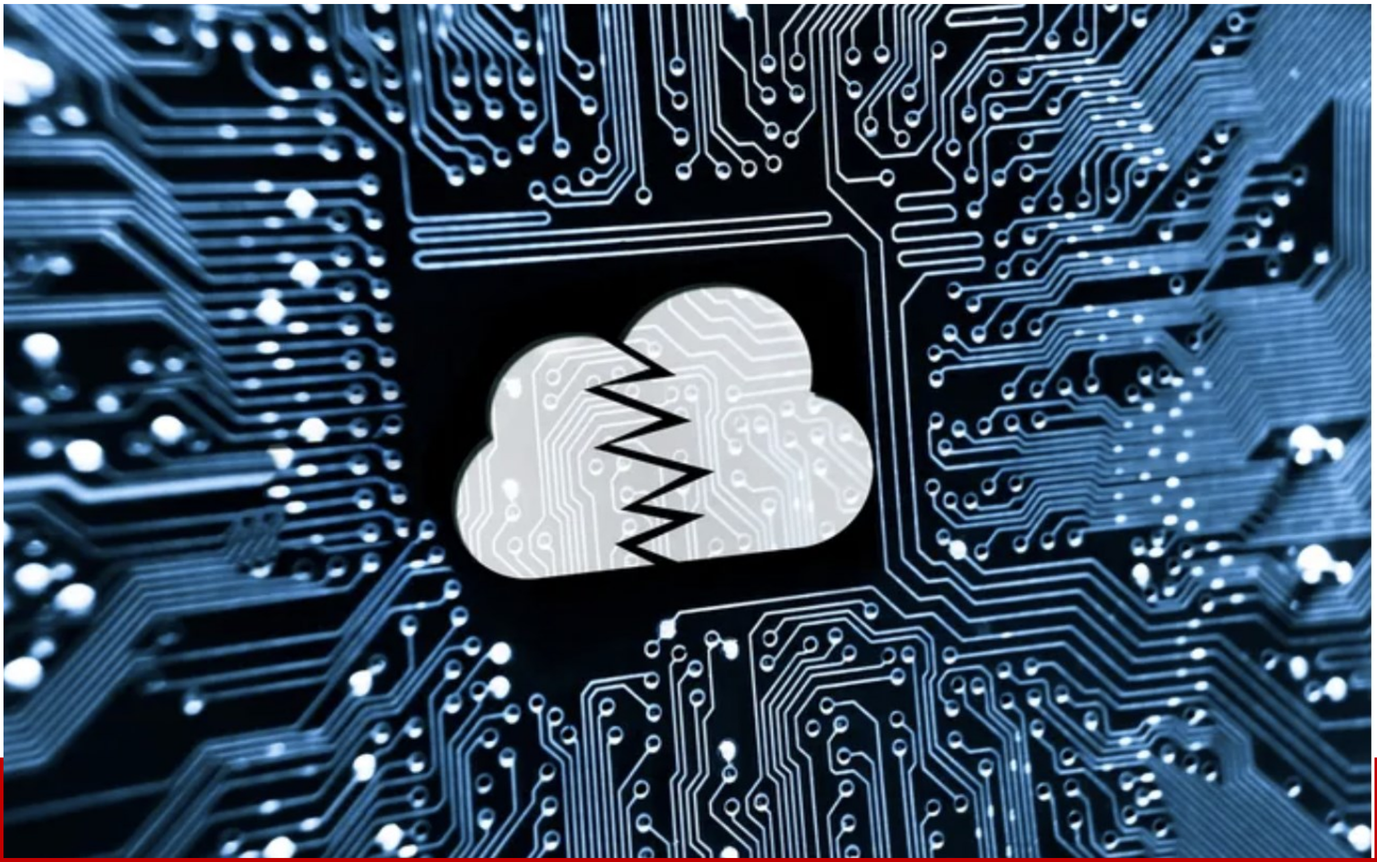
With APIs becoming the gatekeepers of valuable data, our DLP strategies must pivot towards securing these critical links, transforming our approach to data security in this interconnected digital age.

About the Author

By Sudeep Padiyar, Senior Director, Product Management at Traceable AI

Sudeep Padiyar is very passionate about cloud native security and feels the technology we are building at Traceable AI will be the foundation for DevSecOps, API Security and Observability for years to come. Prior to joining Traceable he was at Palo Alto Networks where he started CN-Series - the industry's first Kubernetes next gen firewall, lead automation initiatives for cloud security and managed cloud network security products. He started his career as an engineer at Cisco building core routers and switched to Product Management for Data Center switching after his MBA from Santa Clara University.

When he is not thinking about technology he likes to coach his kids' soccer team, play tennis and go for hikes in the SF bay area. He is into teas and likes to brew everything from Masala chai to loose leaf Jasmine tea. He lives in Sunnyvale with his wife and two kids. Sudeep can be reached online at https://www.linkedin.com/in/sudeep-padiyar and our company website https://traceable.ai.



How to Avoid Common Security Incidents in the Public Cloud

By Jhilam Biswas, Customer Engineering Manager, Google Cloud

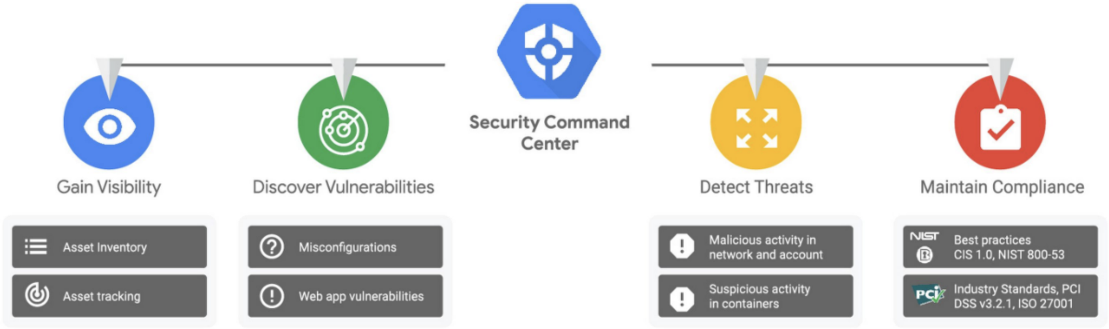
The growth of cloud computing is undeniable. According to Garter's report, the global spending on public cloud services was around $490.3 billion in 2022, and this number is projected to grow by 20.7% in 2023 to reach $591.8 billion. What propels this phenomenal growth are a number of reasons, a few notable ones being accelerating digital transformation and faster time to market, increasing demand for hybrid and multi-cloud deployments, leveraging the pay-as-you-go model of the cloud.

As cloud computing grows, so does the need for cloud security. Cloud environments are complex and often have a large attack surface, making them attractive targets for cyber attackers. In fact, a recent study by Verizon found that more than 80% of enterprise breaches involved threats initiated by external sources and 50% of all social engineering attacks are pretexting incidents—nearly double of last year's total.

Given the importance of cloud security in the age of cyberattacks, in this article, we'll cover some critical methodologies used in Google Cloud to prevent the most commonly seen security incidents in the cloud.

Although the solutions mentioned here are unique to Google Cloud, you can find similar services in other public cloud providers that provide similar functionality.

1. Prevent public exposure of your API credentials, encryption keys and secrets: Developers often unknowingly share API credentials, encryption keys and secrets in their codebase that resides in a code hosting platform such as GitHub or Google Cloud's Artifact Registry. This might sound like a common practice usually done for the sake of "quick accessibility". In the long run though, when the code gets pushed into production with the credentials/keys in the code itself, it might pose a huge risk. If a hacker gets access to those credentials that's publicly available in your code-base, they potentially hold the power to gain unprivileged access to your organization's proprietary data and can cause irreversible damage. Some mechanisms to prevent this is by using extremely granular IAM policies not only for identities but also on the resource itself. For example, in Google Cloud, you can use Organization Policy Constraints to limit who can create service account keys.
2. Prevent user accounts compromise: Password spray and brute force attacks are the most common ways to steal identities and use that access for malicious purposes. As enterprises, you can adopt a couple of solutions to prevent such threats. For example, you can use 2FA / U2F solutions and make its requirement a mandate in your organization. You can also use a tool like "Password Alert" that prevents re-use of passwords that are being used by users in your organization to be used elsewhere on the internet. Consider also using tools such as Google's Password Manager that helps you manage passwords all at one place and identify your passwords that were exposed in a third-party data breach.
3. Monitor virtual machines for cryptojacking: Cryptojacking is a type of malware attack that uses a victim's virtual machine resources to mine cryptocurrency. This can have a significant impact such as data breaches, an unwarranted massive cloud bill or other security incidents that can negatively affect your organization. Cloud-based cryptojacking is on the rise and occurs when an attacker gains access to a victim's cloud computing account and uses it to mine cryptocurrency. This type of attack is more scalable and anonymous, making it more difficult to detect and prevent. Google Cloud's native built-in solutions in the Security Command Center such as the "Virtual Machine Threat Detection" and "Event Threat Detection" can help identify such threats in the cloud. These are critical threats due to the aforementioned reasons and so having that instant visibility can help organizations immediately fix such issues whenever they get identified.



Source: https://cloud.google.com/security-command-center

4. Prevent misconfigurations of cloud storage buckets: If you are starting a new project and need a durable object-storage solution to store, manage and retrieve files, cloud storage is probably one of the widely used native cloud services that organizations use. However, cloud storage buckets are often misconfigured in a way that your buckets get exposed to the internet unknowingly. In order to prevent such misconfigurations, you can use services such as Organizational Constraints for Cloud Storage in Google Cloud to enforce constraints such as public access prevention and object retention policies. You can also use Security Command Center's Storage Vulnerability Findings to proactively detect misconfigurations in storage buckets.
5. Audit your users' Cloud IAM Entitlement Lifecycle to improve security posture: Just about every org has an outlook.com / yahoo.com / gmail.com account somewhere in their IAM structure. These user accounts could potentially be malicious with privileged permissions and pose a threat to misuse your cloud resources. A manual audit of personal accounts/users can be difficult to track in your cloud IAM hierarchy. To help organizations with the detection of such accounts, you can use Google Cloud's Organizational Policies to limit domains with IAM grants. In Google Cloud, you can also use Security Command Center's Event Threat Detection to search IAM for external grants.

Cloud is a complex environment to manage and security in the cloud is even a tougher problem to solve for. However by taking advantage of the approaches called out above, you can shield your organization from the most common threats seen in cloud environments.

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/

IT Modernization Efforts Need to Prioritize Cybersecurity

By Mark Marron, CEO and President, ePlus, Inc.

Organizations are increasingly advancing their digital transformation efforts to deliver internal efficiencies, reduce costs, and improve customer experiences.

As a side-effect of doing this, many have become more reliant on third-party solutions like cloud providers, IoT, process automation, robotics, AI-powered cybersecurity threat detection tools, and more. With every new technology or new vendor that you introduce into your business, you also introduce enhanced risk as your attack surface grows.

Cyber criminals are like chameleons, always changing their skin to elude detection. The rise of generative artificial intelligence (AI) is a welcome addition to their toolkits, offering them new attack vectors to exploit, and even new ways to launch their attacks. For companies of all sizes, the need to double down on cybersecurity has never been greater.

A recent Gartner study forecasts that global IT spending will exceed $4.6 trillion dollars in 2023. Yet, the same survey notes that IT security is projected to make up less than 6% of IT budgets.

Investing in a robust, well-orchestrated and coordinated cyber security plan is a competitive advantage that can provide valuable returns to your business. Keeping your organization, its people and its data safe is top of mind for every CEO.

These are a few of the ways I think about securing the business that protect you but also provide you with a competitive advantage.

Improve Vendor Risk Management

The introduction of AI-powered automation technologies, interconnected systems, and a growing hybrid workforce have all helped to maintain and improve productivity, but they have also created new vulnerabilities and increased the potential attack surface for cyber threats. As companies increase their dependence on third-party products and services, they must have a strong vendor risk management program and/or a strategic partner that can expertly assess and manage the potential benefits and risks. Key components of an effective vendor risk management program include:

- Having an accurate inventory and onboarding of third-party suppliers. Know who you are using and exactly what vendors and technology are at work across your organization. This includes the identification of key contacts, websites, and support portals.
- Running table-top exercises with real-life scenarios to test your procedures and ensure you have a timely and appropriate response.
- Looking at methods of automation and integration with other key systems to ensure that third-party risk data is updated, accurate, and shared as appropriate.

Train Your Workforce to Be Your First Line of Defense

One of the main security challenges that AI poses for companies is its effectiveness at creating far more sophisticated and intricate versions of common cyber threats – including email phishing, malware, ransomware, or social engineering. While malicious attacks may come from disgruntled current/former employees or partners, many incidences occur because well-meaning employees are not well trained on the best cybersecurity practices. As a result, they are more likely to fall victim to these common cybersecurity threats.

An April 2023 survey conducted by Darktrace, Generative AI: Impact on Email Cyber Attacks, highlights the challenges employees and companies are facing from increased cyber threats.

More than 30 % of the 6700 employees polled from companies in the UK, United States, France, Germany, Australia, and the Netherlands admitted that they have previously fallen victim to a fraudulent email, and more than 70% said they noticed an increase in scam emails and texts over the previous six months.

Furthermore, the study noted that there was a 135% increase in novel social engineering attack emails in the first two months of 2023, figures that coincide with the rise in adoption of popular generative AI tools.

Companies need to prioritize cybersecurity training for employees at all levels. Training must be consistent and frequent, so employees are familiar with the latest threats that they may encounter and the protocols that they must follow when they identify and report potential threats.

Ensure Compliance with Increasingly Stringent Data Privacy Regulations

There is now more than 25 years of data circulating on the internet. Think about the first time you used the internet to sign up for a social media account, an email address, a subscription, joined a club, or made a purchase online; that information is still living somewhere. Now, imagine all the times you have done these activities since then. That is a lot of personal data floating around, potentially available to be shared with companies and bad actors alike in an increasingly digitally connected global landscape. Not surprisingly, data privacy regulations and protections are on a rapid rise, driven by concerns over data breaches and privacy.

For companies, non-compliance can be costly and have a substantial impact on your brand's reputation. In the last few weeks alone, several high-profile industry-leading organizations suffered multi-million-dollar data breaches or received heavy fines for privacy violations. Industries like finance and healthcare are imposing stricter regulations and compliance standards related to data privacy and security.

Also, many countries and multiple US states are implementing stricter data privacy regulations. The most well-known regulations in place today include: the very comprehensive European Union (EU) General Data Protection Regulation (GDPR), which came into effect in 2018; the California Consumer Privacy Act, enacted in Jan. 2020; and the Brazilian General Data Protection Law, enacted in September 2020. Other countries like Australia, Japan, and India, are in the process of updating their own data protection regulations.

Invest in Cybersecurity as a Competitive Advantage

Demonstrating and supporting a strong cybersecurity posture will differentiate an organization from its competitors, attract new opportunities, and build a reputation as a trusted and reliable entity in the market. Simply put, as companies advance their digital transformation efforts, cybersecurity needs to be an even greater priority.

Today's increasingly complex nature of cybersecurity threats, interconnected systems, shared infrastructure, and growing data protection privacy laws all necessitate the involvement of multiple key stakeholders – including customers, partners, and employees. With constant diligence and prioritization around cybersecurity, you are empowering your organization to not only adapt, but evolve, in the face of new frontiers in data protection.

Mark Marron is the CEO and President of ePlus inc., a leading global IT solutions provider headquartered in Herndon, VA. A 30-year technology industry veteran, Mark was named CEO of ePlus in August 2016. During his tenure, he has overseen ePlus' significant revenue growth and geographic expansion. Mark has been recognized with multiple Best Workplace honors - including Best CEOs for Women (according to female employees, 2020) and Best CEO (Large Companies, 2019 & 2020).

About the Author

Mark Marron, the CEO and President of ePlus, Inc. Mark can be reached online at LinkedIn and at our company website www.eplus.com

It's Not Me, It's You: Your Biggest Cybersecurity Risks Are Your Partners

By Craig Burland, CISO, Inversion6

You've been laser focused on driving cybersecurity risk out of your organization and made great progress. Kudos, well done. But when the threats and alerts don't stop coming, it's time to consider that it's not just about you. It's about them too.

In our digital, interconnected world, strong cybersecurity practices have become the linchpin holding together the integrity and safety of modern businesses—equally as important as the international supply chain or global monetary agreements. Just as financial markets ebb and flow based on intricate economic ties, so too does the world of cybersecurity, affecting the multifaceted relationships businesses build with one another. Your organization is akin to a single link in a mammoth chain that spans sectors, borders and platforms. A weak link anywhere could compromise the integrity everywhere. The unsettling reality is that, often, your cybersecurity fortress is only as impenetrable as that of your least-protected partner. So, while you might be diligent, what about your partners?

Let's look at three recent examples:

- The Log4j Vulnerability (2021): The discovery of the Log4j vulnerability spotlighted the vulnerabilities lurking within the open-source software supply chain. Log4j, a logging library integrated into a myriad of applications, had a critical flaw that allowed malicious actors to remotely execute arbitrary code. The ubiquity of this library meant that its vulnerability exposed countless systems worldwide, highlighting how a single weak link in the software supply chain can put a vast network of enterprises at risk. The incident served as a wakeup call for organizations to reevaluate and strengthen their software supply chain security.
- SolarWinds Hack (2020): An alarming testament to the chain-link vulnerability was the SolarWinds breach. A seemingly minor weakness in the software update chain of a widely used IT management tool became a conduit for a massive cyber espionage campaign. This breach affected multiple high-profile entities, including U.S. federal agencies and Fortune 500 companies, demonstrating how a single compromised link can endanger many.
- Capital One Data Breach (2019): In this incident, a former Amazon Web Services (AWS) employee exploited a misconfigured firewall in Capital One's operations, resulting in the exposure of data of over 100 million customers. While Capital One was the primary victim, the incident raised eyebrows about the shared responsibilities and inherent risks of using third-party cloud service providers.
- Target Breach (2013): Target's systems were infiltrated through an indirect attack on their network -- an HVAC vendor. This third-party vendor had less stringent security measures, making them an easier target. Once breached, the cybercriminals navigated into Target's more extensive network, eventually accessing millions of customers' credit card details.

Each of these incidents has become a critical milestone in the collective understanding of 3rd party risk. Target highlighted the connection between Non-IT service providers and the IT environment. SolarWinds demonstrated an inherited infiltration, cascading risk from one entity to another. Capital One cast doubt on our understanding of the shared responsibility model. Log4j opened our eyes to the double-edged sword of open-source software.

Lessons from these three events can form the foundation of a solid strategy to mitigate the risk of a supply chain compromise.

1. Thorough and Recurring Vetting: Begin partnerships with a comprehensive cybersecurity assessment. Before integrating any third-party service, software, or tool into your organization, ensure that it meets the highest cybersecurity standards. Commit to reviewing those assessments on an annual basis to ensure your partners remain vigilant.
2. Manage Your Asset Inventory: Catalog and track all third-party software components in your environment, especially those that are open source. Understand their usage, dependencies, and potential vulnerabilities. Prioritize the use of well-vetted, reputable software components. When a threat does materialize being able to mitigate it quickly and surgically is vital.
3. Continuous Monitoring and Communication: Establish real-time monitoring of all interactions between your environment and your partners' environments. This includes email, data transfers, software updates, and any other digital touchpoints. Regularly communicate with partners about shared cybersecurity threats and best practices.

4. Understanding the Power of Knowledge: While advanced software and cutting-edge hardware play their part, the heart of cybersecurity lies in the informed actions and decisions of individuals. The reason is simple: a vast majority of cyber breaches occur due to human oversight or misinformation. By ensuring that every individual is educated about the potential risks and best practices, organizations can significantly minimize these vulnerabilities.
5. Contractual Obligations and Maintenance: Include robust cybersecurity clauses in all contracts with partners. This ensures that they maintain strict security standards, and it delineates clear responsibilities and actions in case of a breach. Insist on maintenance agreements that include security updates covering the useful life of the arrangement.

As your company matures its own cybersecurity, it's critical to recognize and ensure your partners do the same. From workforce vetting to secure development, what your partners do (or don't do) significantly affects your overall risk. As the saying goes, "A chain is only as strong as its weakest link". So, in your next budget cycle, instead of layering on one more security tool, invest in pulling on that chain. Assess, monitor, and educate judiciously. Your cybersecurity, reputation, and ultimately, your business depends on it.

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.

Learning Lessons from The Recent MOVEit Hack

Jack Viljoen, Head of Prodinity Cyber Solutions, provides a cyber safety 101 to avoid vendor-related cyber-attacks.

By Jack Viljoen, Prodinity Cyber Solutions

The recent surge in large-scale vendor-related cyber-attacks has exposed critical vulnerabilities in organisations' cyber security practices. Several prominent companies, including the BBC, British Airways, and Boots, fell victim to the breach of their MOVEit file transfer systems, highlighting the pervasive threats faced by businesses, irrespective of their size.

Such attacks can be extremely damaging in a number of ways, including reputation management, business interruption, and the knock-on financial implications - but they do provide valuable lessons for the industry. Lessons we must learn.

The MOVEit hack serves as a stark reminder of the persistent threats faced by both large corporations and small to medium-sized enterprises (SMEs) in the realm of cyber security. The attack, driven by poor cyber security practices related to vendor access vetting and monitoring to company systems, has highlighted the critical need for heightened security measures across organisations to safeguard sensitive data.

Hackers took advantage of a vulnerability in MOVEit Transfer, a commonly used software tool for secure data transfers. This resulted in the risk of valuable employee information being stolen, including sensitive data like national insurance numbers and bank details. The widespread nature of the hack, affecting multiple organisations simultaneously, is causing concern among payroll providers globally.

Preventative action

The important thing to note here, is that this hack could have been avoided. The MOVEit attack exploited vulnerabilities that should have been addressed through robust cyber security protocols. It is imperative to highlight the weaknesses that allowed such an attack to occur, emphasising the importance of proactively fortifying systems against cyber threats.

First and foremost, insufficient employee awareness and training played a significant role in this breach. Cyber criminals often exploit human error and lack of knowledge to gain unauthorised access. Comprehensive training programmes are essential to educate employees about phishing attempts, malware risks, and the significance of safeguarding sensitive information. Simulated phishing exercises can help employees recognise and avoid phishing attempts, reducing the risk of successful attacks. Furthermore, fostering a culture of cyber security awareness within the organisation encourages employees to report suspicious activities promptly, enabling faster incident response.

A lack of regular security assessments and updates contributed to the vulnerability. Neglecting regular security assessments and updates leaves organisations vulnerable to exploits, so frequent vulnerability assessments are key to help identify weaknesses in systems that hackers can target. Penetration testing and vulnerability scanning should be conducted regularly to assess the organisation's security posture comprehensively.

Patch management, too, is a critical aspect of cyber security. Organisations must prioritise timely application of security patches to address known vulnerabilities in their systems. Automated patch management tools can streamline the process and ensure all systems are up-to-date. Additionally, companies should establish a clear process for handling urgent patches to minimise exposure to potential threats.

How strong is your password?

In addition, weak password practices served as another entry point for attackers. Reusing passwords, employing weak or easily guessable passwords, or failing to enforce multi-factor authentication significantly increase the risk of unauthorised access. Organisations must emphasise the importance of strong password policies, encourage the use of password managers, and implement multi-factor authentication across their systems.

Password management tools can help employees generate and store complex passwords securely. Implementing single sign-on (SSO) solutions can also reduce the burden of managing multiple passwords while enhancing security. Regular password change policies, combined with educating employees on the importance of password hygiene, can further strengthen the organisation's defence against password-related attacks.

Insufficient network segmentation and access controls also contributed to the successful attack on these organisations through the vendor route. By failing to separate critical systems and limit access privileges based on the principle of least privilege, companies inadvertently create avenues for lateral movement within their networks. A compromised account in one department can easily result in widespread access across the entire network, making it easier for cybercriminals to exfiltrate sensitive data.

Vendor-related cyber attacks can be particularly dangerous because they bring the challenge of supply chain vulnerability into sharp focus. Vendors often have privileged access to critical systems or sensitive data of the companies they work with. If a vendor is compromised, attackers can exploit this access to infiltrate the target organisation’s network, bypassing traditional security controls.

Cascading attacks

Since many organisations rely on multiple vendors for various services, products, or software components, this means the impact of a successful attack can span multiple countries and multiple territories. A successful attack on a vendor can have a cascading effect, leading to widespread damage and disruption.

Companies often have limited control over their vendors’ security practices and infrastructure. Even if an organisation has robust security measures in place, a vendor’s weak security posture can undermine the overall defence and become a point of entry for attackers.

Additional risk assessments should also be considered when dealing with vendors, particularly when it comes to the exchange of sensitive information.

At the very least, companies should perform thorough risk assessments to evaluate the security practices of potential vendors before entering into business relationships. This assessment should include evaluating their security controls, incident response plans, and overall security maturity.

This incident does present an opportunity for knowledge sharing and collaboration. By working together, the companies affected by the MOVEit attack can help to establish channels for sharing threat intelligence and security information with vendors. Together, we can collaborate on proactive measures to identify and mitigate emerging threats.

Can we trust our software?

The reliance of companies on the MOVEit file transfer system to exchange highly sensitive information amplifies the significance of the recent hack and the security patch issue. Organisations placed their trust in MOVEit as a secure solution for their data transfers, making the breach in its security infrastructure particularly alarming. The fact that the loophole went unnoticed due to a security patch issue raises concerns about the effectiveness of their security practices and the thoroughness of their assessments.

When companies entrust a third-party vendor with their sensitive data, they are entitled to expect a higher level of security and protection. The occurrence of a hack within a trusted system like MOVEit raises questions about the reliability of vendor systems and their diligence in detecting vulnerabilities.

Organisations should engage in rigorous vendor assessments before implementing third-party software solutions. Evaluating the vendor's security history, conducting penetration testing of the software, and reviewing third-party security certifications can provide insights into the vendor's commitment to cyber security. Establishing clear security requirements in vendor contracts and conducting regular security reviews can help maintain a high standard of cyber security across all vendor relationships.

The time to act is now

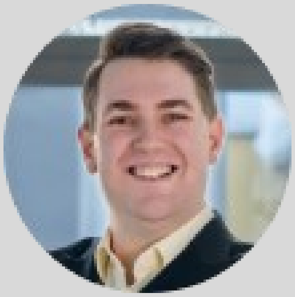
This unfortunate incident also underscores the need for organisations, regardless of their size, to prioritise cyber security. Investing in advanced threat detection and prevention technologies, employing regular employee training programmes, implementing robust access controls, and conducting regular security audits are vital steps to defend against evolving cyber threats.

The recent wave of vendor-related cyber-attacks serves as a wakeup call for organisations to fortify their cyber security measures. Through comprehensive and frequent security assessments, and stronger access controls, businesses can bolster their resilience against cyber threats. Collaborating with vendors and actively engaging in risk assessments can enhance the overall security posture. By assuming greater ownership of their cyber security, organisations can protect sensitive data, preserve customer trust, and ensure a safer digital future. The collaboration between businesses and cyber security experts is crucial in combating the growing menace of cyber-attacks and securing the digital landscape for all.

About the Author

Jack Viljoen is Head of Prodinity Cyber Solutions.

Jack can be reached via email, on LinkedIn, and at our company website: www.prodinity.com



Navigating the Uncertainties of CMMC 2.0: An Urgent Call for Clarity

Unpacking the Complexities, Implications, and Future Outlook of the Cybersecurity Maturity Model Certification

By David Brewer, Director of IT/Cybersecurity (Acting), Saalex Solutions, a division of Saalex Corporation

In the hyperconnected landscape of the digital age, where the onslaught of cybersecurity threats is relentless, robust defense mechanisms are crucial. The Department of Defense (DoD) has taken a leap in this direction with the Cybersecurity Maturity Model Certification (CMMC). Yet, with the introduction of CMMC 2.0, a cloud of uncertainties looms, especially concerning the Level 3 requirements. These uncertainties breed discord within the industry, posing significant threats to prime contracts and the overall integrity of the nation's supply chain.

The Challenge of Ambiguity and its Broad Impact

When looking at the ambiguity surrounding the CMMC Level 3 requirements, the issue extends far beyond inconveniencing contractors; it permeates the entire ecosystem within which these businesses operate. Vital infrastructure and sensitive data find themselves in potentially precarious positions due to the absence of clear guidelines.

In the cyber world, where threats are perpetually evolving, ambiguity can be a catastrophic recipe. Contractors require certainty to safeguard themselves and their partners effectively, ensuring robust protection of vital national interests. The present scenario, wherein the details of the requirements remain nebulous, does not allow for such effective security measures to be put in place.

Moreover, the confusion not only causes an operational hindrance but also stokes the flames of anxiety among industry players. The lack of clarity can result in potentially avoidable mistakes, furthering the risk exposure of the entire supply chain.

A Race Against Time Amidst Unclear Directives

The vacuum of precise information or guidelines concerning the Level 3 requirements has precipitated a frantic race against time among contractors. With a summer deadline for Level 3 announced, businesses find themselves in a maelstrom as they grapple with the lack of specifics.

Adding to this complexity, the National Institute of Standards and Technology (NIST) has released a draft revision to the SP 800-171. Revision 3's industry comment session ended on the 15th of July and is looking to have the revision ratified in late 2024 or early 2025. This not only affects the CMMC standard, as Levels 1 and 2 are solely based on the NIST SP 800-171 standard, but also increases the number of controls from 110 to 138, introducing new Organizational-defined Parameters (ODP). The Rev 3 standard's introduction of ODP allows for a company to define cost and effort based on their size and budget, somewhat alleviating stress for smaller companies without the budget for high-dollar security infrastructure.

This scenario sets up an alarming situation where businesses are preparing for a certification process that might span anywhere from several months to an entire year. Without definitive guidance, businesses are forced to speculate, leading to increased stress levels and potential oversights that could have severe repercussions. Furthermore, the changes to the SP 800-171 standard present additional challenges, as businesses must now adapt to new controls and guidelines.

Such frantic preparation also eats into valuable resources, both human and financial. The inherent uncertainties can lead to companies allocating more resources than necessary, leading to inefficiencies that strain the entire process. The looming changes to the SP 800-171 standard further compound these issues, making the race against time even more critical.

The Ripple Effects: Concerns over Auditors and Industry Implications

The impact of the delays and uncertainties extends far beyond the immediate circle of the contractor community. It causes ripples throughout the cybersecurity industry. There is growing concern about the readiness of CMMC auditors and the quality of training they receive. With the forthcoming new requirements, there is apprehension regarding the auditor's preparedness and the effectiveness of their assessments.

Moreover, in the face of the upcoming new requirements, there's concern over the time and costs associated with maintaining compliance. Companies find themselves in a tight spot, balancing the need to safeguard prime contracts while also managing the financial strain of adhering to the new requirements.

This situation, combined with the uncertainty surrounding the future, could potentially compromise national security. The risk of slowing down the certification process might disrupt the nation's supply chain, leaving it vulnerable to cybersecurity threats.

A Glimmer of Hope Amidst Uncertainty

Despite the prevailing uncertainties, recent developments offer a glimmer of hope. The submission of the proposed CMMC framework to the Office of Management and Budget (OMB) for review is one such silver lining. This step officially kick-starts the final rulemaking process, a crucial milestone indicating progress is being made towards defining and implementing CMMC 2.0.

However, the sense of anticipation that comes with this development is tempered by the fact that the review process can take up to 90 days or longer. And despite the final rule's submission, the final shape it will take remains uncertain, keeping the industry on tenterhooks.

The Waiting Game and Potential Outcomes

Even with this step towards finalizing the CMMC rules, a substantial degree of uncertainty lingers. The review period could go on for months, and the final outcome remains in the realm of the unknown. However, the fact that a consensus on a final rule has been reached and that the framework has been submitted for review suggests that the formal introduction of the latest version of CMMC is on the horizon.

The next steps could see the rule published in the Federal Register under one of two classifications. If published as a proposed rule, it could take a significant amount of time to get to the finish line, potentially taking the better part of a year. However, if the office agrees to publish CMMC as an interim final rule, the rule could take effect over the following 60 days, allowing the CMMC to hit DoD contracts soon after.

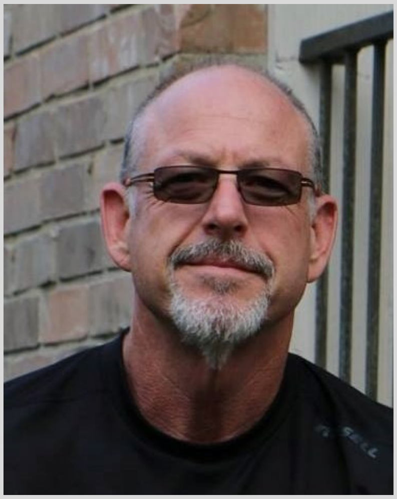
Implications for the Future: An Urgent Need for Clarity

Despite these advancements, the intricate details of the program remain a mystery, casting a long shadow of uncertainty over contractors who handle the Pentagon’s sensitive information. As the industry navigates this ever-evolving landscape of cybersecurity, the ongoing discussion surrounding CMMC 2.0 underscores the critical need for clear, consistent guidelines.

Given the gravity of the situation, there is an urgency for all parties involved – from contractors and auditors to the DoD – to unite in their efforts. By working together, they can navigate these uncertainties, overcome the hurdles, and ensure the integrity of national security. The future success of CMMC 2.0, and thus the fortification of our cybersecurity defenses, depends on the clarity of guidelines, effective communication, and the collective will to navigate this challenging landscape. This collective effort is needed to ensure that the process is as smooth as possible, and the disruptions caused by these uncertainties are minimized.

Indeed, the road to CMMC 2.0 is fraught with challenges. Yet, by focusing on fostering understanding, unity, and clarity, the industry can overcome these hurdles and fortify our nation's cybersecurity framework. This journey is not merely about achieving certification; it's about shaping the future of cybersecurity in our nation's defense apparatus, ensuring the integrity of our supply chain, and preserving our national security.

About the Author



Dave Brewer is an accomplished information technology professional with over 20 years of experience in IT and cyber security. He currently serves as the Program Manager and acting Director of IT/Cyber Security at Saalex Solutions. Previously, he held positions as Network, VoIP/VTC, Hardware Operations Manager at Peraton and Director of Operations at Hoyt Communications Inc. Dave is pursuing a degree in Information Technology - Security at Western Governors University and boasts an extensive array of certifications, including CompTIA Network Plus, Security Plus, ITIL Foundation, BICSI RCDD, and various CCNA and CCNP certifications. With a recent Cisco Certified Specialist in Data Center Core, Dave's expertise in both management and technical roles has solidified his status as an industry leader. His unwavering commitment to professional development reflects his dedication to staying at the forefront of technological innovation.

David can be reached online at david.brewer@saalex.com and at Saalex’s website https://www.saalex.com/.

New Phishing Attacks Use .ZIP to Target Brands

By Eric George, Director of Solutions Engineering, Fortra

Researchers at Fortra have observed cybercriminals abusing New Top-Level Domain .zip in two separate phishing campaigns targeting a large social media conglomerate and global technology company. These are the first attacks identified by PhishLabs that use Google Registry's recently released.zip TLD.

TLDs resembling common file extensions are capable of shrouding the distinctions between a legitimate domain and a scam. As of July 2023, the IANA database represents 1,591 top-level domains (TLDs), including the eight announced by Google on May 3: .zip, .dad, .phd, .prof, .esq, .foo, and .mov. The risks associated with new TLDs .zip and .mov have specifically been a source of controversy, with .zip already emerging in large scale campaigns (referenced below).

TLDs can be used or abused in any number of ways as threat actors register and manipulate URLs to serve their own malicious purposes. Humans are liable to mistake the URL for a legitimate file, while browsers may associate and autolink a .zip file with the same name to an actor-owned website, unknowingly leading the user to a malicious destination.

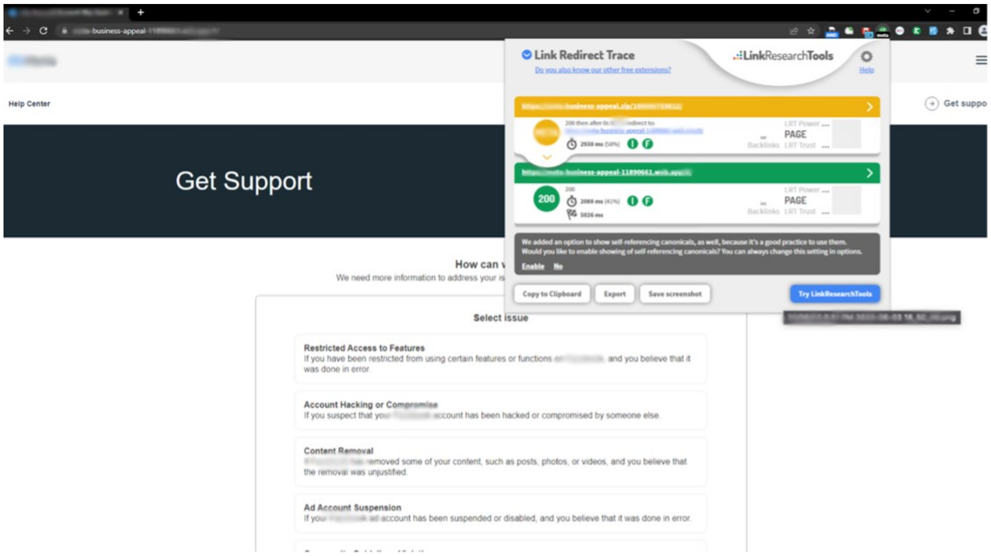
TLDs can also be used in context with the remainder of a URL to convince a victim they are clicking on a link associated with a financial institution, retail organization, or any other host of legitimate websites. New Generic TLDs (gTLDs) that use familiar terms are often registered by cybercriminals to mislead victims with lookalike domain attacks. A lookalike domain is dynamic, and can be used to target a brand with Business Email Compromise scams, credential phishing sites, social media posts or advertisements, and more.

.ZIP Attack Example 1

In the attack below, the cybercriminal registered a .zip lookalike domain redirecting from a large social media organization to a third-party, actor-owned website. In addition to using the .zip TLD, the domain uses HTTPS, the organization's brand name, and the language "business-appeal" to convince the victim of its legitimacy.

Domain: hxxps://xxx.business-appeal.zip/

ISP: NameCheap



We added an option to show self-referencing canonicals, as well, because it's a good practice to use them. Would you like to enable showing of self-referencing canonicals? You can always change this setting in options.

We need more information to address your is

Restricted Access to Features
If you have been restricted from using certain features or functions [redacted] and you believe that it was done in error.

Account Hacking or Compromise
If you suspect that your [redacted] account has been hacked or compromised by someone else.

Content Removal
[redacted] removed some of your content, such as posts, photos, or videos, and you believe that the removal was unjustified.

Ad Account Suspension
If your [redacted] account has been suspended or disabled, and you believe that it was done in error.

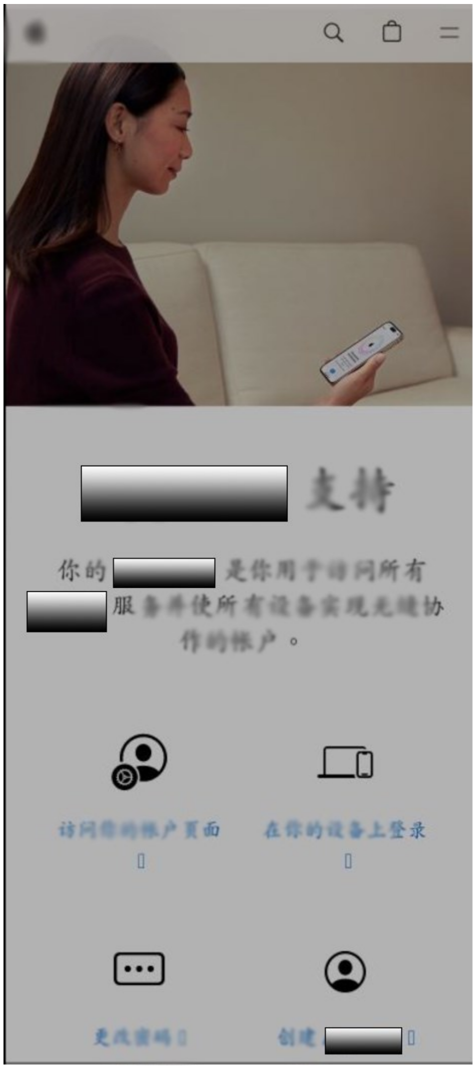
.ZIP Attack Example 2

In the second campaign, the cybercriminal used a .zip lookalike domain to send the victim to a credential theft phishing site. In addition to using .zip, the domain includes language associated with a known application available through the targeted brand. The cybercriminal also registered an SSL certificate for the domain in an effort to further enhance the appearance of legitimacy.

The phishing page itself also uses images, language, and branding associated with the targeted organization.

Domain: hxxps://xx29xzy.zip

ISP: BGPNet Global



[redacted] 支持

你的[redacted]是你用于访问所有[redacted]服务并使所有设备实现无缝协作的帐户。

访问你的帐户页面 ▯

在你的设备上登录 ▯

更改密码 ▯

创建[redacted] ▯

In addition to detection of .zip campaigns, PhishLabs has observed a shift in TLD usage in Q2, with newcomers using familiar terms used more.

Some examples of TLDs with common terms include:

- .info
- .click
- .app
- .shop
- .vip
- .work
- .online

TLDs .app and .shop specifically have shown significant increases in volume in Q2, with .app moving from the 19th most abused spot to the sixth. TLD .shop was the tenth most abused, previously occupying the #36 spot.

Additionally, gTLD .online has been heavily abused so far in 2023, representing the #13 most abused TLD in Q1 and #15 in Q2.

The increased use of these TLDs may indicate a shift in cybercriminal behavior to incorporate more common terms into lookalike domain attacks beyond the root domain.

It is important that security teams are familiar with terms and variations associated with their brands and consistently monitor for activity that may target their organization. PhishLabs will continue to provide updates on TLD threats as they evolve.

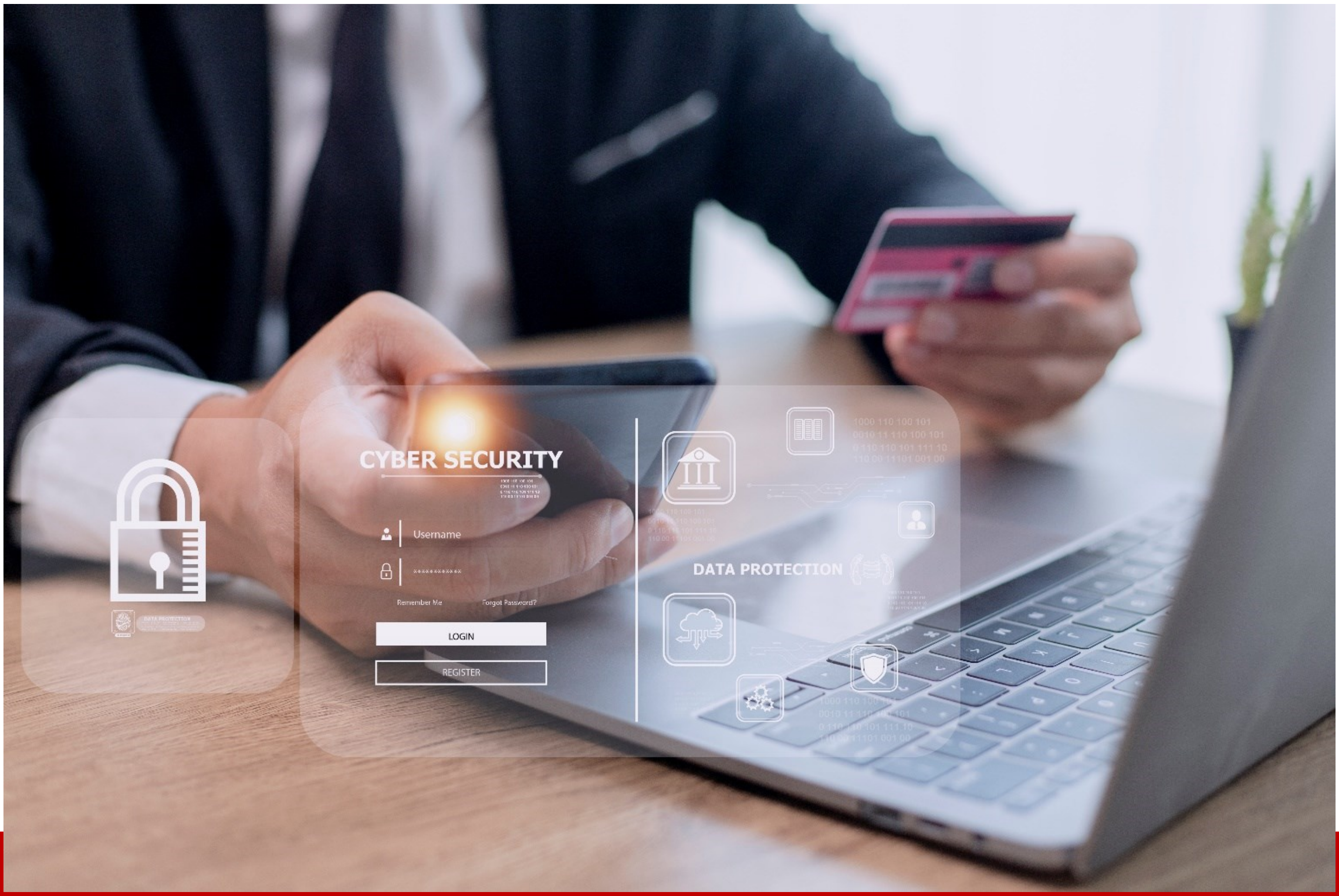
About the Author

Eric George is the Director of Solutions Engineering at Fortra. Eric began his career at Fortra's PhishLabs as an analyst in its Security Operations Center. He then advanced to multiple lead roles and built considerable security knowledge while specializing in the detection, analysis, and mitigation of account takeover attacks for enterprises from multiple industries.

Eric then transitioned to Solutions Engineer, supporting sales and business development efforts before taking on his current role where he leads Solution Engineering, Targeted Intel, and Technical Client Support efforts. PhishLabs was acquired by Fortra in October 2021.

In addition to his work at PhishLabs, Eric has held over 10 industry certifications including CISSP and serves as a Technical Malware Co-Chair for the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG).

Eric can be reached on LinkedIn, Twitter, and our company website https://www.fortra.com.



Safeguard Business Transactions with Online Payment Security Tips

By Zac Amos, Features Editor, ReHack

Secure online payments have become an integral part of the shopping experience. More people are using e-commerce than ever before, and business owners must ensure transactions are secure. There are many ways to make them safer without compromising the customer experience. Here are eight online payment security methods every company should implement.

1. Educate Staff About Online Payment Security

Many data breaches happen by mistake. One study found that negligent contractors or employees caused 63% of cybersecurity incidents in a year. That's why business owners must teach workers about strong online payment security practices.

Employees should refrain from sharing customer payment info with unauthorized people. They should also avoid clicking unfamiliar email links and leaving work computers unattended.

2. Don’t Store Payment Data

Holding onto customer data may be convenient for future transactions, but businesses that do this have more to lose during a security breach. Some of the riskiest information to store includes users’ payment information. One of the safest online payment security methods is to discard this information after a transaction.

However, sometimes a business needs to store sensitive user data. In that case, the best action is to keep it on an external server, like in the cloud. Cloud-based billing systems can protect customer information if hackers breach a company’s website.

Plus, using a third-party transaction partner removes some of the burden of responsibility from a business. That company will be responsible for safeguarding the data and paying any fines if it mishandles it.

3. Accept Only Secure Online Payments

Business owners can improve their online security by taking only secure forms of payment. The safest ones include:

- **Credit cards:** The money comes from a credit card company, and payment compliance standards regulate their use.
- **Debit cards:** Like credit cards, debit cards are subject to strict payment compliance standards.
- **Electronic checks:** The processing Automated Clearing House system verifies each transaction, and account numbers are confidential.
- **Digital wallets:** They are encrypted and require user authorization for each payment.

Business owners looking to boost their online safety profile should avoid accepting cryptocurrency. In 2021, Americans lost an estimated $680 million in crypto investment scams, and there is no way to communicate with customer support to resolve payment issues.

Phone transactions — in which a customer completes a payment over the phone, usually by talking to a representative — are also less secure. Hackers can intercept these calls. Additionally, confirming that someone is actually paying the intended merchant and not a scammer can be hard.

4. Turn on Multifactor Authentication (MFA)

MFA adds an extra layer of security to a website. It requires users to enter a temporary pin and their password to log in or make a payment. The code typically comes through in a text message or email.

Even if hackers steal a user's login credentials, they still have to access their phone or email account to get the one-time login code, which is much harder.

5. Verify Transactions

Another vital online payment security method is to verify all transactions. Since a customer's credit or debit card is not physically present, business owners must use other ways to confirm the payment, such as:

- Requiring shoppers to enter their card's CVV number or security code
- Allowing personal verification — such as a driver's license — for large purchases
- Using security software to flag unusual transactions, such as very large orders or several purchases in rapid succession
- Looking for an address verification match

6. Stay Updated

One of the best online payment security methods is to keep software current. Software updates often include patches or bug fixes that address loopholes. Most e-commerce sites and antivirus software update automatically, but it's still wise for business owners to check for updates periodically. Up-to-date networks are much harder for threat actors to access.

7. Use a Secure Sockets Layer (SSL) Certificate

The padlock symbol beside a site's URL signifies it's encrypted with an SSL certificate. It makes website visitors feel safer and secures the data between browsers and servers so hackers cannot intercept it, letting customers make online payments without worrying about prying eyes. Virtually all reputable sites use an SSL certificate for added security.

8. Purchase Cyber Insurance

Businesses can fall prey to hackers or unintentional data breaches even with strong safeguards in place. Cyber insurance helps close the gap by covering various costs associated with a security incident, including notifying customers, recovering lost income, retrieving stolen data and repairing damaged computer networks.

Using Online Payment Security Methods

Secure online payments are more important than ever as e-commerce becomes commonplace. It might feel daunting, but several methods can protect clients' information. Employee training, multifactor authentication, software updates and SSL certificates are just a few ways companies can keep customers safe while providing a great user experience.

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.

Increase In Mobile Threats Calls for A Proactive Mindset.

By Nicole Allen, Senior Marketing Executive at Salt Communications

Mobile threats are always evolving in the world of business.

Threats to mobile security are increasing: More than 60% of cyber attacks now occur on mobile devices, including phishing and smishing scams and password theft within organisations.

One crucial issue that is all too frequently ignored in businesses' ongoing efforts to boost productivity and reduce expenses is mobile security. Yet, how can an IT team effectively respond to the numerous cyberthreats that are becoming more prevalent and serious?

It's critical that businesses adopt a security strategy that is less reactive and more proactive. Companies that embrace a proactive mobile security model are not only more efficient and able to save money in these volatile markets, but they are also more secure. It's crucial to adopt a different perspective and approach this area with more vigilance.

The rise in mobile threats

Now that mobile usage has surpassed desktop usage, the time has come to understand how attackers target mobile apps, the motivations behind their actions, and what you can do to ensure your organisations are resistant to such dangers.

The rising use of mobile devices in itself isn't the alarming part. What employees do with these devices and the data they have access to are more worrisome. Verizon's annual Mobile Security Index survey indicates that 53% more mobile devices have access to sensitive data than they did a year ago. According to the same survey, customer lists, employee personal information, banking information, and other data that was formerly solely available through office computers are now also accessed through mobile devices.

One device is all it takes

Businesses might not be aware that one of their most vulnerable spots is mobile security. One unprotected mobile device in a business is all it takes for a cybercriminal to access the whole network.

Such intrusions can be fatal to a business of any size, disrupting its operations, jeopardising its vital data assets, and destroying customer relationships. In fact, the effects can be so severe that, after six months of a cyberattack, almost 60% of small businesses are unable to recover and cease operations.

Although technology has completely changed the way we conduct business, increased employee mobility has also brought us new security vulnerabilities.

Top 3 mobile threats

1. Obtain company data

Since they are one-stop shops for massive data dumps, businesses are the top targets for hackers. Data breaches at both large and small firms give hackers access to millions of user credentials, which they can then use to their advantage.

Companies pay hackers a lot of money to gain access to rivals' personal information. You might add things like trade secrets, client information, prices, sales and a lot more. By stealing its ideas and even clients, all of these can help the firm outperform the victim company.

2. Land and expand.

That is, to move beyond device control to higher value goals like the company network. A mobile device that has been compromised can be used in several ways to access business networks. The hacker may also use the device's connection to the corporate Wi-Fi network when the user returns to the workplace and reconnects by taking control of the device itself.

3. Delivering malware

We are engaged in a cyberwar where hackers are the enemy and malware is the tool, and insecure apps are the battlefield. Which is why it's crucial to understand the principal methods through which malware is disseminated.

Phishing emails are by far the most popular way for hackers and state-sponsored hacking groups to disseminate malware such as ransomware. Hackers have gotten very good at creating emails that fool recipients into clicking links or downloading files with malicious software. A prime example of this was the 2018 Atlanta, Georgia, SamSam ransomware assault, which shut down city operations and reportedly cost the city $2.6 million to recover from.

How to adopt a proactive mindset when it comes to secure mobile communications

You must establish a zero-trust mentality to shield your company from potential risks in order to safeguard it from a possibly catastrophic cyber-attack. Consequently, you must manage threats proactively and keep an eye on the devices, programmes, and services that access your network.

Many businesses treat communication as a series of dos and don'ts: encrypt important information; refrain from opening attachments from unidentified senders. However, this kind of directive approach is ineffective at motivating staff to become vigilant about new ways that hackers can cloak their attacks. Instead, the importance of secure communication must be embedded into your organisation's whole culture.

Each device that connects to your network puts your company at danger. You'll be on the right track if you begin by considering these possibilities as the framework for what you require to safeguard your company from the increasing quantity of cyber-attacks that are coming your way. Choose to adopt a proactive approach by protecting your mobile devices with a secure communications system, that will help turn your organisation's vulnerabilities into strengths.

If you require any additional assistance, please contact our experts for more information at info@saltcommunications.com or to sign up for a free trial of Salt Communications or to speak with a member of the Salt Communications team.

Discover why your organisation should learn more about your workforces mobile threats.

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://aag-it.com/the-latest-cyber-crime-statistics/

https://saltcommunications.com/news/how-to-identify-your-mobile-blind-spots/

https://saltcommunications.com/news/theres-no-way-youre-still-using-consumer-messaging-apps-for-business/

https://www.servicemax.com/uk/fsd/2018/01/25/you-shouldnt-risk-using-consumer-apps-for-work-communication/

https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/

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/

SEC’s New Cybersecurity Rules to Strengthen Transparency and Accountability

Why public companies should prepare now to safeguard their operations, reputation, and financial success.

By Paul Truitt, Principal and National Cybersecurity Practice Leader, Mazars

In a world where technology drives innovation, the security of enterprises and their assets has become of paramount concern. According to the latest IBM Data Breach Report, 83% of organizations experienced more than one data breach during 2022. With every company in the crosshairs, federal regulators have taken a key step that will require publicly traded businesses to rethink their approach to cybersecurity and avoid severe financial, operational and reputational damage.

In late July, the U.S. Securities and Exchange Commission (SEC) published its final rule on Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure. Set to take effect in December, this new mandate requires publicly traded companies to disclose “material” cyber events on a Form 8-K within four business days of the organization determining materiality (materiality should be established per current federal securities law).

The final rule also requires companies to describe their cybersecurity risk management, strategy and governance and how they are maintaining and assessing their security program in their annual Form 10-K filings. The implications of this new obligation are widespread and will stimulate a new era of cyber transparency for investors, the media and other key stakeholders. It ratchets up an already intense level of scrutiny on executives, particularly CTOs, CIOs and CISOs, who must now develop and execute yet another strategic program to strengthen and report on their cybersecurity posture.

Building stakeholder confidence through clarity

The new regulations will give investors and other stakeholders a new level of visibility into the cybersecurity approach of the organizations they invest in and follow. By mandating that companies disclose cyber incidents, the SEC is giving stakeholders a window into the threats facing enterprises and how well and how often they thwart these threats...or otherwise.

Similar to how external stakeholders now evaluate publicly available financial information to judge how well a company executes on its business model, they soon will be able to evaluate how successfully an enterprise is implementing its cyber strategy. Historically, cybersecurity has been a relatively obscure domain when assessing a business, with information usually coming to light through voluntary reporting from affected companies – sometimes well after the event. For example, a large service provider to managed-healthcare organizations reported in March 2023 that a data breach had impacted 4.2 million individuals. The incident occurred nearly one year prior to the public disclosure.

After the new SEC reporting rules take effect, however, the potential repercussions are almost limitless to consider. Will securities analysts grill executives during earnings calls about reported data breaches or gaps in their security program? Will we see journalists publishing league tables of companies that file the most cyber-attack disclosures or grading them on their security control frameworks?

Strengthening cybersecurity through accountability

Apart from being required to report material cyber events almost immediately, public companies will also need to provide annual disclosures about their cyber risk management strategies and the cyber expertise of the company's executives. This not only adds an additional layer of accountability for companies, but also presents an opportunity to strengthen current risk management strategies.

As organizations think about developing more comprehensive risk management strategies in response to the SEC's admonition, they may want to consider investing in performing an annual security assessment by a trusted third party. By making certain their organization complies with industry standards such as ISO 27001/27002, NIST 800-53 or NIST Cybersecurity Frameworks, business leaders can better position themselves and their teams to identify risks, implement controls and reduce the chance for trouble in areas of potential exposures.

Partnering with trusted third parties that track the latest threats — and cutting-edge mitigation strategies and tools — can benefit almost any organization. But this tactic can be particularly important for smaller public companies that may lack a robust cybersecurity and reporting plan, as outside experts can act as a team extension of an organization’s existing talent when it comes to evaluating vulnerabilities, rethinking investments, implementing controls and determining when and how to report the information the SEC will soon demand.

The roles of executives and directors

One of the most important aspects of this new rule is the involvement of executives and members of a company’s board of directors, as their engagement in and understanding of the organization’s cybersecurity posture become essential. Not only will this require a level of understanding of the new SEC rule, but it also necessitates adding a layer of governance to ensure the company follows it. Impacted companies should immediately begin hosting internal conversations between executives, directors and the organization’s cybersecurity experts to provide a close look into current controls in place to assess their efficacy. This may include reviewing assessments from outside experts and penetration-testing reports. Additionally, executives and directors should ask questions about how security controls are being implemented and how processes are being assessed to gain further insight into the current controls in place — and areas for improvement.

Final thoughts

The SEC’s new rule marks a crucial step in bridging the cybersecurity information gap between organizations and external stakeholders, while simultaneously encouraging public companies to reassess and strengthen their overall cyber strategies. For many enterprises, this will require a significant amount of work to be accomplished before the rule takes effect in December. At this stage, working with third-party advisors to leverage their expertise should be a key consideration. When the reporting and disclosure requirements become mandatory, companies will have to expect that news of their cyber incidents will be broadcast far and wide. But the enterprises that begin preparing now for this eventuality will be better positioned to safeguard their operations, reputation and financial success when the time comes.

About the Author

Paul Truitt is Principal and Cybersecurity Practice Leader at Mazars. He has over 20 years of experience providing business and technology solutions, with a deep background in identifying and mitigating security risks and performing cyber assessments for clients in the retail, healthcare, manufacturing and banking industries.

Prior to joining Mazars, Paul was a Managing Director in a mid-sized national accounting firm where he led the US Cyber Practice. He focused on managed detection and response (MDR), vulnerability management, penetration testing, security assessments and cloud security services. He also worked at a national managed services organization where he was the head of cyber services and Chief Security Officer.

Paul received his Bachelor of Science in Marketing and Management Information Systems from Salisbury University. He also holds a Master of Business Administration from Widener University.

Paul was awarded a bug bounty for submitting a remote exploit of an automotive remote access system that allowed remote starting and unlocking of the doors to any vehicle with the system deployed.

Paul can be reached online at LinkedIn and at our company website.

Redefining Operational Readiness with Predictive Maintenance Maximize the Resiliency of Our Nation’s Defense Assets

By Michael Weigand, Co-Founder and Chief Growth Officer, Shift5

In its annual threat assessment, the Office of the Director of National Intelligence (ODNI) warned that China is “almost certainly capable” of – and would consider – undertaking aggressive cyber operations against U.S. military assets worldwide if a major conflict were imminent. And recent data suggests that the results could be catastrophic as our defense resources remain vulnerable to operational failures and cybersecurity risks. In order for the U.S. to maintain its military edge, we need to proactively ensure the reliability, security and efficacy of our critical assets especially as it relates to the Department of Defense (DoD).

The DoD uses mission capable (MC) rates to assess the health and readiness of its military fleets – and just last year, the GAO reported that the MC rates of F-22s dropped nearly 17 percentage points over a six-year period. It also found that the DoD did not meet its MC goals for FY 2021 for 47 of the 49 aircraft in its review, with most aircraft more than 10 percentage points below the goal.

With national security depending on the safety and reliability of critical defense assets – predictive maintenance is key to ensuring operational readiness. Predictive maintenance refers to the use of hardware, software, and service components to provide predictive analytics for mechanical assets, infrastructure maintenance, and reliability objectives. Used to monitor emerging failures, predictive maintenance uses real-time condition-based monitoring and artificial intelligence (AI)/machine learning (ML) inferencing to identify expected failure points and determine remaining asset life. This intelligence enables military organizations to enhance operational readiness, enable cyber survivability, lower costs, shorten sustainment cycles, and increase platform availability [i.e., MC rates].

The DoD issued an interim predictive maintenance policy back in 2002. But in a December 2022 report on improving military readiness, the GAO found that in the 20 years since, military services have made limited progress in implementing it – despite pilot programs and evidence of improved maintenance outcomes. In a recent survey, 73 percent of DoD operations, maintenance, and IT leaders said they feel the lack of predictive maintenance across the DoD directly correlates to a low platform readiness/availability. However, if implemented and utilized correctly, the DoD can use predictive maintenance to its full potential, boosting the resilience and readiness of critical defense assets.

From Reactive to Proactive

In the absence of predictive maintenance, unplanned or reactive maintenance leads to more operational downtime and higher costs in the long run. DoD officials report that reactive maintenance often requires more materials and a higher level of effort than planned maintenance. In fact, by waiting until things break to fix them, the DoD spends $90 billion a year to keep ground systems, ships, and aircraft combat-ready, according to the GAO.

Downtime of critical defense assets puts personnel and national security at risk – but it is preventable. Minimizing downtime is key to improving operational readiness. In the same survey, 62 percent said they experienced weapons systems or aircraft downtime that could have been prevented with the use of predictive maintenance in the past year.

Turning Data into Intelligence

DoD operations, maintenance, and IT leaders need real-time knowledge of what is happening across all equipment and systems, unfortunately 73 percent say their current tooling fails to provide the data access and observability needed for effective predictive maintenance. Often, that's because sensors, log files, and recording devices capture data at prescribed intervals, rather than in real time, because of storage limitations. As a result, when an anomaly pops at a millisecond, it often escapes detection by a sensor.

The problem underpinning these challenges, however, is access to this onboard data when digital anomalies arise. Weapon systems today lack an onboard sensor capable of capturing, storing, and analyzing these massive amounts of data on the edge in real time. Consider this: if you don't have a complete dataset to begin with, the output of whatever you are trying to do with the data – in this case, take action for cyber or maintenance purposes – will only be as beneficial or accurate as the input.

In one of its pilot programs, the U.S. Air Force used AI and ML algorithms with data collected from condition-monitoring technology to predict when B-1 bombers will break. The Air Force estimated saving $5 million in two years – just by reducing unscheduled maintenance on ten B-1 bombers.

However, success is fragmented because the DoD has not consistently adopted and tracked implementation of predictive maintenance. In the survey of DoD operations, maintenance, and IT leaders, 84 percent said their organization must improve its ability to predict and prevent equipment failure.

Observability Builds Resiliency

Operational readiness hinges on real-time knowledge of what's happening onboard critical defense assets. But 60 percent of DoD leaders say that when an issue arises, their organization struggles to determine if the root cause is a cyberattack – or an equipment maintenance issue.

This stems from a lack of full system observability – a full view of system performance. With onboard observability, maintenance teams have the knowledge to evaluate operational readiness and differentiate between cyber and maintenance issues. The best way to visualize the full system is to capture all data communications on the operational technology (OT) and from every component on the platform. To capture real-time onboard data from legacy OT, the DoD needs full-take data capture, which records every frame down to the millisecond – across the entire fleet.

Armed with onboard observability, the DoD can confidently act on data-driven insights to optimize the availability and resiliency of defense assets and boost MC rates across the services. On average, DoD leaders expect a 35 percent increase in their department's MC rate from the successful implementation of predictive maintenance, according to recent research.

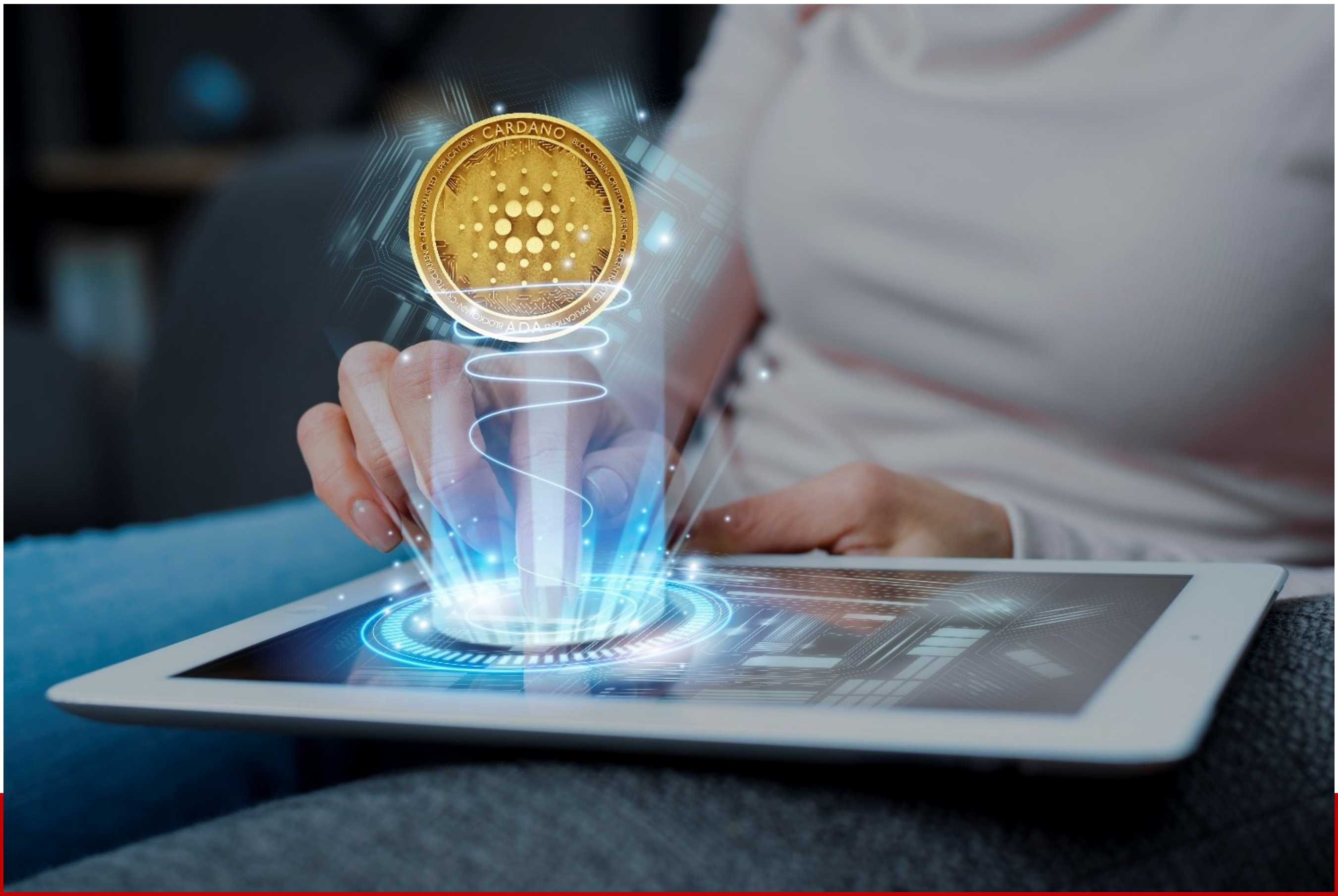
The growing complexity of technology and critical defense assets, paired with the increasing threats to national security, requires an urgent reform of the DoD's approach to maintenance. Predictive maintenance offers solutions to some of the DoD's greatest challenges: shifting to a proactive approach to maintenance by predicting and preventing cyberattacks and critical failures.

About the Author

Michael Weigand is the Co-Founder and Chief Growth Officer at Shift5. He is responsible for defining and overseeing execution of Shift5's long-term growth objectives. Prior to Shift5, Michael served eight years in the U.S. Army as an Airborne, Ranger-qualified Infantry officer and was selected as one of the first cyber operations officers. While at a Department of Defense support agency, he served as an engineering and operations officer conducting both applied research and development (R&D), development, and field operations.

Michael has established and commanded multiple cyber organizations and skunkworks-style teams across the Army and DoD. Notably, he was instrumental in the establishment of the Army's platform mission assurance program, the Army's expeditionary cyber forces, the Army's first cyber capability development unit, and multiple high-profile projects in conjunction with the Defense Digital Service. Michael holds a BS in Computer Science from the United States Military Academy. Other than defending OT, Michael's secret superpower is flying small airplanes into small places.

Michael can be reached online at linkedin.com/in/michael-weigand/ and at our company website shift5.io/.



The $390 Million Alarm Bell: Why Cold Wallets Are No Longer Optional in Crypto

By Mark Venables, CEO of The Crypto Merchant

In July 2023, the cryptocurrency sector saw a significant escalation of cyber-related incidents. The loss was initially reported at $486 million but has since been recalculated to reflect new information and placed close to $390 million. The reduction gave little comfort to those who saw losses during the month and didn't do much to set the crypto world at ease.

Most losses were attributed to the Ethereum platform, which lost over $350 million in 36 incidents. Binance recorded notable losses totaling around $11 million from 18 incidents. Regarding the recovery efforts, their success was minor — only $7.63 million were reclaimed.

The gravity of this July's incident report becomes even more apparent compared to July 2022, when slightly more than $80 million in cryptocurrency was lost in incidents. The fivefold increase occurred over access control exploits, rugpulls, and reentrancy attacks. It was a stark reminder that cryptocurrency holders must take security more seriously.

Cold Wallets: An Underutilized Line of Defense

Cold wallets are an effective security measure that can help safeguard cryptocurrencies against various attack vectors. They are called “cold” because they’re not connected to the internet, which means they can’t be attacked the same way a regular, “hot” wallet can. They are also called “hardware wallets” because they often come in the form resembling a USB stick — they use external hardware devices to store private crypto keys safely.

Cold wallets have additional safety features besides their offline nature. They can be dust- and waterproof for extra physical durability. Some will have automatic data elimination for breach detection. They come with PINs and seed phrases that help retrieve data if they’re lost. Cold wallets can offer different levels of tamper protection and can use biometric security features.

The biggest problem with them, however, is that their market penetration is only at ten percent — they are incredibly underused.

Cold Wallet Sales Surge in Crisis Moments

Cryptocurrency holders need an occasional nudge to remind them that there are additional things they could be doing to keep their funds safe. Sadly, it’s usually when something terrible happens that people choose to react.

When FTX collapsed in November 2022, Trezor and Ledger, among the most prominent makers of cold wallets, confirmed to Decrypt that their sales had increased. Talking to Cointelegraph, Ledger’s CEO Pascal Gauthier noted how disruptions in the market usually cause an uptick in the company’s sales. He cited Coinbase’s declaration of losses and Celsius’ fund freezing as two other events.

Chances are the most prominent players on the market will see another surge right about now. The problem remains that, despite the advantages of cold wallets, many cryptocurrency enthusiasts will remain unaware of them or hesitate to invest in one until an event or report nudges them into buying it. And hopefully, it will be a report, not a security event where their assets are compromised.

Breaking the Misconceptions

Crypto enthusiasts have been slow to adopt cold wallets for several easily identifiable reasons. One popular misconception is that the setup and maintenance of cold wallets are complex. Manufacturers have done great at streamlining the process over the years, reducing the initial learning curve. Plus, there’s a wealth of online resources for guidance.

The cost might be another obstacle. A high-quality wallet from a renowned brand with solid features comes with a price tag that might seem too much for some, especially novices. There are always cheaper options, but a costly cold wallet can still be an excellent investment. The potential costs of losses from a cyber-attack can easily justify the investment.

How to Get a Good Cold Wallet

When people decide to get their cold wallet, they first have to consider where to buy it. Cold wallets should be purchased from the manufacturer or authorized resellers. Manufacturer websites such as Ledger.com will hold a list of authorized resellers.

The next step would be determining how someone wants to use the wallet. Some users prioritize trading, while others wish for long-term storage wallets. Some cold wallets even allow crypto-loaded gift cards, a great way to pass on digital assets to others.

Wallets have many features that make them more or less complicated and secure. Some can be as simple as a thumb drive. Others will have biometric scanners. Seasoned traders will have different cold wallets for various purposes, too — there's no need to restrict oneself to only one cold wallet.

The bottom line is that the bigger and more successful the cryptocurrency industry is, the more of a target it becomes for hackers. One of the best ways for people to safeguard their digital assets is to take an active role in self-custody. The reality is that adopting cold wallets en masse isn't a precaution but a necessity. And no one should wait for the wake-up call of becoming a target or losing their assets.

About the Author

Mark is a multifaceted entrepreneur who has excelled in multiple industries. His diverse portfolio includes a long-standing staffing agency, a background screening business, a UK-based real estate business, and a prominent ecommerce business - The Crypto Merchant. The Crypto Merchant, his latest major acquisition in 2021, is now the largest reseller of crypto cold wallets in North America.

The 5 Things Every Leader Should Know for A Cyber-Vigilant Summer

By Michael Nizich, PhD, CISSP

As another summer comes and goes and we start to prepare for another school year, IT departments all over the country are dealing with fallout from yet another season of traumatic and devastating security breaches that seem to become more prevalent during the summer months. IT Governance identifies 85 major breaches in July alone in 2022 and with average recovery costs now hovering at around four million dollars per incident according to IBM, the damage to our economy is becoming unbearable and consumer trust in our organizations to keep our personal and customer data secure is dwindling quickly. So, why are the summer months different with regard to data breaches? Below are 5 things that every leader should know to enjoy a cyber-vigilant summer.

1. We do not share the same holiday and vacation schedule as cybercriminals

Cybercriminals know that organizations and their employees are quite understandably less vigilant during the summer months and holidays in general and thus focus on these particular times to take advantage of a less vigilant workforce. They also know that the summer workforce may be dotted with temporary staff or contractors that may not have had the same security training as their full-time staff. Many employees, quite admirably, also continue to work remotely at least part of their days during the holidays and this creates a very attractive target for cybercriminals...corporate leaders working on company devices using public Wi-Fi to connect to their headquarters. Everyone has a busy season and unfortunately for us, the busy season for cybercriminals tends to be holidays, weekends and of course the summer months.

2. Public devices are just that...public!

Try to avoid using public devices during your travel. It is so enticing to see a very nice, comfortable business center and decide to sit down and do some work. These devices are always available to hotel guests and employees around the clock and, in some cases, anyone at all who happens to access the lobby. These systems can be easily installed and configured with keyloggers or other malware that may compromise your login credentials and other personal information.

3. Public Wi-Fi is a hunting ground for cybercriminals

There are things you can do, and more importantly as leaders, there are things that you can enforce through corporate policies that will make your organization more secure. One is to confirm that while traveling and working outside the office, you are using a secure Wi-Fi connection or simply using your mobile wireless connection to ensure encrypted transmissions between your device and the Internet. This can minimize, or even eliminate, the risks of popular attacks like Man-in-the-Middle (MitM) attacks where you may really be attached to a private router even though you assume that you are attached to a trusted router, or malware injections where someone else on the same wi-fi network is infecting your device with malware from another device on the network. Another thing you can do is to use a Virtual Private Network or a VPN once you connect to your public Wi-Fi. This will create a secure tunnel between you and your organization in which all data is strongly encrypted so that if the data is intercepted then it will be essentially unusable to whomever intercepted it.

4. You wouldn’t call a criminal and tell them you are going away so why post it on social media?

This is the most difficult one to adhere to and to stay diligent about. Who among us does not want our friends and family to know that we are on a beautiful mountaintop with our loved ones and simply enjoying life? However, while you are on that mountaintop, it is very evident to cybercriminals that you are not at your home, and more importantly, you are definitely not at your place of business. This means that there are myriad opportunities for cybercriminals to cash in on your inability to do anything to prevent a breach and they enjoy the fact that you may not even know about the breach until you return. Try your best to keep your personal details and whereabouts just that, personal. The more we give the criminals to work with the more information they can use against us.

5. Don't focus on just the technical aspects – Social engineering and physical theft is part of the crime.

It is a fact that there are more personal property crimes including stolen wallets, passports, ID's and cell phones during the summer months and tourist attractions and highly visited locations are some key hunting grounds. This makes both the time of year and the locations highly attractive to all kinds of criminals and this is no exception for cybercriminals. Be extremely cautious and conscious of the security you are using on your phones including locator services, biometric security and complex pins and passwords as well as device lockout services and remote wipe capabilities. Having these activated and configured properly can make you feel comfortable that, as frustrating as having your phone stolen would be, the information on that phone is both backed up and secured from cybercriminals.

There is no guarantee that you will not experience a data breach or identify theft during the summer months nor is it set in stone that you will. However, it is completely possible to drastically reduce that risk of experiencing a breach by staying cyber vigilant as you travel the globe and enjoying what we are all here to enjoy...our lives. Hopefully these 5 tips will help you as leaders to stay cyber-vigilant during the summer months.

About the Author

Michael Nizich, PhD, CISSP is an Adjunct Associate Professor of Computer Science and Cybersecurity at New York Institute of Technology and is the author of the new book, The Cybersecurity Workforce of Tomorrow

The Embedded Systems and The Internet of Things

By Milica D. Djekic

The Internet of Things (IoT) is a quite new concept dealing with the devices being connected to each other and communicating through the web environment. This concept is gaining its popularity amongst the embedded systems that exist – let's say – 10 or more years back. The main applications of these systems are in mechatronics that is a synergy of electrical and mechanical engineering as well as computer science. Through this chapter, we intend to discuss how the entire IoT concept could get applied to the embedded systems as well as mention some aspects of their security in order to clarify all sorts of risks and threats being present within those paradigms.

What are the embedded systems?

The embedded systems are still a quite recent concept that is only the part of a long-term technological evolution we are witnessing during the last several decades. The entire new revolution would start with the digital systems and first logic gates being used for that time – pretty robust electronic devices. As time would go on – the devices would get more and more sophisticated and today we have so simple and helpful solutions. The embedded systems are nothing else – but computing systems in small – usually dealing with the microcontrollers being the central processing unit to some electronic board.

These units could get found nearly everywhere including mobile technologies, traffic systems, mechatronics devices, medical equipment or portable solutions.

The smart equipment is mainly the part of a developed world, while some of those systems already got used in a developing society. The best possible example to describe which of the devices being exposed to the web use the embedded technology is to mention the case of medical devices being the quite common target of the hacker's attacks. This equipment is usually correlated with each other and normally has the access to the internet. Many studies, researches and conference efforts would talk about how that sort of devices got vulnerable to cyber attacks. So, in other words – the majority of embedded systems got threatened from the hacker's community. Being online or not – the embedded technologies could get hacked and if they are on the web, that would mean they are the part of the IoT.

So commonly, we would use the expression an IoT-driven embedded systems meaning by that the embedded systems being capable to talk to each other or use the web signal to deal with some computer's units. Their microcontrollers frequently deal with the microprocessors that got a quite similar role as standard processors within some computer's systems. The majority of today's experts would call the IoT-driven embedded systems – the smart digital solutions – and, for real, those systems would have many advantages and offer a certain level of convenience to their users. If we would talk about the hacking of those devices – we should mention that there could get used different strategies that would provide the access to those devices and use some of their weaknesses to get control over them.

As we would suggest before, all of those solutions would be digital and use the electricity to obtain their operations. In other words, this equipment would deal with some sort of electromagnetic field which could be affected applying the interference or used to detect such a device and conduct the hacker's campaign on so. In other words, the main challenge of those smart devices is their cyber defense and for such a reason – we would appeal on their designers to take into consideration those requirements. At the moment, there would be some security's procedures included that would support us to deal with less risk, but one of the challenges for tomorrow would be to design a solution that would deal with the better cybersecurity.

The IoT-driven embedded systems

Through this chapter, we would mention the IoT-driven embedded systems suggesting they are nothing else – but smart digital solutions talking to each other through some communication means. For the communication purposes, we can use the standard internet protocols being wired or wireless or another way of the signal carrying. The internet itself would rely on many signal carriers and almost any sort of electromagnetic wave could serve as a carrier of the information. For instance, many variations of the wireless internet would use radio signals, while satellite communication systems would deal with the X-band range.

So, if we talk about the internet as a medium being used to carry on our information – we would talk about a wide variety of electromagnetic waves belonging to many different frequency's spectrums. These sorts of communications could get applied to the embedded systems making them being linked to each other and communicating using those waves. It's quite clear that anyone could try to break into such a communication, so it's highly recommended to apply some sort of encryption – either being an end-to-end or link cryptography. Finally, a technological progress is something that would always go on and for such a reason we should think about security's requirements as we still live in a quite unsafe world dealing with a plenty of risks, threats and challenges.

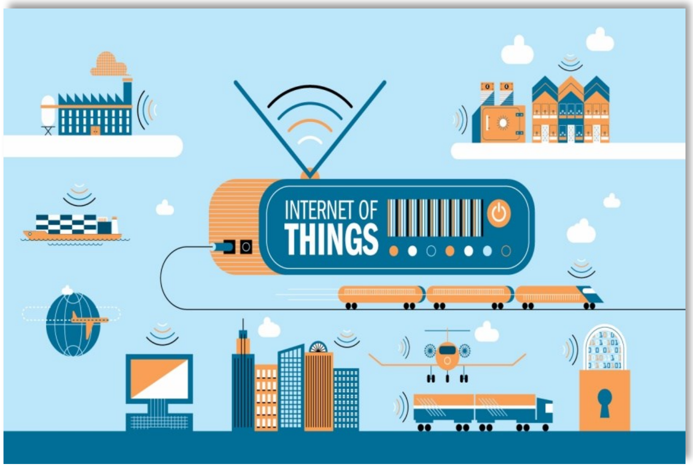
The security's aspects of that concept

The security's aspects are gaining their attention in a modern time and it seems in a current era of many security's concerns – we need to think about these requirements more than ever. Unfortunately, through this time – we are witnessing many threats such are organized crime or terrorist groups that would use the advantages of new technologies to obtain their certain goals. As the entire human society got dependable on emerging technologies – the similar situation is with the majority of defense's threats. We all would rely on computers, digital devices, embedded systems, smart solutions, internet and mobile technologies, so it's crucially significant to take care about our security's aspects.

One of the good advices would be to include some of security's requirements to product's designers, while – on the other hand – we should always try to follow the best practice and some of the security's procedures. In conclusion, we could realize that the future of this digital era would be the security's age that would make us think hard how to cope with all today's challenges.

The final comments

At the end, it's so important to highlight that the embedded systems are something that exist in our world at least a decade back and only new thing is that the current time would make those systems talking to each other. That's how we would come to the IoT-driven embedded systems which would become one of our today's imperatives. Finally, a great deal of defense's threats would make us think about better security to all of those solutions.



About The Author

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

The Emergence of AI In the Enterprise: Know the Security Risks

By John Anthony Smith, CEO Conversant Group, and Eli Nussbaum, Managing Director, Conversant Group

As businesses strive to keep up with the rapid pace of technological advancement, many are turning to artificial intelligence (AI) tools as an increasingly vital component of their strategies. One such tool is ChatGPT, an OpenAI language model being leveraged by cross-departmental employees in customer service, marketing, research, and more. However, as is often the case with any new, emerging technology, using AI comes with security risks, and it's essential to understand them and impose the proper guardrails around them to protect company, customer, and employee data.

While we could delve into some of the defensive cybersecurity concerns AI presents—such as its use to create more realistic and compelling phishing emails and social engineering tactics as well as broader "Skynet" type concerns—we will confine our discussion to the risks inherent in leveraging ChatGPT and other Artificial Generative Intelligence (AGI) as productivity tools. There are real, tangible risks businesses must address today, as AI/AGI is a relatively immature technology actively making its way into the corporate environment. Specific to ChatGPT, there are many unknowns regarding its ongoing evolution and how it impacts data and information security. From an infosec perspective, managing "unknowns" is not anyone's view of ideal. Cybersecurity is the art and science of attempting to achieve full transparency to risk and then mitigating and controlling that risk.

Even if an organization secures its connectivity to OpenAI, it is challenging to ensure data protection, particularly granting the tremendous data troves gathered by ChatGPT. In late March, OpenAI disclosed a data breach that exposed portions of user chat history as well as personal user information including names, email/payment addresses, and portions of credit card data over a nine-hour window. That same week, threat intelligence company Grey Noise issued a warning regarding a new ChatGPT feature that enabled expanded data collection features using a plugin, which they believed had been exploited in the wild. Samsung employees also leaked sensitive data into the ChatGPT program; as a result, Samsung lost control of some of its intellectual property. Since there are little to no legal precedents for this activity, these types of leaks have the potential to cost organizations billions in lost opportunity and revenue. There is also little evidence of how the large tech companies that control these platforms may leverage this newly found treasure trove of previously undisclosed intellectual property.

These issues highlight the vulnerability of the product and raise serious concerns about the security of sensitive information that businesses, knowingly or unknowingly, entrust to ChatGPT. As with all third parties, these platforms must be vetted and their vendors contractually bound to protect the data to your organization's standards before being permitted access to it.

The security issues also underscore the legal obligations of organizations to secure their own and their clients' data. Law firms with attorney-client privilege and those subject to regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the EU's General Data Protection Regulation (GDPR) are particularly affected. Organizations must ensure the security and privacy of their information. Using a third-party service like ChatGPT creates challenges to these obligations.

Importantly, OpenAI's ChatGPT and Google's Bard learn from and store information from many sources. Organizations should never place corporate and client information into these platforms, as it must be assumed it can be viewed by those unauthorized to do so (intentionally or otherwise). The lack of clarity and transparency around how data is being handled creates a real risk for businesses using ChatGPT. Yet, lacking direct action by IT or security teams to impose controls, users can easily copy and paste data of any level of corporate sensitivity into the platform, without their organization's knowledge or consent. Thus, these platforms should be blocked by default, despite their current attraction and whirling popularity. For organizations that require research and development in these platforms, access should only be permitted for those groups.

Today, it is quite difficult to block these platforms by default because they are popping up quickly (as well as their related scams). Fortinet, Palo Alto Networks, Cisco, and other security vendors have not yet created holistic lists that include all the OpenAI and ChatGPT options available. Thus, IT is left to compile manual lists of these tools for blocking.

To mitigate the risks of AI tools, organizations need to take a proactive approach. They should conduct thorough risk assessments to understand their exposure and ensure that appropriate security measures are in place, such as encryption, access controls, data leakage protection, and active monitoring. Proper policies must be defined and approved. Until such policies and controls are in place, the use of ChatGPT and similar tools must be blocked—just as they would (or should) any other non-approved IT system.

Though powerful and seemingly useful, organizations must not allow ChatGPT and similar tools access to their systems and data until they can clearly understand the risk inherent in them and can control against or accept those risks. And, as AI and technologies like ChatGPT and Bard are evolving at a lightning pace, continuously securing these iterations will certainly provide new challenges for both organizational IT and security researchers.

There continues to be much debate about the risk vs. reward of AI/AGI in enterprise settings. Clearly, a tool that produces instant data, content, and analysis provides value; whether the risks can be contained, controlled, and managed to a sufficient degree to justify these rewards will be tested over time. Just like any other tool, AI's effectiveness and impact must be weighed. Organizations need to separate hype from reality before even considering the use of these tools. After all, an OpenAI spokesperson recently commented on its product's ability to "hallucinate" and "make up information that's incorrect but sounds plausible."

While the fear of AI evolving into Terminator or Skynet is certainly fun to hypothesize, the immediate risk is to today's data and customers' networks. Therefore, it is essential to prioritize data security to protect our organizations and the clients we serve.

About the Authors

John A. Smith is CEO of Conversant Group and its family of IT infrastructure and cybersecurity services businesses. He is the founder of three technology companies and, over a 30-year career, has overseen the secure infrastructure design, build, and/or management for over 400 organizations. He is currently serving as vCIO and trusted advisor to multiple firms.

A passionate expert and advocate for cybersecurity nationally and globally who began his IT career at age 14, John Anthony is a sought-after thought leader, with dozens of publications and speaking engagements. In 2022, he led the design and implementation of the International Legal Technology Association's (ILTA's) first annual cybersecurity benchmarking survey.

John Anthony studied Computer Science at the University of Tennessee at Chattanooga and holds a degree in Organizational Management from Covenant College, Lookout Mountain, Georgia.

John can be reached at @ConversantGroup on Twitter and at Conversant's website: https://conversantgroup.com/

Eli Nussbaum is Managing Director at Conversant Group and its family of IT infrastructure and cybersecurity services businesses. He has over 25 years of expertise as an information technology consultant, with a focus on aligning IT strategies to current and future organizational goals, developing cloud migration and security strategies, and helping services businesses get laser focused on the security and efficiency needs of their clients.

Prior to joining Conversant Group, Eli held numerous roles over 22 years at Keno Kozie Associates (an IT outsourcing firm for the legal industry). He is a regular content contributor to top legal publications and frequently speaks at legal technology events.

Eli can be reached at @ConversantGroup on Twitter and at Conversant’s website: https://conversantgroup.com/

The Human Firewall: Strengthening the Weakest Link in Cybersecurity

By Steve Soukup, CEO, DefenseStorm

Innovative technology has revolutionized the way we work and live by unlocking a wealth of new capabilities. As artificial intelligence makes daily operations more efficient and flexible, people become increasingly reliant on the luxury of digital technology. Of course, businesses then competitively introduce the latest and greatest to meet the demands. With new technology and changed business operations comes exposure to new cyber risks, prompting companies to prioritize and invest in stronger cybersecurity measures.

Ominous headlines touting 2023 as the “Year of Risk,” have organizations scrambling to increase their cybersecurity budget and buy the latest threat detection technology. The technology and supportive resources to prevent threats from becoming attacks are important, but what if I told you that while you have the newest, state-of-the-art technology safeguarding your systems, your employees are your biggest vulnerability? Even the most technologically savvy employees are a liability. Just ask NASA about the Mars climate orbiter…a simple human mistake in measurement conversion by scientists led to a navigation error sending the climate orbiter to its demise, burning up in the Martian atmosphere. The result? A loss of nearly 200 million dollars and red faces all around.

The reality: Despite having the most effective cybersecurity measures implemented, a simple human error can lead to significant financial losses, interruptions in business operations, and harm to the organization's reputation.

The Weakest Link

Companies become confident and ready to take on the threat of cyberattacks after implementing the newest and most advanced solutions in cyber risk management. Most businesses eagerly invest in the best security products, hire external monitoring support for their internal teams, and implement proactive strategies for preventing and mitigating cyberattacks. Money spent, new technology employed, defenses at the ready – you're prepared. And then, a targeted C-level executive mistakenly clicks on a phish - cue data breach, assets are at risk, and sensitive client information is compromised. This cyberattack was 100% preventable.

A joint study by Stanford University Professor Jeff Hancock and security firm Tessian, found that a staggering 88% of data breaches result from employee mistakes. IBM Security's research reports an even higher figure at 95%. So, you've secured your house, purchased the strongest locks, and installed the most advanced home security system…and then someone leaves a window open.

An understanding of cyber risk awareness is just as vital to the maturity of your program as having the right products in your cyber toolset or implementing a proactive plan. Integrating all these essential components is what makes your company fully prepared to tackle cyber threats, but recognizing the importance of security awareness is also crucial to prevent costly errors.

The WHY and HOW

Understanding how employees can inadvertently cause a hole in your security is vital to protect your business. Mistakes are made at ALL levels and across ALL departments due to insufficient cyber risk awareness training, distraction, burnout, or even complacency. Some of the worst breaches occur from a simple lack of knowledge.

Ask yourself: Do your employees casually open emails on their phones, oblivious to the telltale signs of a phish? Are they click happy just clicking links and downloading files without regard for the source? Do they reuse the same password across multiple accounts? Is their professional device automatically connecting to an unsecured Wifi? More importantly, do they even realize that these actions make them vulnerable?

Another challenge associated with cybersecurity awareness is outright distraction. Most employees are constantly running busy and opening messages on the go. Most of us are juggling three tasks at once, and we are aware of the risks, BUT are we paying attention?

Consider this incident: You're hurrying to shut down for the day so you can get to your kid's soccer game on time when an email pops up in your inbox. It's from your CEO with the subject line: Explain these numbers. Your heart practically stops. *What numbers?* The clock is ticking to get to that game, so you immediately open it, quickly skim through the email, and download the attachment. You fell for it - CEO spoof. Had you stopped for a second, you would have realized that the email says your CEO's name, but the address is from an outside entity. If you had carefully read through, the message has slightly broken English, and the signature line is wrong. You've been duped. It happens, but how can this costly mistake be prevented from occurring over and over again?

Cyber Risk Awareness

Whether caused by distraction or lack of awareness, the consequences of a breach are still the same - compromised data, interruption of service, monetary loss, and a tarnished reputation. Strengthening cyber risk awareness is important for all employees to prevent these simple but egregious mistakes. Keeping employees trained, aware, and motivated can be done by employing these best practices:

1. Integrate cyber risk awareness training in the onboarding process for new hires.
2. Train all employees; we mean ALL – from the interns to the C-Level executives.
3. Provide ongoing training and workshops to identify questionable links, emails, and other potential threats. Equally important is teaching proper protocol to create strong passwords, handle sensitive information, and responsibly use technology. Simulated phishing exercises can help employees learn how to distinguish between a possible threat and genuine communication.
4. Motivate and empower! Participate in cyber awareness campaigns with memorable slogans that can be used internally on posters, magnets or mouse pads; use catchy reminders like "Think Before you Click" or "One Click is all it Takes" to keep it fresh in everyone's mind.

One of DefenseStorm's clients recently shared that they motivate employees to pause and think about cybersecurity by using two monthly raffles. Employees are entered into the first raffle when they successfully identify a campaign phish and are submitted for the second raffle if they identify a real phish. Getting the conversation going by using motivational tools and incentives creates an opportunity for positive reinforcement and open communication, so your employees remember to stay alert even amidst distractions. If everyone is talking about it, can they really forget?

5. Cybersecurity awareness also includes the collection and distribution of important alerts and news. Ensure all employees are signed up for the latest cybersecurity news updates. Send out messages internally to alert employees of possible threats.

DefenseStorm provides Daily Security Intel Bulletins, which is a collection of the most important cybersecurity news and alerts for the day, to all clients and employees. The bulletin promotes peer-to-peer sharing and builds a community of trust to work together against the threat of cyberattacks.

Prioritize Cybersecurity Personnel

Even the most technologically savvy employees can become a significant liability. Burn out, gap in talent, waning skills, and complacency among internal cybersecurity teams can easily be a cause of vulnerability in your security.

Have you checked in with your cybersecurity team? How are they managing? Companies report major burnout because the workforce ratio versus cyber events is overwhelming. The demands to scrutinize the constant flood of cyber events can't be managed by outdated manual processes and understaffed teams. When employees are overloaded, mistakes happen. There is also concern that internal Security Operations Center (SOC) tasks become redundant for individuals. Boredom fuels complacency, which in turn, spawns errors and oversights. Build a stronger internal team through evaluation and training to keep them alert, motivated, and ready for emerging threats. Consider these effective strategies:

1. Ensure your internal cybersecurity team receives active support from the executive team.
2. Address employee burnout by leveraging AI technology and partnering with external teams to co-manage your cybersecurity.
3. Combat redundancy by cycling employees through different roles and providing learning opportunities with new technology for analysts.
4. Bridge the talent gap by creating partnerships between base analysts and incident responders which provide advancement of skills.
5. Strengthen skills with Maturity Mapping to evaluate your internal team's capability and preparedness. Running through simulated exercises and evaluations gives insight into your institution's performance and readiness. Understanding your internal team's response, resilience, and recovery abilities allows for setting goals, benchmarks, and performance expectations.

Staying Informed and Alert

With cyber threats, emerging technology, and daily operational demands contending for priority, it’s easy to forget the pivotal role human factors play in the success or decline of a business. It’s possible for any one of your employees to make a damaging error, so while you are beefing up your cyber defenses, remember the cautionary tale of the Mars orbiter mishap and how even rocket scientists can have their "oops" moments. Don’t wait until an avoidable mistake - foster a culture of continuous cyber risk awareness, nurture your cybersecurity teams, and implement comprehensive training programs. With education and empowerment, companies can prevent mistakes, reduce the impact of human error, better safeguard their valuable assets, and maintain a strong and resilient defense in the face of the ever-evolving cyber risk landscape.

About the Author

Steve Soukup is the Chief Executive Officer for DefenseStorm. He was first appointed Chief Revenue Officer in 2017 with a primary focus to drive business growth while leveraging his extensive experience serving the banking vertical. Before joining DefenseStorm, He has held leadership positions at Intuit, S1 Corporation, and KPN and acquired direct banking experience through management positions at Key Bank, BankBoston, and State Street Bank. Based on his ability to successfully deliver results, Steve was promoted to DefenseStorm President in October 2019 and then to CEO in April 2020, where he leads all aspects of the business. Under his direction, DefenseStorm has set the standard for enabling banks and credit unions to achieve cyber risk readiness while establishing an empowering tone and culture through the company's core objectives. Steve serves with a passion to live, work, and promote the DefenseStorm mission to *build a community of trust so we can grow and thrive together*. He prides himself on nurturing relationships between the company, employees, and clients, which has resonated deeply into the fabric of DefenseStorm's client base, proving that a positive culture starts from the top. Steve holds a bachelor's degree in finance from Boston College and an MBA from Boston University's Questrom School of Business.

Steve can be reached at Steve.Soukup@DefenseStorm.com – www.DefenseStorm.com

The Rising Tide of Cybercrime as A Service (CaaS)

By Nik Hewitt, Sr. Content Marketing Manager, TrueFort

Welcome to the era of Cybercrime as a Service, or CaaS, which, quite alarmingly, is like an online marketplace for cybercriminals and their services.

While nothing new, it's on the rise and a game-changer. Now, anyone with an internet connection and a chip on their shoulder – an unhappy customer, a scorned ex-lover, a disgruntled ex-employee, or a bitter competitor – can employ illicit services such as fraud, cyberattacks, social account takeovers, and even deploy ransomware.

And all this, believe it or not, for the price of our morning coffee and bagel.

How Much Does Cybercrime Cost?

Loading up Tor, we took a dive into the digital underworld of .onion sites and forums, exploring official reports and braving the murky corners of the dark web to gauge the cost of these unlawful digital deeds. Everything we found was from just one evening of exploration. To maintain ethical boundaries, we've chosen not to share links to these illicit services, but be assured that a chilling array of options are available for prospective CaaS customers.

Interestingly, the dark web also provides escrow services that hold funds until the buyer is happy with their underhanded 'purchase,' ensuring a somewhat bizarre level of customer service in these illicit transactions.

Devious DDoS on Demand

Fancy crippling a website with a torrent of bogus traffic? It’s possible to commission a targeted Distributed Denial of Service (DDoS) attack for just $5. If you're willing to shell out $500, you can ramp up the chaos to a 24-hour onslaught potent enough to buckle most commercial servers. The fallout? Lost sales, exhausted security personnel, and a battered reputation - a nightmare scenario, especially if timed to coincide with peak traffic.

DDoS attacks are so powerful that they’re being used as weapons of war. In recent months, hackers with ties to Russia have launched sophisticated cyberattacks against Ukrainian state services, notably targeting the application known as "Diia." These attacks have been executed using a combination of malware and phishing techniques. The Ukrainian defense and security agencies are among the most vulnerable and primary targets of these cyber onslaughts.

Invading Personal Spaces

Your personal life is up for grabs in the shadowy marketplace of the dark web. Despite the existence of legal background screening services, the dark web is rife with illicit offerings that promise to delve deeper into a person's life, background, and financial details for a mere 120-200 USD.

The price tag for thieves might be low, but the cost to society adds up. One recent report concluded that almost 42 million Americans had their identities compromised in 2021, and that the total cost to US consumers was over $52 billion. Young people and the elderly are at increased risk, as are those whose wealth makes them attractive targets for theft of any kind.

Social Media Mayhem

Should someone want to gain control over someone else's social media accounts, or recover their own after a security mishap, the dark web provides this service for only 300 USD. This reality underscores the urgent need for beefed-up personal security, strong password practices, and the savvy use of password managers at home and work.

Trust forms the cornerstone of any social platform. It's what lures people into sharing (often confidential) information. Yet, this very trust can also be a gateway for cybercriminals to gather invaluable data that are then used in orchestrating attacks against organizations or to conduct wider attacks using credential-stuffing tactics. Each month, social media platforms bear witness to the hacking of an astounding 1.4 billion accounts [Gitnux].

Bad actors also exploit personal accounts that are admins' of business accounts. By assuming a brand's identity, they can target a company's employees and customers to pilfer their credentials. Social media is implicated in approximately 81% of all hacking-related data breaches. The greater a business or communities' presence and engagement on social media, the higher the likelihood that cybercriminals will set their sights on their users. Apart from directly targeting businesses and communities, cybercriminals are also known to exploit social media to engage with potential victims for phishing purposes – an obvious call for MFA and strong personal password protocols.

Points for Pilfering

Even loyalty points aren't safe. In a concerning trend for the industries that rely on these rewards, like gaming, aviation, and eCommerce, stolen loyalty points are available for purchase on the dark web. With prices determined by the number of points desired, the digital theft of these assets can also extend to cryptocurrency. Price seems to depend on the number of points desired – 50,000 gaming loyalty points could cost as little as 16 USD, while 200,000 frequent flyer miles might be as low as 70 USD.

One Akamai report found that there were over 100 million "credential stuffing" attacks between July 2018 and June 2020 in which bad actors gained access to one account and used that same password to infiltrate another. 63% targeted the travel, hospitality, and retail loyalty programs. With the global loyalty market expected to reach a value of $11.4 billion by 2025, it's easy to see the incentive for thieves.

Sneaky Spyware

The past decade has seen countless scandals around hacked phones and privacy breaches. The dark web is a marketplace for these services, too, with prices starting at 240 USD to plant spyware on a person's phone, with costs varying based on the target and desired level of access.

How big is the spyware issue? TechCrunch recently reported on an Iranian-developed app called Spyhide that is already believed to be on tens of thousands of Android phones around the world. According to the report, "Spyhide's database contained detailed records of about 60,000 compromised Android devices, dating back to 2016 up to the date of exfiltration in mid-July. These records included call logs, text messages and precise location history dating back years, as well as information about each file, such as when a photo or video was taken and uploaded, and when calls were recorded and for how long."

TechCrunch analyzed the data and concluded that Spyhide is gathering data on every continent, with primary efforts focused on Europe and Brazil.

The Vendetta Package

The services offered by hackers-for-hire have become more sophisticated and fees have certainly risen since 2014, when FBI agents arrested Zachary Buchta, then only 17 years old and charged him with conspiracy. Part of hacker groups called LizardSquad and PoodleCorp, Buchta was responsible for DDoS attacks and other malfeasance, including online harassment and attacks for $20 each. He was sentenced to a fine and prison time after pleading guilty to one count of conspiracy to commit damage to protected computers

Today, in the web's darkest corners, malicious actors offer personalized digital attacks for prices between $1,500 to $2,500. This 'service' promises total chaos and the potential to disrupt an individual's life. But remember, these are shady operators - can you really trust them? No. And let's not forget the very real possibility of walking into a law enforcement trap.

The Cybercrime Boom

Our shared examples touch on the sprawling underground economy driven by Cybercrime as a Service. With the proliferation of hacking tools, botnet rental operations, and even hacker training courses on the dark web, it's no surprise that this illicit industry is booming. According to Forbes, there is a relationship between the increase in cybercrime and the increase in remote work spurred by the pandemic. Remote and hybrid employees are less likely to take recommended security precautions, often working outside of normal office hours and using unprotected personal devices for work tasks. Compounding the work-from-home issue is the widespread use of contractors, who work without supervision and are often less invested in company security.

Experts recommend that businesses take steps, including upgrading hardware and software and implementing mandatory two-factor authentication to protect themselves from hackers. Individuals would be well-served to heed the same advice.

Final Thoughts

This grim reality serves as a powerful reminder of the critical need for cybersecurity readiness. The old adage rings true - prevention is better than cure. Particularly when cybercrime comes cheaper than cybersecurity, yet the damage it wreaks on businesses and reputations can be crippling. The need for security-minded individuals and organizations has never been more crucial.

About the Author

Nik Hewitt is the Sr. Content Marketing Manager at TrueFort, the leading lateral movement protection platform. He is a BAFTA-winning digital storyteller with nearly three decades of experience in digital content creation and IT/cybersecurity journalism. Now living in rural Ireland, he has worked with some of the world’s largest cybersecurity providers. Currently thriving with the team at TrueFort, Nik is a committed advocate for workplace equality and a champion for the use of AI in digital marketing

Nik can be reached online at www.linkedin.com/in/nikhewitt and at https://truefort.com/

Ushering in the Next Phase of Mobile App Adoption: Bolstering Growth with Unyielding Security

By Alan Bavosa, VP of Security Products, Appdome

In recent years, mobile apps have surged in popularity providing consumers with instant access to a variety of life essentials such as finances, education, and healthcare to life's pleasures such as shopping, sports, and gaming. In fact, a recent study titled "United States Consumer Expectations of Mobile App Security," revealed a significant shift, with approximately two-thirds of Americans now preferring the use of mobile apps over more traditional web channels, ushering in a new dominant channel for brands to connect with consumers.

With the popularity of mobile apps reaching new heights, the responsibility to protect mobile users against diverse security threats has become paramount as the attack landscape shifts focus to where most consumers are – mobile apps. And it's evident that consumers expect and demand protection when using mobile apps, and they are not willing to compromise. For example, when asked to rank the priority of security vs features, an overwhelming majority of U.S. consumers, say that security is equal to or higher in importance than features.

Not only is the level of protection that consumers expect in mobile apps is also on the rise. For example, when consumers were asked what type of protection, they expect mobile brands to provide when using their app, 72.7% of U.S. consumers said that they expect either "the best protections" available, or protection of the login and data, as well as protection against malware. Taken together this clearly underscores the pressing need for mobile app developers to deliver enhanced protection in their mobile applications.

To help mobile developers and cyber-security teams wrap their heads around what this means, this article will illustrate both the new and emerging threats mobile apps face, along with the "tried and true" threats and attack methods that hackers have been using for years. Combined, this will give mobile developers a blueprint that will enable them to craft a strategy that addresses these threats head on and deliver the protections that their mobile customers demand.

Emerging Threats:

Accessibility Service Malware

In recent years, there has been an emergence of malware specifically created to exploit the Android Accessibility Service framework which allows bad actors to gain unauthorized access to in-app events, steal personally identifiable information (PII), perform or even hijack transactions and evade detection. Notable examples include FluBot, Teabot, PixPirate, Brasdex and Xenomorph. Mobile banking apps often fall prey to these attacks, which monitor Accessibility Service events and user activity to harvest transactions, PII, and other valuable data.

Screen Overlay Attacks

A screen overlay attack is another tactic used by cybercriminals that has become more prominent. In this technique, part of the app screen is covered by a fake and malicious screen that the user is tricked into clicking on or interacting with to commit mobile fraud. Victims of this attack think they are interacting with a legitimate app or service, but they are actually interacting with the overlay screen controlled by the attacker which can put PII, transactions and other sensitive data at risk. A classic example of this type of attack is the Cloak & Dagger, with more recent variants including Strandhogg and others.

Credential Stuffing

Credential stuffing poses a major risk to mobile banking apps and developers should take note with 4.8 billion people projected to use mobile wallets by 2025. This attack method involves automated injection of breached username/password pairs to fraudulently gain access to user accounts. Attackers employ automation to send large numbers of properly formatted but random username/password pairs into a targeted system until a match to an existing account is achieved. Once a match is found, the next step of the breach can be executed, effectively taking over the victim's account.

Traditional Threats

Malicious Reverse Enginering – Static and Dynamic

The very first layer of defense in any mobile app security strategy should consist of hardening or "shielding" the app by implementing basic runtime application self-protection (RASP) measures like anti-tampering, anti-debugging, anti-reversing, and preventing emulators or other virtualized environments.

Lack of Obfuscation

Code obfuscation makes it difficult for attackers to understand an app's source code and control flows. Hackers use open source, freely available disassemblers, decompilers and debuggers to reverse engineer mobile apps and understand the source code. With this information, they can craft more successful attacks.

Even more skilled cybercriminals can use dynamic instrumentation toolkits such as Frida to attach to running processes, hook into applications remotely, and dynamically inject code into memory during runtime, allowing attackers to alter an app's behavior, functionality, logic, and state — all while the app is running. Plus, these tools can help them cover their tracks to remain undetected.

Weak or Insufficient Encryption

The next major area of concern is a general lack of sufficient data encryption in mobile apps. Most apps employ weak or insufficient encryption, and some ignore encryption altogether for data stored in the code. This often includes extremely sensitive API keys and secrets stored in the clear as strings in the app, which would allow for easy extraction or interception of usernames and passwords, both stored in the app, as well as when they traverse a network, such as when a user logs in to a mobile banking app. Other places where we find an abundance of unprotected data are app preferences, XML strings, and app resources.

You might expect that this data would be encrypted by default. Simply put, it's not. Encrypting data can complicate sharing authentication and authorization with back-end servers and other apps, which degrades the user experience if encryption breaks it. Plus, there are a dizzying number of choices to make in terms of key size/strength, key derivation technique, cipher strength, and encryption algorithms. Every one of these choices can have a dramatic effect on performance and security if it is wrong.

As a result, in the name of releasing apps quickly and delivering a smooth user experience, these critical areas of mobile app security are often given short shrift. The consequences, though, can be dire. These security deficiencies enable hackers to take over accounts, compromise financial transactions, conduct screen overlay and man-in-the-middle attacks, inject code remotely, and create Trojans that look and feel like the real thing.

Man-in-the-Middle Attacks

Man-in-the-Middle Attacks (MitM) often target mobile apps belonging to the service, finance, and retail industries. Hackers place themselves in between the mobile user and the remote service or server that the user is trying to reach. These two trusted parties believe they are conversing with one another but are communicating with the hacker. This attack allows bad actors to gain unauthorized access to passwords, credit card, contact, and loyalty account information.

Combating Attacks

To secure mobile apps from the above-mentioned threats, implementing a multi-layered security model is crucial. Having a multi-faceted security approach that is both proactive and reactive can, not only prevent attacks, but quickly detect and remediate the threat before harm is done. Organizations should pivot towards embedding security at the very start of the development lifecycle. Leveraging no-code tools empowers them to do just this by better operationalizing mobile app security in the CI/CD pipeline and taking an engineering approach to DevSecOps. By doing this, developers can leverage tools that provide mobile development and cyber teams with comprehensive, automated systems to build, test, release and monitor security defenses and protections directly into iOS and Android apps during the app development process.

As mobile apps continue to be the apple of U.S. consumers' eye, serving as a gateway to brand relationships, Americans have a growing appetite for advanced protection from malware, hacking, fraud, and other destructive cyber actions.

Not only do consumers value security as much or more than new features, 51.2% want the best protection possible. To achieve this, developers and cybersecurity professionals need to work together with a mobile-first mindset to ease any concerns Americans may have with their mobile apps.

Security is materializing as the next driving force for mobile app adoption, serving as a pillar for a successful transition into the mobile realm. Those businesses that ignore this will not only do a disservice to their customers but will be left behind as it evolves into a fierce battleground among companies in all industries. Embracing security as a fundamental element is not just a necessity, but a strategic imperative to thrive in the enter-evolving landscape of mobile technology.

About the Author

Alan Bavosa is the VP of Security Products at Appdome, the leading pioneer in no-code, automated mobile app defense. He is passionate about helping mobile developers build secure mobile apps rapidly as part of the DevOps CI/CD pipeline. Prior to Appdome, Alan held numerous executive and entrepreneurial roles at leading cybersecurity firms including ArcSight, NetScreen, and Palerra as well their respective acquirers HP, Juniper, and Oracle. Alan can be reached online on LinkedIn, Twitter, and at our company website https://www.appdome.com.

Why It’s More Important Than Ever to Align to The MITRE ATT&CK Framework

By Michael Mumcuoglu, CEO & Co-Founder, CardinalOps

As we approach the second half of a year punctuated by ransomware and supply chain attacks, a top concern on nearly everyone’s mind is security budgets. A closely-related topic is management-level reporting. With strong economic headwinds, how do we effectively report our security posture to executives and boards in order to demonstrate effective use of our limited resources?

A big part of this is rethinking how security executives approach reporting. Typically, the report to the board has been around metrics like mean time to detect (MTTD) and mean time to respond (MTTR). However, MTTD and MTTR metrics only describe how good your team is at responding to attacks after you have detected them, but they’re missing critical information about which attacks were never – and will never be – detected in the first place.

These missed attacks often stem from either hidden gaps in detection coverage — or due to alerts that got buried in a sea of noisy alerts and were never even pursued by the Security Operations Center (SOC) team.

According to IDC, 20-30% of all alerts are simply ignored or not investigated in a timely manner, frequently due to classic "alert fatigue" caused by too many noisy alerts.

Another disadvantage of MTTD and MTTR metrics is that they don't give management an accurate representation of risk to the business. Instead, we should be looking at metrics that describe the organization's readiness to detect Tactics, Techniques, and Procedures (TTPs) that target business-critical systems such as cloud applications, or crown jewel assets such as databases with PII and other sensitive data. In other words, we need to be able to report on the organization's detection posture.

Why prevention is insufficient

A key tenet of security is that you cannot effectively prevent all attacks. The current thinking is that our mindset needs to shift from prevention to rapid detection and response. In fact, according to Dr. Eric Cole, a well-known SANS Fellow and security consultant, prevention is ideal, but detection is a must.

Our constantly-expanding attack surface is part of the challenge. One report found that enterprise cyber assets have increased by 133 percent year-on-year, from an average of 165,000 in 2022 to 393,419 in 2023. With that many assets to defend – including cloud assets like containers that don't even support EDR agents – you are setting yourself up for failure by trying to prevent every attack. But where do you begin?

Following the roadmap

Enter the MITRE ATT&CK framework. The framework extends the traditional intrusion kill chain model to go beyond IOCs (like IP addresses, which attackers can change constantly) in order to catalog all known adversary playbooks and behaviors (TTPs).

As the standard framework for understanding adversary behavior, MITRE ATT&CK now describes more than 500 techniques and sub-techniques used by threat groups such as APT28, the Lazarus Group, FIN7, and LAPSUS$.

According to ESG research, 89% of organizations currently use MITRE ATT&CK to reduce risk for security operations use cases such as determining priorities for detection engineering, applying threat intelligence to alert triage, and gaining a better understanding of adversary TTPs.

Another advantage of MITRE ATT&CK is that it provides a common language to communicate about attack behaviors across internal security teams (threat hunters, red teams, detection engineering, etc.) as well as across organizations (like ISACs).

As a result, tracking MITRE ATT&CK coverage is an ideal metric to track and report on your organization's detection posture.

The inherent challenges

Despite the benefits of MITRE ATT&CK, many organizations find it challenging to measure their detection coverage and address the highest-priority coverage gaps that can lead to breaches.

In fact, based on our data-driven research analyzing more than 4,000 rules across diverse SIEM platforms in production environments — including Splunk, Microsoft Sentinel, IBM QRadar, and Sumo Logic – enterprise SIEMs are typically missing detections for 76% of all MITRE ATT&CK techniques used by adversaries. Put another way, using MITRE ATT&CK v13 as the baseline, they are blind to around 150 techniques used by adversaries.

Is it lack of caring that prevents organizations from ensuring they have the right detections in their SIEMs? Absolutely not. The simple truth is that effectively managing SIEMs is incredibly complex. New log sources are constantly being added and detection engineers find themselves struggling to keep up with the latest vulnerabilities and changes in their attack surface. Plus they constantly find themselves scrambling in a reactive mode after successfully being attacked by Red teams and penetration testers.

These challenges are compounded by the biggest challenge: finding and retaining skilled detection engineers, especially when organizations are at the same time adopting newer SIEMs – such as cloud-native SIEMs with unfamiliar query languages – to reduce data ingestion costs.

What needs to happen: focus on streamlining detection engineering processes

Automation is widely-accepted as a top priority for improving the effectiveness of the SOC, but until now it has only been applied to other areas besides detection engineering, such as incident response (with SOAR) and anomaly detection (with behavioral analytics).

In fact, in most organizations, detection engineering tends to be based on highly-manual processes, tribal knowledge, and individual "ninjas" rather than formal, documented workflows enabled by automation.

For example, security teams are often required to manually map detections to MITRE ATT&CK using spreadsheets, which is time consuming and error-prone. And they are responsible for manually identifying existing detections that are broken or misconfigured, due to missing telemetry or other data quality issues, for example (in fact, our research found that on average, 12% of existing detections in production SIEMs are broken and will never fire). Finally they are also responsible for continuously researching the latest exploits and manually developing high-fidelity detections for them.

These are not tasks that require the creativity of a human. In fact, automation is better at these kinds of tasks that are tedious and exhausting for a human practitioner.

Despite the buzz around AI created by ChatGPT, which can create impressive answers to a wide range of questions, automation isn't a silver bullet – but it also shouldn't be discounted either. The future of security is found in the marriage of automation and human creativity. Security leaders will benefit greatly from freeing their security professionals to think creatively and focus on more complex and interesting challenges – such as threat hunting and understanding new and novel attack behaviors – rather than mundane tasks related to managing their SIEMs and tracking their MITRE ATT&CK detection coverage.

Once this is accomplished, CISOs will be well-equipped to answer strategic questions such as "How prepared are we to detect the latest high-priority threats?" and "What is the roadmap for improving our detection posture over time?" And because they will not only be using standard metrics in their response – the metrics will also be achievable, predictable, and based on a thoughtful, threat-informed strategy.

About the Author

Michael Mumcuoglu is the CEO and Co-Founder of detection posture management company CardinalOps. He is a serial entrepreneur that is passionate about technology, cybersecurity, and leadership. Prior to CardinalOps, Michael co-founded LightCyber, a pioneer in behavioral attack detection acquired by Palo Alto Networks (NYSE: PANW) in 2017, where he served as Vice President of Engineering for the Cortex XDR platform. Prior to founding LightCyber and other startups, Michael served in various cybersecurity roles in an elite intelligence division of the Israel Defense Forces.

Michael can be reached online at @xmichaelm and to learn more about CardinalOps, visit https://cardinalops.com/ or follow at @CardinalOps.

EVENTS

4TH CYBER SECURITY FOR ENERGY AND UTILITIES CONFERENCE

6 – 7 SEPTEMBER 2023
SHERATON DAMMAM HOTEL & CONVENTION CENTRE
DAMMAM, SAUDI ARABIA

250+ DECISION MAKERS

25+ SPEAKERS

10+ COUNTRIES REPRESENTED

5+ PANEL DISCUSSIONS

2+ FIRESIDE CHATS

12+ CASE STUDIES AND TECHNICAL PRESENTATIONS

SUPPORTING PARTNERS

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

معادن
MA'ADEN

Eskom | 100 1923-2023

(CS)2AI CONTROL SYSTEM CYBER SECURITY ASSOCIATION INTERNATIONAL

معدنيه
MAADANIYAH

ISACA
Riyadh Chapter

KINGDOM OF SAUDI ARABIA
JUBAIL INDUSTRIAL COLLEGE

2006
جامعة تبوك
University of Tabuk

THE 4TH CYBER SECURITY FOR ENERGY & UTILITIES CONFERENCE

will address the increasing demand for digitalization in the energy and utilities sector. Some of the topics to be discussed will include cybersecurity risk management, incident response, threat intelligence, cloud security, IoT & IIoT as the cybersecurity landscape continuously evolves, giving rise to new trends and threats.

The two-day event will provide a valuable platform for industry experts hailing from the region to convene, exchange knowledge, and actively contribute to enhancing the cyber resilience of their respective industries. Attendees will have the chance to acquaint themselves with cutting-edge practices, innovative technologies, and emerging trends in cybersecurity.

TO LEARN MORE

GET INVOLVED TODAY

Email us directly at partnerships@gmevent.ae or call +971 52 969 7209 and a member of the team will be happy to help.

cybersecurityksa.com

SCAN THE QR CODE

CYSEC UAE-23
7th EDITION

7TH GLOBAL EDITION OF CYSEC GLOBAL SERIES

ORGANIZED BY
MAK

CYSEC UAE 2023

EXCLUSIVE CYBER SECURITY SUMMIT

20 SEPT, 2023 | CONRAD ABU DHABI ETIHAD TOWERS - ABU DHABI, UAE

FEATURED SPEAKERS

25+ SPEAKERS TO TAKE THE STAGE AT CYSEC UAE SUMMIT 2023

DR. LT. COL. HAMAD KHALIFA AL NUAIMI

Head of Telecommunication Infrastructure Dept.

ICT Center,
Abu Dhabi Police GHQ

AHMAD M.D. ALI AL EMADI

Department Head of Cybersecurity & Innovation

Nakheel

AHMED NABIL MAHMOUD

Head of Cyber Defense Security Operations

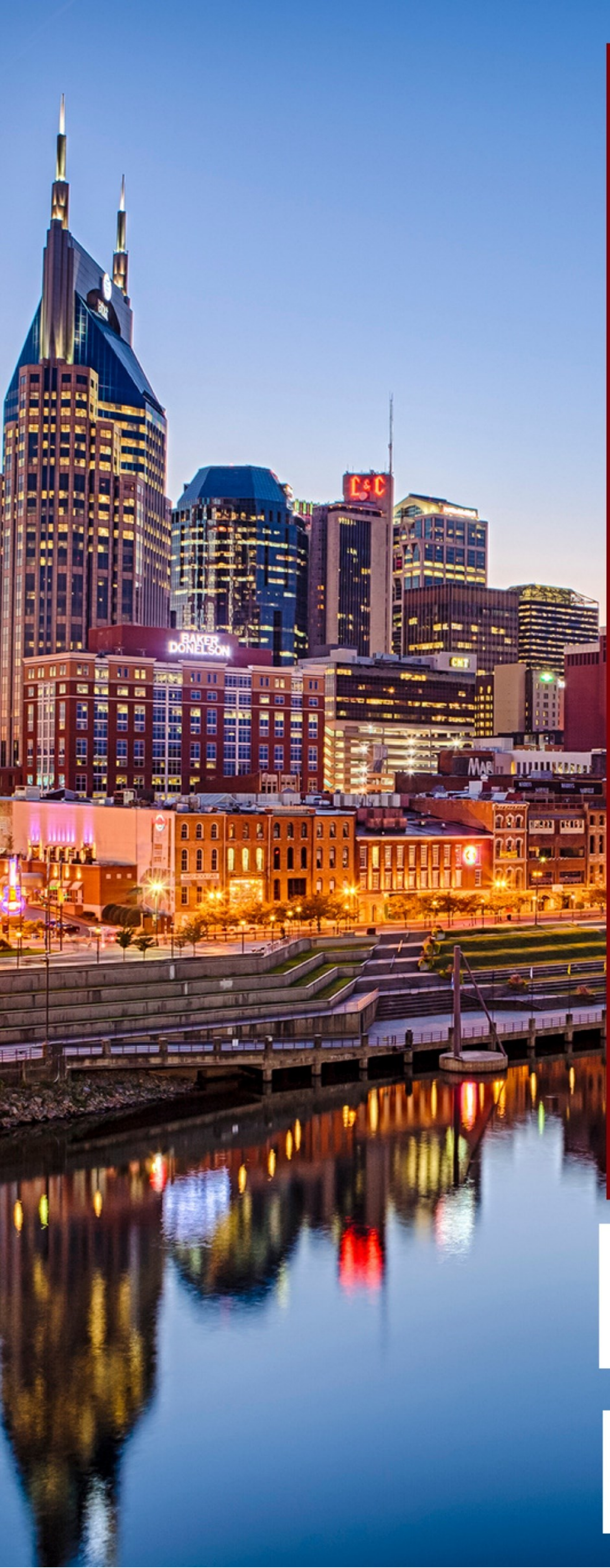
ADIB
Abu Dhabi Islamic Bank

- Embracing Next-Gen Cyber Resilience To Drive UAE's Digital Agenda Forward
- 120+ IT Security Leaders & Government Authorities
- 1:1 Networking
- Keynotes & Panels
- Cyber-Tech Exhibition

SCAN ME

FOR MORE

Info@cysecglobal.com
+971 50 376 1665



Data Manag

THALES
Building a future we can all trust

pepsi
NextgenID
Identity Starts Here

NSS

20
YEARS

AVAR 2023

26TH INTERNATIONAL CYBERSECURITY CONFERENCE

SECURE ECOSYSTEM: STRATEGIC, PRAGMATIC, FUTURISTIC

28 NOVEMBER – 1 DECEMBER 2023 | DUBAI

Call for Papers

Last Date for Submission: 12 August 2023

Share Your Research with the International Cyber Security Community!

Submit Your Abstract On

- Cyber Forensic Investigations
- EDR/XDR Evasion Techniques and Mitigations
- 0-days and High-Impact Vulnerability Exploitation
- ML and Big Data in Cyber Security
- Threat Intelligence Based Protection
- Offensive Security Techniques
- Supply Chain Attacks
- Cyber Espionage and APT Groups
- Latest Mobile Malware
- Mac Malware TTPs and Analyses
- UEFI Security Compromise
- Attacks on IoT/OT Infrastructure

...or any other threat research of interest to cyber security practitioners.

Your Audience at AVAR 2023

CEOs | CTOs | CSOs/CISOs | Regulators
Law Enforcement Agencies | Academia

Submit Your Abstract

www.aavar.org

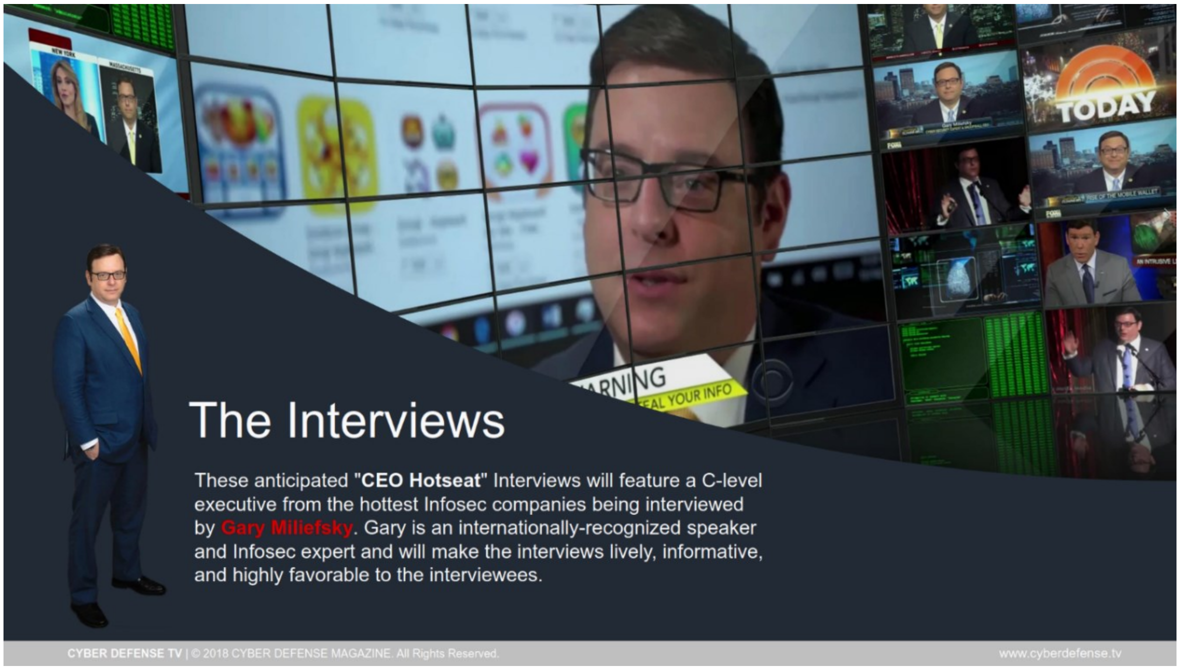
CYBER DEFENSE TV

INFOSEC KNOWLEDGE IS POWER

CyberDefense.TV now has 200 hotseat interviews and growing…

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

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



The Interviews

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

CYBER DEFENSE TV | © 2018 CYBER DEFENSE MAGAZINE. All Rights Reserved. www.cyberdefense.tv

Copyright (C) 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

Cyber Defense Magazine

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

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

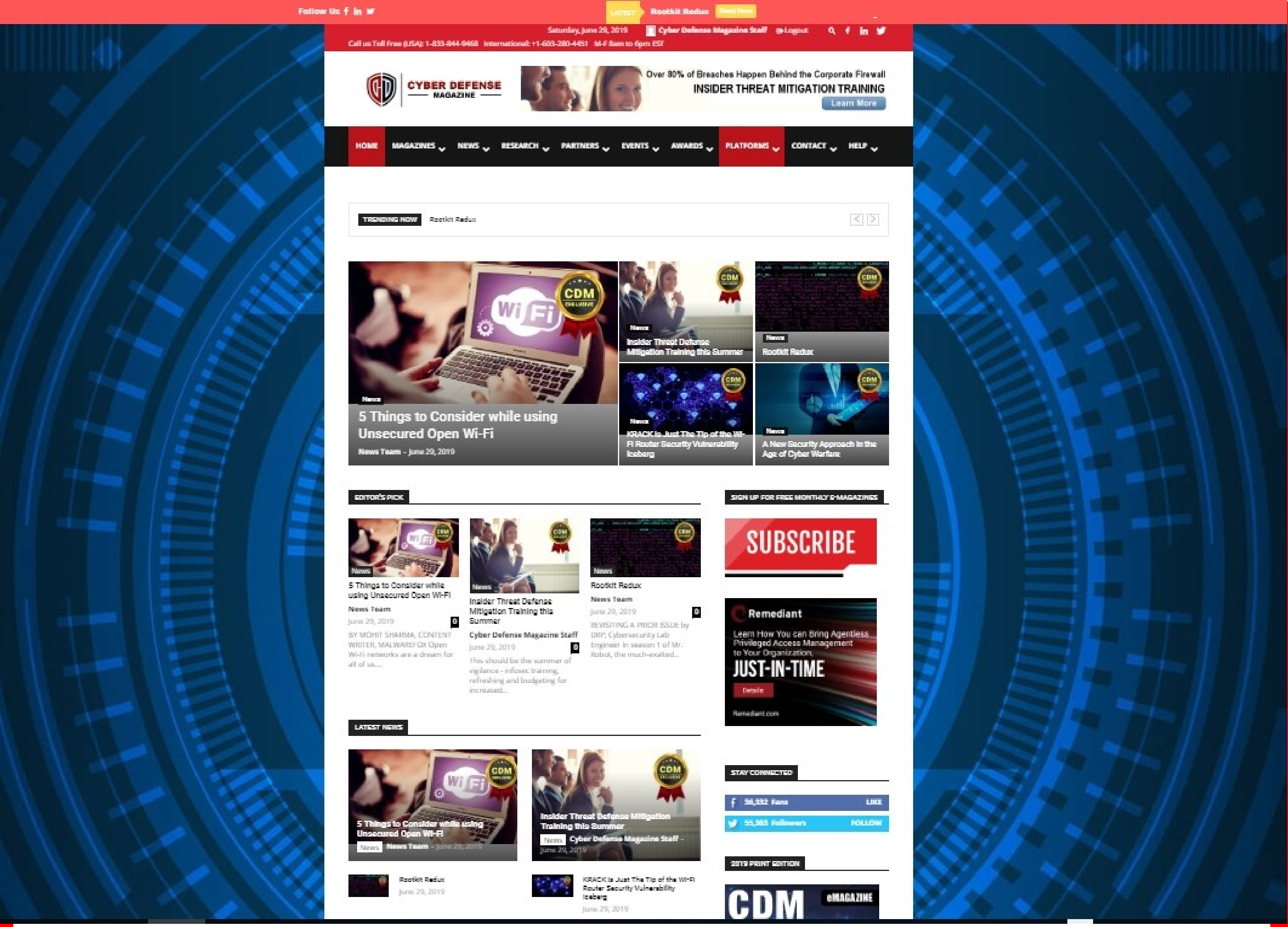
All rights reserved worldwide.

marketing@cyberdefensemagazine.com

www.cyberdefensemagazine.com

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

Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 09/01/2023



Follow Us

LATEST Rootkit Redux Read Now

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

CYBER DEFENSE MAGAZINE

Over 80% of Breaches Happen Behind the Corporate Firewall
INSIDER THREAT MITIGATION TRAINING
Learn More

HOME MAGAZINES NEWS RESEARCH PARTNERS EVENTS AWARDS PLATFORMS CONTACT HELP

TRENDING NOW Rootkit Redux

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 Redux

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 Redux
News Team
June 29, 2019 0
REVISITING A PRIOR ISSUE by DRP, Cybersecurity Lab Engineer In season 1 of Mr. Robot, the much-exalted...

SIGN UP FOR FREE MONTHLY E-MAGAZINES

SUBSCRIBE

Remediant
Learn How You can Bring Agentless Privileged Access Management to Your Organization,
JUST-IN-TIME
Details
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 Redux
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

55,305 Followers FOLLOW

2019 PRINT EDITION

CDM eMAGAZINE

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

CBS NEWS
abc
AS SEEN ON TV
CNN
FOX NEWS channel
NBC
FOX
MSNBC
USA TODAY
Inc.
The New York Times
Bloomberg NEWS
The Washington Post
FOX BUSINESS
BusinessWeek
YAHOO!
Forbes
Entrepreneur
REUTERS
The Boston Globe
ALWAYS FREE
NO STRINGS ATTACHED

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