CYBER DEFENSE MAGAZINE

eMAGAZINE

SEPTEMBER 2022

In This Edition

Critically Important Organization?

Federal Progress On Zero Trust: A Report

Information Warfare and What Infosec Needs to Know

…and much more…

MORE INSIDE!

CONTENTS

@MILIEFSKY

From the

Publisher…

We'll be celebrating our 10th Year in business, Young Women in Cybersecurity and our Top InfoSec Innovators, Black Unicorns and Top Global CISO Awards this October at CyberDefenseCon 2022

Dear Friends,

Reflecting on 10 years of cybersecurity knowledge and innovations we love to share with our loyal readers, it seems, when it comes to cybercrime and nation state 'soft and quiet' cyberwarfare, we, the citizens of the world end up dealing with more privacy and identity risks now, more than ever. Breaches and data theft have become daily news. Therefore, our mission of sharing innovation and infosec knowledge remains more important every day. We at CDMG choose to focus on innovative people, processes, products, and solutions in cyber defense that help protect our way of life, our data and our privacy. Our Top InfoSec Innovators in the World competition as part of our annual Black Unicorn awards remains open for entries. All innovative information security companies of any size may apply for this prestigious award. Cybersecurity companies that wish to apply may visit https://www.cyberdefenseawards.com/

In the cybersecurity industry, I coined the term black unicorn as a cybersecurity company that has the potential to reach a $1 billion dollar market value as determined by private or public investment. The Black Unicorn Awards are designed to help showcase companies with this kind of potential. Ultimately, the judging in our awards is tough and it's still up to the finalists and the winners to execute a flawless business model to reach this potential. It takes innovation, dedication, passion – the right team and the right cyber security solution, harmoniously executed to become a unicorn. We continue to seek nominees for our annual young Women in Cybersecurity scholarship program for entries. We have one scholarship open and remaining for the year. Any young woman in high school who will be entering college in 2022/2023 can apply now:
https://cyberdefenseawards.com/women-in-cybersecurity-scholarship-fund-for-2022/
Readers can learn about the prior winners, in 2020, Annabelle Klosterman, here: https://cyberdefenseawards.com/women-in-cybersecurity-scholarship-winner-for-2020/ in 2021, Olivia Gallucci, here: https://cyberdefenseawards.com/women-in-cybersecurity-2021-scholarship-winner/ and in 2022, Veronika (Nikki) Jack, here: https://cyberdefenseawards.com/women-in-cybersecurity-2022-scholarship-winner-1st-of-2/ who each remain an inspiration for other young women to enter the field of cybersecurity.

As in past years, a panel of judges will review each entry and choose one scholarship winner and a backup winner in case there are issues on the winner's college entry in 2022/2023. Now is an excellent time for young women to plan their future careers in cybersecurity. It's a hot field with hundreds of thousands of career openings and unlimited opportunities for those who wish to make a positive impact on today's digital world – with our free https://www.cyberdefenseprofessionals.com/ job site awaiting your visit, today.

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@cyberdefensemediagroup.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:
http://www.cyberdefensemagazine.com/about-our-founder/

10 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 2022 Issue

From the Editor-in-Chief

On behalf of Cyber Defense Media Group and our affiliates, we are delighted to bring you this new issue of Cyber Defense Magazine for September 2022.

We are pleased to recognize our contributing authors and their organizations. We now enjoy a steady stream of submitted articles on a broad variety of cybersecurity and closely related topics of value to our readers.

The growing trends in remote workforce aka work from home (WFH) have created new opportunities and new challenges we will continue to face in the coming years. The movement in Zero-trust is here and it's a journey not a product, service or destination. Cloud security remains a high priority for us and our readership as well. The internet continues to evolve, as you can see from the wonderful content we deliver each month as a thought leadership platform with articles on these and many more relevant subjects in cybersecurity.

As always, we encourage CDM readers to read all articles objectively and reach your own conclusions, especially in this era of freedom of speech issues. If they inspire you to think outside of the box, then we've accomplished our mission each month, to help you find new ways to get one step ahead of the next potential breach.

Wishing you all success in your cybersecurity endeavors,

Yan Ross
Editor-in-Chief
Cyber Defense Magazine

About the US Editor-in-Chief

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


SPONSORS

CYBER DEFENSE CONFERENCES

THREE EVENTS IN ONE

Orlando, Florida, USA | October 27-28, 2022

One of the most exclusive, fun and educational CISO conferences of the year!

Limited to our selection of the top 100 CISOs in the world, amazing speakers and insider threat mitigation training by a world reknown expert - meets 100 top cyber defense companies in an intimate, high value two day summit

www.cyberdefenseconferences.com

CionSystems

Next Generation Enterprise Identity Management (EIM)™

THE SECRETS OF HARDENING ACTIVE DIRECTORY

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

GET YOUR FREE eBook

Get https://cionsystems.com/

plainID
THE AUTHORIZATION COMPANY

Power of the Policy

Move to an Identity-First Security paradigm.

Download the eBook


DATATRIBE
CYBER STARTUP FOUNDRY
Forging dominant companies from nation-state domain expertise
CAPITAL | RESOURCES | GUIDANCE | SUCCESS
HOME TO THE WORLD'S FASTEST GROWING CYBERSECURITY AND DATA SCIENCE COMPANIES
attila SECURITY
DRAGOS
ENVEIL ENCRYPTED VEIL
INERTIALSENSE
PREVAILION
the cyberwire
refirm labs
BlueRidge.ai
STRIDER
CodeDx
BLACKCLOAK™
SightGain
JOIN THE TRIBE
DATATRIBE.COM

Is your AI Secure?

BOSCH

Widespread AI adoption has profoundly exposed AI/ML models to adversarial attacks. Hackers can subvert AI/ML systems causing financial loss, reputational damage, loss of competitive advantage and intellectual property theft.

> **It's hard to patch or mitigate what you can't find**

Bosch AIShield

Cybersecurity solution for your AI assets

An industry-first, ready-to-deploy and production-optimized solution to secure AI systems against adversarial attacks such as model extraction, model evasion, data poisoning and model inference attacks

www.boschaishield.com

Consulting

Consulting led AI security impact assessment & mitigation plan

Services

Customized enterprise implementation service for AI security

Product

Leverage AIShield API every time a new AI/ML model is deployed or changed

+91 8951989144

AIShield.contact@bosch.com

Bosch Global Software Technologies
alt_future

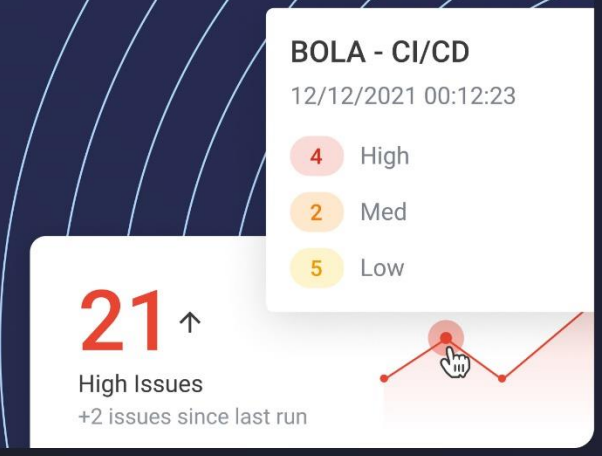
noname

The Complete, Proactive API Security Platform

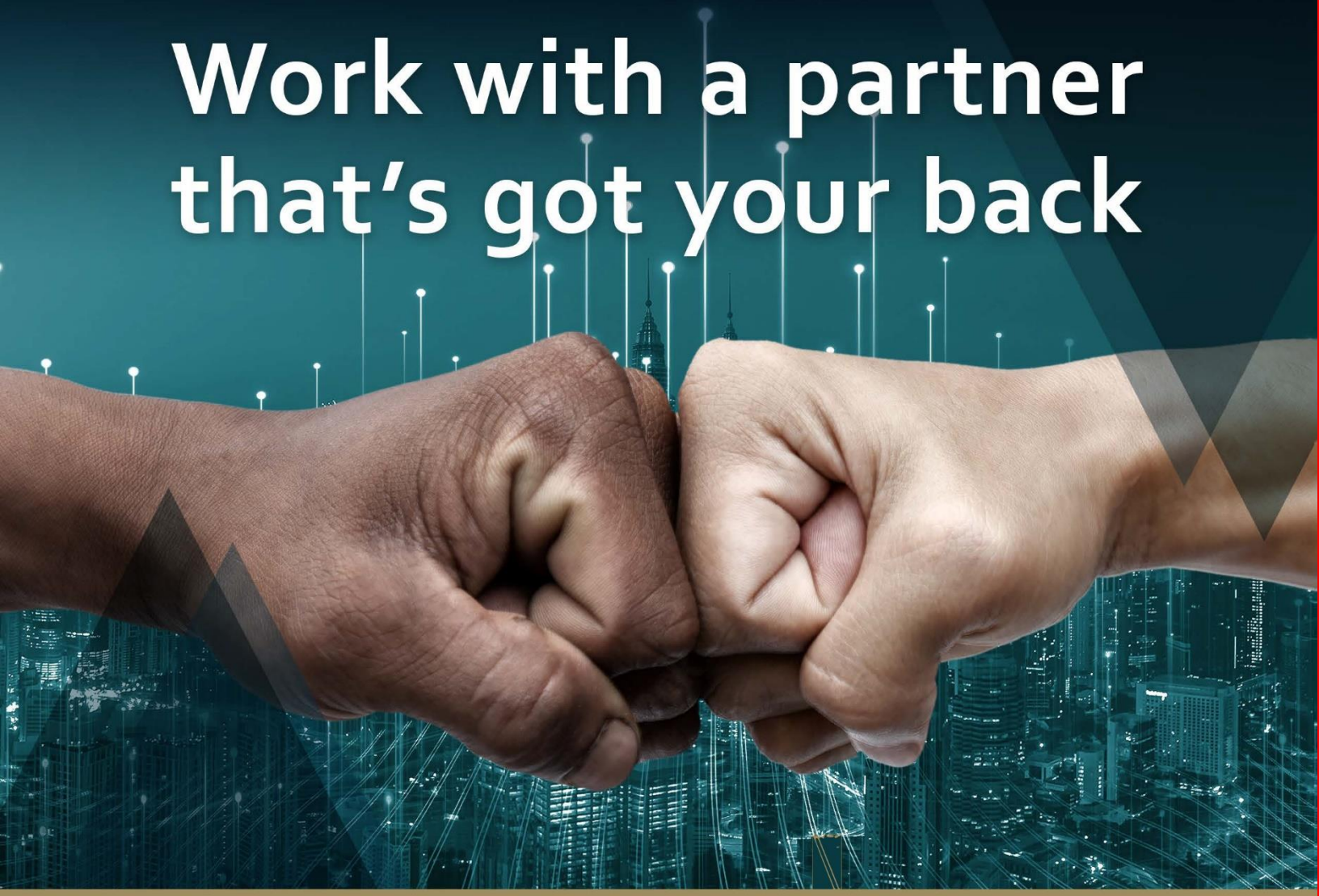
nonamesecurity.com >

Shift Left with **API Security Testing**

Industry-leading posture managment, runtime security and API security testing



Work with a partner that's got your back



Up Your Security Game

WITH A PARTNER 100% COMMITTED TO MICROSOFT SECURITY

MANAGED SIEM - powered by Microsoft Sentinel

MANAGED EDR - powered by Microsoft Defender for Endpoint

MDR FOR IT - powered by Microsoft Sentinel and Defender XDR Platform

MDR FOR OPERATIONAL TECHNOLOGY (OT) - powered by Microsoft Sentinel & Defender for IoT/OT

ADVANCED VULNERABILITY MANAGEMENT - powered by Microsoft Defender TVM

MICROSOFT SECURITY PROFESSIONAL SERVICES - Design, Implement, Configure & Optimize

DIFENDA

CONTACT A DIFENDA SECURITY EXPERT TODAY

Microsoft Partner

Microsoft

Gold Security
Gold Cloud Platform
Gold Application Development
Advanced Specialization - Threat Protection

Member of
Microsoft Intelligent Security Association

Microsoft

MYTH

Data can't protect itself from ransomware criminals.

FACT

Now it does! No matter where it goes in the world,
who has it or how many copies exist.

DATA ITSELF IS NOW ITS OWN FORTRESS

Learn more at Keyavi.com

keyavi

Making data self-protecting, intelligent and self-aware

Join the conversation!
#TransformCybersec, #TransformingCybersec

Transform your datasecurity strategy
with the power of Keyavi.

Download your free whitepaper

How People, Processes, and Technology Shape the Future of Cyber Security

By Milton Security

Start my **FREE** 15-day POV

In 2016, Gartner released their top 10 technologies for information security,[1] containing Intelligence-driven Security Operations Centers, which would shift the paradigm of threat detection and response by incorporating adaptive architecture and context-aware components. At this time, detection and response budgets were 30% of overall security budgets and were expected to double by 2020 because no amount of preventative security controls were able to catch all intrusions or attempts.[2]

These two reports paved the way for organizations to understand this dichotomy - the security of an organization can not rely solely on humans or tools. Milton Security has been preaching (and practicing) this shift since 2007 through Dynamic Threat Hunting. Dynamic Threat Hunting occurs when creative, human Threat Hunters are enhanced by AI/ML. Pair that with deep threat intelligence, telemetry, and billions of daily messages and you have an intelligent, context-aware, and just-in-time security operation to your organization protected.

Standing up a Dynamic Threat Hunting Team internally could lead to a few possible outcomes:

- Take decades to get it right, all while leaving your network vulnerable to threat actors;
- Completely burn out and decimate your team with data deluge; OR
- Increase your security budget to that of Amazon3 and still see threat groups slip through.[3]

In 2017, Gartner's principal research analyst Sid Deshpande wrote, "The shift to detection and response approaches spans people, process and technology elements and will drive a majority of security market growth over the next five years." Mr. Deshpande realized that PPT is essential to the future of cyber security, which is why Milton Security, over the last 15 years, has combined these three elements to pave the way in becoming the leader in Dynamic Threat Hunting. Sure, you could go at this alone and struggle with the three outcomes listed above, or you could sign up for a free 15-day Proof of Value trial from Milton Security and see for yourself how effective our Dynamic Threat Hunters are in protecting your brand.

About Milton Security

Milton Security is the global leader in Dynamic Threat Hunting. For over 15 years, Milton's team of Threat Hunters have stopped hundreds of thousands of threats and assisted organizations in protecting themselves around the clock. Milton focuses on the best combination of AI, ML, and Humans, to zero-in on threats, assist with remediation and incident response activities, and keep your brand protected.

1. https://www.gartner.com/smarterwithgartner/gartners-top-10-technologies-for-information-security
2. https://www.gartner.com/en/newsroom/press-releaes/2016-06-06-gartner-says-by-2020-60-percent-of-digital-businesses-will-suffer-major-service-failures-due-to-the-inability-of-it-security-teams-to-manage-digital-risk
3. https://blog.twitch.tv/en/2021/10/15/updates-on-the-twitch-security-incident/

Stony Lonesome Group

MISSION FOCUSED INVESTING

EST 2011

Founder & Managing Partner

SEAN DRAKE

U.S.ARMY

"At Stony Lonesome Group, we believe that Freedom Is Not Free and we do not take it for granted. SLG is a pioneer and thought leader in Mission Focused Investing protecting American Exceptionalism and National Security by investing in a vital areas of Cybersecurity, Big Data Analytics, and Artificial Intelligence. "

Sean Drake
Managing Partner
Stony Lonesome Group LLC
203-247-2479
www.stonylonesomegroupllc.com

Database Cyber Security Guard

Don't be the next data breach. Equifax paid $575 million, British Airways $230 million and Marriott $124 million in fines.

Prevents confidential data theft by Hackers, Rogue Insiders, Phishing Emails, 3rd Party Cyber Risks, Dev Ops Exploits and SQL Injection Attacks.

Product Features

- Detects Informix, MariaDB, MySQL, Oracle, SQL Server and Sybase data theft within milliseconds and shuts down Hackers immediately.
- Advanced SQL Behavioral Analysis of the database query activity learns the normal query patterns and detects database data theft.
- View all suspicious database activity and attempted data theft.
- Supports key GDPR compliance requirements. Non-intrusive detection of data theft. Runs on a network tap or proxy server.

Get a FREE COPY now.

www.DontBeBreached.com/Free

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

Critically Important Organization?

Now It Is Critical to Report Security Incidents

By Trip Hillman, Partner, IT Advisory Services, Weaver

Reporting cybersecurity attacks and ransomware payments will no longer be optional for certain businesses under a new federal law. The Cyber Incident Reporting Act of 2022, signed into law by President Biden on March 15, 2022, mandates that covered entities inform the Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours of a 'significant' cyber incident. CISA will analyze reports from covered entities and produce and distribute anonymized bulletins to government agencies and key technology and cybersecurity companies, hopefully in time to prevent other businesses from falling victim to similar attacks. Additionally, ransomware payments will need to be reported within 24 hours.

With the enactment of this law, one key takeaway for organizations is the overall change in tone from 'you should report…' to a 'you will report.' However, key aspects of how this will play out, such as the necessary content, method for reporting, reporting distribution and retention and process for amending or recalling submissions have been left for CISA to determine. This gives CISA the flexibility to adjust and revise rules as new threats appear and existing ones evolve rather than having to wait for Congress to enact new legislation.

To date, CISA has not released specific information about the nature of cyberattacks to be reported, but the agency has indicated that it will expand the traditional definition of 'critical infrastructure' to include at a minimum 16 Critical Infrastructure Sectors defined in a 2013 Presidential Policy Directive:

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food & Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Transportation Systems
- Water and Wastewater Systems

To further define the industries covered, several sectors include subsectors. For example, the commercial facilities sector includes seven subsectors covering, among others, casinos, stadiums, retail centers, and malls under the rationale that they constitute "sites that draw large crowds of people," but without defining what "large" is. Other sectors define covered activities instead of relying on subsectors.

Together, the 16 Sectors represent a significant expansion of what was once considered critical. For instance, they cover the entire food supply chain from farms to restaurants and grocery stores, water and electric utilities, retail banking, and telecommunication networks, including internet access providers and cell phone networks. The law gives CISA wide latitude to expand the list of covered entities within and beyond the 16 Sectors, whether it is by adding new covered activities or subsectors to an existing Sector, or adding a new Sector altogether.

Most medium and large businesses may want to review the list of Critical Infrastructure Sectors, publicly available on the CISA's web site. While many covered activities and terms are subject to further clarification, a review of CISA's rational for labelling a sector as critical may help in determining the likelihood that a business will be required to report cyber incidents. To encourage disclosure and assuage concerns about releasing potentially sensitive business data, the law includes protections against legal liability and freedom of information requests for companies that report to CISA.

Organizations that have implemented NIST or another Cyber Security Framework (CSF) should already have processes in place to triage and investigate security incidents, identify external stakeholders, and disseminate relevant information. Once CISA publishes details implementing the act, these organizations will need to update their existing processes to cover areas required under the new law that weren't included in the original framework, including:

- Factors and metrics to consider in evaluating whether an incident is reportable
- Data to be gathered for submission to CISA
- Process to communicate with CISA
- Personnel or roles with responsibilities related to evaluating and reporting an incident

Organizations may need to include a frequent feedback loop in their external communication processes, as it is possible that a cybersecurity event may not become reportable until hours or even days later. An attack may initially appear to fall below the definition of 'significant' per the CISA, only to become significant and reportable upon further analysis or as new facts, such as an unexpected disclosure of data, come to light. Covered entities should implement processes to periodically review attacks deemed insignificant to ensure that a new understanding of the nature and scope of the attack does not elevate it to a reportable cyber incident.

Another important element will be determining when the 'clock starts' for notification. A covered entity is required to report a cyber incident no later than 72 hours after it "reasonably believes" that one has occurred. However CISA defines reasonable belief, communication processes will have to be nimble enough to react quickly to changes related to the understanding of the security incident.

For organizations that do not yet have processes defined for communicating about cybersecurity issues with external stakeholders, government or otherwise, the new law may be the necessary driver to implement an appropriate strategy. Multiple cybersecurity and IT control frameworks such as NIST-CSF, NIST 800-53 v5, ISO27001, or COBIT 2019 provide guidance and examples that help to establish procedures for communicating security incidents in an appropriate manner.

With each new cyber security breach and ransomware attack, the need for a coordinated, substantive response becomes more evident. It remains to be seen whether this new law will live up to expectations, but every organization should monitor developments to see how it will affect their operations. For more information about cybersecurity response plans, contact us. We are here to help.

About the Author

Trip Hillman, CISSP, CISA, CEH, GPEN, GCFE, GSNA

Trip Hillman is a partner in Weaver's IT Advisory practice. Focused on evaluating cybersecurity in a broad range of IT environments, he has consulted with Fortune 100 companies, private equity groups, small enterprises and government entities alike on security and compliance.

Federal Progress On Zero Trust: A Report

Federal Agencies are Making Progress on Zero Trust but Challenges Remain

By Dr. Matthew McFadden, Vice President, Cyber, General Dynamics Information Technology (GDIT)

A little over a year ago, the Biden administration issued the Executive Order (EO) on Improving the Nation's Cybersecurity, which set a common objective for all agencies: adopt security best practices to advance toward Zero Trust Architecture. Zero trust is a cybersecurity framework developed around the concept of "never trust, always verify." It requires all users, whether they are inside or outside an organization's network, to be continuously validated to access applications and data.

Extensive guidance about zero trust implementation followed the EO, including an OMB zero trust strategy memo, technical reference architectures, and the Cybersecurity Maturity Model from the Cybersecurity and Infrastructure Security Agency (CISA).

To assess progress and identify continuing pain points on the journey toward zero trust, GDIT's Cyber Practice conducted industry research by surveying 300 federal leaders (60% civilian and 40% defense) who are influential in the IT decision-making process. The report found solid momentum around zero trust planning, some misconceptions about zero trust, and some anticipated implementation challenges.

Zero Trust Momentum

Seventy-six percent of respondents reported their agency had a formal zero trust plan in place or in the works. Two-thirds said they will meet federal zero trust requirements on time or ahead of the fiscal year (FY) 2024 deadline; another 21 percent will come close to meeting the requirements by then.

Approximately half of the respondents are building their zero trust implementation using CISA's Zero Trust Maturity Model, a roadmap to assist agencies in the development of their zero trust strategies and implementation plans. This model is built around five core pillars: identity, device, network, application workload, and data.

Using the pillars in the maturity model as a framework to assess maturity levels, most respondents reported that they are either currently at a traditional or advanced maturity level; few have reached the optimal level. Respondents are most mature in the data and identity pillars. Nearly all said their top future investment priorities are device protection (92 percent) and cloud services (90 percent). Six in ten believe they will be able to continuously run device posture assessments (e.g., using endpoint detection and response tools) by the end of FY24.

Zero Trust Misconceptions

The survey results also identified some misconceptions about the benefits of zero trust, pointing to the need for continued education about the concept and its implementation. For example, respondents said the top benefit (57 percent) of a zero trust approach is that the right users have the right access to the right resources at the right time, but only one quarter said granular data protection at rest and in transit is a top benefit. In order to provide the right access to data and applications at the right time, agencies must coordinate with internal stakeholders, other agencies, and non-governmental organizations to provide the access that employees need. A granular data protection scheme is required.

Furthermore, less than half (42 percent) of respondents said a top benefit of zero trust is reduction in the cyberattack surface. This is surprising, and it seems to reflect a fundamental misunderstanding of the zero trust concept: Because users are only granted access to the applications and data they need, the impact of any breach is limited. Essentially, micro-perimeters are created around each user's resources; attackers can only go so far.

Zero Trust Implementation Challenges

The survey also highlighted hurdles in the zero trust journey. More than half (58 percent) of respondents said the biggest challenge to implementing zero trust is that existing legacy infrastructures must be rebuilt or replaced. Many of these legacy systems rely on implicit trust, which allows bad actors to gain broad access to agency systems following a breach.

Perhaps not surprisingly, 46 percent said costs are a concern. Replacing legacy systems will require significant investment. At the same time, half of respondents said they are having trouble identifying what technologies they need. This suggests that IT teams are not always collaborating closely with program

managers. Improving collaboration between mission owners and IT teams will ensure stronger alignment between the mission and cybersecurity technology implementation, making it easier to know which tools to choose.

Zero Trust and Agency Missions

The journey to zero trust will be different for every agency. It will depend on the technology that is already implemented, the agency's mission requirements and current cybersecurity posture, agency and contractor staffing, and more.

The survey data suggests that agencies are working to meet the aggressive zero trust implementation deadlines laid out by the White House, but lack of resources and fundamental gaps in understanding may hinder their progress. To overcome these challenges, agency IT teams can:

- Partner with mission owners to understand the impacts of data and services on each mission. Understand what data they rely on, where it lives, and how they use it
- Identify digital assets and how cyber compromise of those assets would affect the agency mission. Prioritize security controls based upon the importance of the asset
- Demonstrate quick wins by optimizing current infrastructure. Identify applications and services that can transition to zero trust through configuration changes and policy updates
- Then, look for incremental zero trust projects that provide the greatest value relative to the mission, regardless of which zero trust pillar they fall under

Zero trust is a not just a cybersecurity strategy, it's also a mission enabler. Its primary value is in improving agency missions by providing data and services to the people who need them, right when they need them. By partnering with mission owners, systems integrators, and taking an incremental approach to zero trust that focuses on the greatest value to the mission, IT teams will ensure not only compliance with zero trust requirements, but also mission success.

Read the full report here.

About the Author

Dr. Matthew McFadden, Vice President, Cyber, GDIT. Dr. Matthew McFadden spearheads cyber strategy for GDIT, leads cyber research and development, and develops advanced cyber solutions for the Federal Civilian, Defense, Health, Intelligence and Homeland Security markets. He represents a cyber workforce of more than 3000+ professionals, 30+ commercial cyber partners and programs supporting some of the largest, cyber missions in the federal government sector.

Information Warfare and What Infosec Needs to Know

By Wasim Khaled, Co-Founder and CEO, Blackbird.AI

Cyberthreats are growing more sophisticated by the day, which in terms means cyber is at the top of every CIOs list. Known as Information Warfare (IW), it is the evolution of cybersecurity which now includes misinformation, disinformation, and mal-information (MDM). It is an imminent cybersecurity threat and the cost of being unable to detect and shut down known and unknown threats can cost large organizations potentially millions of dollars. These risks are driven by a new breed of threat actors who exploit digital media to harm organizations, employees, and executives. In this new risk landscape, Information Warfare attacks may come in parallel with traditional cyberattacks which can further amplify the situation. Platforms that provide a real-time solution to detect and quickly shut down threats are a necessary first step to aid in the defense of every company, corporation, and brand.

The Problem

Disinformation is scary because it's the umbrella threat that amplifies the danger of all other systemic and existential threats. Digital actors can influence and manipulate buying and selling behaviors online, amplifying volatility with incredible speed. A study done by Nature reviews says, "Today, misinformation campaigns can leverage the online infrastructure that is unparalleled in its reach. The internet reaches

billions of individuals and enables senders to tailor persuasive messages to the specific psychological profiles of individual users."

Safety filters don't often work for disinformation and harmful content and legitimate publishers end up demonized on important topics. MDM uses AI as a radical force multiplier and only AI-powered solutions can fight back. Active monitoring of key narratives, key terms, hashtags, and sources used to initially spread MDM and subsequent outbreaks can help them be eliminated quickly.

Current media monitoring tools were built to support marketing and customer support teams and were built to passively listen. Marketers typically use these tools to identify key trends and conversations online by aggregating numbers of likes, shares, mentions, and comments. While these are important criteria when assessing immediate virality, they don't inform or protect a company or brand from the new information risks that exist today. Assessing threats based on volume and engagement, for example, is inherently reactive in nature.

Organizations must build out their information warfare strategy as part of their cyber-first efforts.

What's needed is a real-time solution that takes cyber teams inside trends to determine what's authentic human behavior and what is the work of bots and other bad actors to help mitigate any threats. Using technology or even individuals to analyze data will help companies to understand things like public perception which will show how to drive better strategic actions. Understanding the severity of the risk is a necessary first step to aid in the defense of every company, corporation, and brand.

The Solution

Fighting Information Warfare means having the right platforms, processes, and procedures in place to compete in this rapidly changing environment with a game plan built on the foundation of Detect > Measure > Plan > Mitigate > Monitor. Enterprise software platforms that combine AI-driven narrative intelligence, threat intelligence and impact intelligence can reduce costs overall and potentially save time, money and resources for a brand's public perception, bottom line and almost every other major business indicator.

There are five key parameters used to categorize information dissemination and how to mitigate it:

Narrative: Identify potential threat narratives, storylines, "fake news," and conspiracies on social media and other content

Networks: Determine whether the threat is bot-driven or the work of a coordinated group, with supportive relationships between users and shared beliefs.

Cohorts: Determine group affiliations of threat actors to understand how they have impacted your narrative across sectors.

Manipulation: Detect and gauge the impact of deception and manipulation to prioritize action.

Influence: Surface and measure the impact of harmful actors and trusted voices, who shape conversations

Information Warfare Needs to Be Part of Every Organization Cyber-First Strategy

Cybersecurity revenue is expected to approach $400 billion by 2028. Organizations must deploy automated, real-time contextual awareness, algorithmically evolving threat detection, and rapid narrative identification – all executed with the intent to keep business leaders at least a step ahead of emerging trends and threats. This will allow them to detect, measure, plan and mitigate with greater resolution and speed. Battling a harmful information landscape that is full of unexpected risks but planning and preparing is the way to ultimately prevail.

InfoSec professionals must be aware of the potential consequences of IW attacks and put in place the necessary assets to protect their organizations and networks from exploitation. They should also be prepared to respond effectively when an attack does occur. The problem is clear that these systems and methods are evolving fast and the industry needs to respond in real-time.

Disinformation, left unchecked, can be the single vulnerability that puts modern day organizations in the red by billions. The severity of disinformation problems comes down to the ability to identify a narrative before it explodes and it is now essential to a company's cyber survival.

About the Author

Wasim is the CEO and Co-Founder of Blackbird.AI, He brings with him a lifetime of entrepreneurial acumen combined with a background in computer science and human-interface design. For the past five years he has been deeply entrenched with the disinformation analysis and OSINT community and has studied psychological operations, propaganda, AI methodologies, and defense applications. Wasim has consulted and advised government agencies and companies around the world on the dangers and countermeasures of the escalating information warfare arms race. Prior to Blackbird, Wasim founded LuxMobile, an Inc. 500 Company, earned the distinction of Inc. 500's Asian Entrepreneur of the Year and has built businesses with Fortune 500 clients across e-commerce, manufacturing, logistics, fashion and adtech.

Wasim can be reached online on twitter and LinkedIn profile as well as the company website https://www.blackbird.ai/

3 Cybersecurity Solutions Likely to Gain Traction In 2022 And Beyond

How are recent developments in cybersecurity solutions transforming the business outlook?

By Vinisha Joshi, Team Lead – Content Development, Global Market Insights Inc.

A recent research report by Global Market Insights Inc. claims that the global cyber security market size is anticipated to be worth USD 400 billion by 2027.

Driven by the fast-paced digital transformation of businesses worldwide during the COVID-19 pandemic, the cyber security market is foreseen to grow into a highly profitable investment avenue over the forthcoming years. The robust adoption of digital technologies by businesses brings along its own set of concerns such as cyber threats, wherein a system's vulnerabilities are exploited by malicious bodies to damage or steal data for financial gains.

'In June 2021, there were nearly 78.4 million ransomware attacks worldwide. This implies that about 9.7 ransomware attempts per consumer were made for every business day.'— SonicWall.

Data breaches cost organizations millions of dollars on an annual basis. An IBM and Ponemon Institute report of 2021 depicted that the average data breach costs in 2021 accounted for USD 4.24 million,

recording a 10% hike from 2020 findings. In consequence, organizations have been giving significant importance to their digital security requirements, enabling cyber security market to be the recipient of incredible growth prospects.

The industry is characterized by some highly dependable cybersecurity solutions capable of reducing the prevalence of cyber-attacks in the near future. A gist of the same has been outlined below:

1. Identity Access Management

Identity access management (IAM) is a crucial aspect of cyber security. These systems allow enterprises to manage access to systems, applications, and data, making sure that obtaining sensitive information is only possible for authorized personnel.

Some of the pivotal benefits offered by identity access management systems include increased compliance, reduced risk of data breaches, enforceable security policies, and automated IAM. Propelled by such advantages, cybersecurity leaders are largely opting for new identity access management systems.

To illustrate, in 2022, Thales announced building on its expansion strategy via its acquisition of OneWelcome- a European leader in the fastest-evolving market of Customer Identity and Access Management. The deal, which was worth USD 102.4 million, is estimated to complement Thales' existing Identity services in an attempt to meet the most holistic identity platform in the industry.

2. Cloud Security

Conventional IT security has undergone an evolution owing to the paradigm shift to cloud-based computing, propelled massively by the COVID-19 pandemic. While cloud security is convenient, consistent connectivity requirement calls for new considerations to keep enterprises safe and secure. Cloud security, as an advanced cyber security solution, stands out from legacy IT models offering ample benefits to organizations.

A few of the advantages of incorporating cloud security solutions include high scaling speed, optimum data storage, proximity to other networked systems and data, and end-user system interfacing. To that end, SMEs are now moving towards the deployment of cloud security models to ensure maximum protection against data thefts. This is evident from the below statistics:

- About 94% of the global enterprises are already using a cloud service
- Nearly 50% of enterprises spend more than over USD 1.2 million on cloud services per year
- Experts speculate that the data stored in cloud data centers would potentially exceed 100 Zettabytes by 2025 end

Recently, Fortinet unveiled the FortiCNP solution that would allow security specialists to gather data from multiple cloud environments and optimize security processes. This will help manage risks that take place

while switching to cloud environments. It also works closely with a recently launched AWS solution- Amazon GuardDuty Malware Protection.

3. Virtual Private Network (VPN)

With the coronavirus infection spread pushing people and businesses to work remotely, the chances of data breaches increased exponentially in the last couple of years. This has led to increased adoption of the virtual private network (VPN) solution to make the network secure, maintain anonymity, enhance efficiency, and secure confidential data while using the internet.

As per the Global Web Index Study,

- About 72% of VPN users worldwide access their services on PCs or MACs while IoS or Android mobile devices users are not far behind.
- Close to 69% of VPN users are currently using the services on mobile devices.
- Nearly 34% of internet users utilize a VPN to maintain their online anonymity

These numbers have driven the adoption of VPN at a large scale across different organizations that are leveraging its benefits like improved security, remote access, bypass restriction, minimal cost, and more.

Future of cyber security- ***How would the industry look like in 2022 and beyond?***

The future of cyber security industry may be characterized by escalating technological developments in the field with the introduction of Artificial Intelligence, IoT, or blockchain. In fact, with the proliferating trends of Bring Your Own Device (BYOD) and remote working, the demand for network security solutions is expected to soar to new heights in the coming years. Industry experts anticipate the network security product category to register a CAGR of 15% through 2027.

With the healthcare industry worldwide employing digital systems and progressing towards digitization, the adoption of cyber security solutions would surge considerably in the near future.

About the Author

Vinisha Joshi. A qualified Engineering graduate, Vinisha Joshi takes pride in playing with words. Presently, she pens down insightful articles on business, core industry, technology, and the like. Creativity comes naturally to her, and Vinisha makes sure to effectively combine the same with her technical expertise in the articles she writes.

Vinisha can be reached online at (Email, LinkedIn, etc..) and at our company website https://www.gminsights.com/

5G Technology – Ensuring Cybersecurity for Businesses

By Mohit Shrivastava, Chief Analyst ICT, Future Market Insights

5G network, the fifth generation of the cellular technology is promising to offer faster and better connectivity across the globe. The deployment of the 5G network in different parts of the world is promising a change to end user industries such as IT sectors, manufacturing units of different consumer-based products, automotive, transportation and logistics, automotive and energy & utilities. Thus, the use of the 5G network is augmenting productivity, improving scalability and seamlessly integrating different domains of businesses.

Future Market Insight states that the 5G technology market is expected to register a staggering double-digit CAGR of 71.9% by garnering a market value of US$ 248.4 billion by the end of 2028. The penetration of the 5G network is accelerating developments in telecommunication technologies. Moreover, increasing adoption of Internet of Things (IoT), the growing number of smart technologies along with rapid growth of internet users is overall changing the way 5G network is perceived and used.

5G technology not only helps in improving responsiveness but also helps in increasing the speed of wireless networks. Additionally, the availability of advanced antenna networks along is helping 5G technology to offer 20 GBPS speed to carry and transfer data. The development of smart networks is allowing the emergence of smart homes, cities or towns. Thus, the dependency on 5G technology has increased massively.

Although most end user sectors are planning to maximize the use of 5G technology, the potential of cyber threats has multiplied more then ever. Thus, the same 5G technology that has opened the doors for innovation in technology has invited more cyber threats. Future Market Insight states that the cyber security market is expected to register a CAGR of 10.5% by the end of 2032. This is due to cybersecurity becoming a necessity across IT industries rather than a want.

An increase in incidences of computer intrusion (hacking), denial of services and virus deployment has become a matter of concern for end user industries. This had led to governmental authorities of different countries to invest in cyber security to save their private and important data from being misused. Government regulation on data privacy along with increasing number of data centers are effectively deploying the use of 5G networks to combat cybersecurity threats. This, in turn, not only promises the use of 5G networks for better connectivity but also ensures safety from cybersecurity from threats.

5G Network Services: Securing Internal and External Communications

Telecom operators deploying 5G networks and edge services are constantly at the receiving end of facing cyber threats. This, in turn, affects the confidentiality of data of users and attracts a negative reputation for the company. External and internal threats to cybersecurity are expected to grow owing to the increasing development of IoT devices. In addition, the modernization of telecom operators to hybrid cloud-based architectures has further increased the chances of digital threats in the technology world. Thus, companies are planning to deploy 5G networks to prevent enterprises from cybersecurity threats.

IBM and Palo Alto Networks have collaborated to help operators build secure 5G networks. Through this collaboration, the companies are working together to deliver cyber security solutions to enterprise and telecom customers around the world. The collaboration of these two companies combine various features such as automation spanning multifunction network devices and VNFs, control plane security and container security. Thus, the combination of integrated security services and services designed for 5G networks and eco systems is helping end user industries to combat cybersecurity threats in more ways than one. Furthermore, IBM is working with communication service providers on a “secure by design” strategy that will help in building cybersecurity capabilities for every part of the business.

5G Networks – Protecting Data and Network Intrusion

Penetration of technology in nearly every sector of human life has increased the interconnectivity between various electronic devices, thus, increasing the chances of cyber security threats. Today, data storing and saving have changed drastically. The innumerable options of capturing data and redirecting it has increased cybersecurity threats. Although 5G networks have increased accessibility to information

on a great scale, the newness of the same is giving attackers an opportunity to find loopholes in the network system. Thus, end user industries are looking for solutions that ensure secure exchange of information along with prevention of confidential data. This has led to companies designing solutions that will help companies to combat cybersecurity threats, especially in a network embedded with 5G network.

Although the pandemic helped industries digitalize themselves overnight, the increasing number of cyber attacks became more prevalent. The sudden shift of communication networks along with less to no protection created more chances of cyber threats. But, with the penetration of 5G networks across various end user industries, networks will use artificial intelligence to detect the possibility of threats at an early stage. Artificial intelligence not only protects access points but also all the networks they connect. 5G's intelligent edge solutions have the capability to prevent and detect network intrusion. Moreover, it has the potential to detect anomalous behavior that constantly learns and adapts to the target environment, thus, making 5G technology more reliable.

Advantages of Using 5G Network for Cyber Security Threats

- Low latency – 5G network's low latency has the capability to support augmented reality, artificial intelligence and virtual reality efficiently. This helps in creating transparency between different IoT devices and ensures security of information and confidential data across organizations.
- Securing Cybersecurity Threats - 5G networks are helping tech experts to strengthen existing cybersecurity software. Devices connected with 5G networks have the potential to self-detect suspicious activity and act on the same immediately. Thus, making 5G networks essential for cybersecurity threats.
- High Speed and Increased Capacity – 5G network's capacity to process information at a lightning speed is helping end user industries to understand the potential threats of cybersecurity. Furthermore, most tech companies are using key features of 5G network that can be customized to combat different kinds of cybersecurity threats.

Conclusion – 5G Technology – Enabling Safer Future

In the upcoming years, 5G networks are expected to become more prevalent along with becoming usable across business domains. This will not only help businesses to grow rapidly but also help in deploying workflows, monitoring and controlling solutions at remote locations. Although end user sectors such as healthcare, critical infrastructure and automotive industries are more prone to getting targeted by cybersecurity threats, usage of 5G network not only assures prevention of threats but also detects them at an early stage.

Owing to the aforementioned developments, the popularity of technology in large enterprises is expected to increase with time. Thus, most end user enterprises are looking forward to capitalizing on the use of 5G network. Tech-savvy industries are designing and customizing multiple ways of security networks against cybersecurity threats by maximizing the use of 5G. The increasing importance of cross-industry partnerships along with venture capital investments fuelling the chances of cybersecurity threats. This, in turn, is creating opportunities for the increasing use of 5G networks.

Technological advancements at a global level have surged the use of big data at the end user industries. The increasing penetration of artificial intelligence along with augmented and virtual reality is creating more opportunities for cybersecurity threats. Governments of different geographical locations are investing in cybersecurity and 5G networks, accelerating the overall growth of using 5G to combat threats.

With the innumerable benefits 5G network has to offer, the chances of cyberattacks are bound to increase. But simultaneously, 5G network has the potential to offer security at every level for end user industries. 5G network's immaculate ability to change the dynamics of most end-user industries, especially on the front of preventing threats is making it a reliable source to carry out safe and secure work. Owing to this, the future of security from cyber threats looks safer than ever, thanks to the features 5G network has to offer.

About the Author

Mohit Shrivastava, Chief Analyst ICT, Future Market Insights. Mohit has 10+ years of experience in partnering with globally large enterprises to identify new revenue opportunities in high-growth niche IT markets across Cybersecurity, the Internet of Things (IoT), Blockchain, Telecommunications, Cloud Computing, Big Data & Analytics, Electronics & Semiconductors, and others technology markets. https://www.linkedin.com/in/shrivastavamohit/ and Future Market Insights (FMI), is an ESOMAR-certified market research and consulting market research company. FMI is a leading provider of market intelligence and consulting services, serving clients in over 150 countries; its market research reports and industry analysis help businesses navigate challenges and make critical decisions with confidence and clarity amidst breakneck competition. Now avail flexible Research Subscriptions, and access Research multi-format through downloadable databooks, infographics, charts, and interactive playbook for data visualization and full reports through MarketNgage, the unified market intelligence engine powered by Future Market Insights. Sign Up for a 7-day free trial!

Are Cyber Scams More Common and How Do We Avoid Them?

By Harry Turner, Freelance Writer

Cyber scams seem to become more and more common and are something that you will hear on the news a lot. Furthermore, it isn't just the average citizen that gets scammed. Additionally, there are thousands of businesses that get scammed each day. Internet fraud is very standard and something that everybody should be aware of.

It is easy to become a victim of internet fraud although those from the older generation are more likely to fall for it, and are at greater risk of losing more money. Due to people being afraid of falling for cyber scams, they will likely avoid browsing the internet.

It is time to understand the risks of the internet and what you need to be aware of on the internet. Not only will you educate yourself but you can also educate others.

Avoid Fake Credit Reports

Many credit reports claim to be free but in hindsight, they look to gather your information. You must avoid these at all costs. Additionally, once you have used their “free trial” they will begin to charge you. Ensure that you don’t provide your credit card details.

We advise you to check your credit cards at least once a year, ensuring that you have not been a victim of an internet scam. Furthermore, you need to know how to avoid these particular scams.

It is simple to avoid these scams. All you need to do is avoid social media ads, emails, text messages and pop-up ads offering fake credit reports. There are many websites where you can get a free credit report however, there are many URLs which are very similar to those legitimate websites. Ensure that you are checking these URLs and then you will be safe.

Dating Scams

Living in the digital age, we have become more reliant on it than ever. We rely on it to do our clothes shopping, food shopping, communicate with friends and use it for work. Many people will even use the internet for potential relationships that may lead to possible dating scams.

Yes, dating scams are a thing and it is more likely to happen to women than men. In 2021, over $304 million was lost due to dating scams in the United States. Again, this is common with those who are from the older generation.

There are many different forms of romantic fraud. One of the more common methods is by those who build a fake relationship with someone to the point where they have built enough trust to ask for money. They will usually say that it is down to an emergency which is something that a lot of people fall for. Furthermore, there have been people that will give them access to their accounts, another typical method.

The question is, how do you avoid this? You may think it is easy but many people fall into this trap. Many people will usually use fake accounts and nine times out of ten, they will have few images. Furthermore, you want to ensure you meet these people before giving away any personal information. Don't be guilt-tripped into anything you are unsure of and cut them off when you sense anything dodgy.

Phishing

Phishing is one of the more common cyber scams you will hear of a lot. It is the most common and just as effective as the rest. Furthermore, it is similar to dating scams but more in a friendly way. They will pretend as if they know you or a friend of a friend and just get to know you. They could pretend to be a friend and say that they have a new phone or something along those lines.

There are so many social media platforms where people can pretend to be others. Some platforms such as Facebook now require you to provide an identity card before you create an account. Similar to what betting sites get you to do. Phishing is common and happens all over the world. That is why you have to be careful with what you are doing. If you sense anything out of the ordinary, find another way to contact the person they are pretending to be. Maybe contact another friend to see if they have spoken to them recently. If you sense it is dodgy, it probably is, especially if you know that family member or friend well.

Antivirus Software

Keeping your computer safe is essential and one of the ways to do that is by installing antivirus software. Additionally, a new computer or laptop will likely come with a year's worth of antivirus. If it doesn't, enquire about it at the shop you are buying it from. You might be able to pay a little extra for antivirus software to be installed on your computer.

There are many fake antivirus software out there that exist. However, these are also easy to spot. It will usually appear when downloading a file or on a website. A popup will come on your screen and say “your computer is now infected with a virus” or something along those lines. Avoid clicking on these downloads at all costs because once you do, they will install a virus onto your computer.

These are very common but also easy to spot. The only time you should trust an error is through your antivirus software. If you don’t have one on your computer already, we suggest you go out and buy one. You can even buy anti-virus software from Amazon if you want to buy them from a trusted website. Some of the best antivirus software include; Bitdefender Antivirus, Norton, Trend Micro Antivirus and others.

Investment Scams

If you are active on social media and follow many people, you may already know what we are talking about. These are very common in the past decade and seem to be the most common during Covid. A lot of people were getting into investment and buying stocks and cryptocurrency.

Scammers browse pages about investment and cryptocurrencies to see who follows them. They will then reach out to these people because they know they are interested in investing. Furthermore, the scammer will promise a ridiculous return for only putting a small amount in. For example, they may ask you to put in £10 and promise a £1000 return or even more.

If someone reaches out to you through social media, text message or even email then avoid these at all costs. They are a scam and will take the money off you and never speak to you again. Although you might think that you are not putting in a lot of money, they are probably doing this to hundreds, if not thousands of people. That is how they make their money.

Finally, Fake Shopping Pages

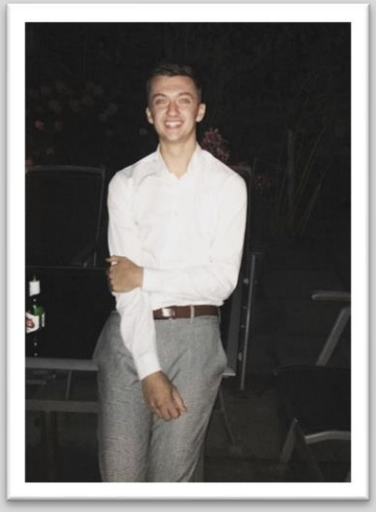
Another common scam is fake shopping websites and pages. If you are new to online shopping, this is a scam which is easy to fall for. During the festive period, you may come across a lot of brands that are new to you.

The question is, how do you spot a fake brand? Well, it is really easy. One of the first things you should do is check social media platforms to see if they have a page. If they do, check the comments section on their posts to see if people are commenting about the product. Additionally, you want to ensure there are a variety of opinions on there and not just one-sided. Sometimes, websites pretend to be other brands, ensuring it is the official URL and not a fake.

Conclusion

As you can see, there are many scams where you can lose money. Businesses are also susceptible to scams which could lead to businesses going bankrupt. A company should always have a form of cyber incident response team in place to deal with scams. They should have software in place to keep their whole network secure. Both you personally and a business are vulnerable to scams. Make sure you make yourself familiar with these scams to avoid them. The more the digital world develops, the more common scams will become so you must be aware.

About the Author



Harry Turner is a freelance writer. He is a writer that graduated with a journalism degree back in 2020. He has a passion for writing and enjoys watching Football and boxing over the weekend. He also likes to write about a variety of different topics that are relevant and on-trend. Harry can be reached online at https://twitter.com/HarryTurner77.

Avoiding the Risks of Ransomware Strikes in Life Sciences

By Travis Tidwell, Business Development Lead, Rockwell Automation

While Life Sciences companies have become even more important to all of us during the pandemic, they have always been challenged with unique cybersecurity risk. Operating within a highly validated environment that typically runs 24x7, these manufacturing systems do not follow a standard lifecycle timeline and these systems typically cannot implement security updates in a timely manner.

In addition, many pharmaceutical and biomanufacturing companies are under pressure to reduce cost, adapt to market demands and increase quality across their products. This is leading to an accelerated adoption of digital technologies, more interconnected systems and highly automated manufacturing processes to meet business initiatives around agile manufacturing capabilities and stronger data integrity compliance. However, these digital transformation initiatives are adding more complexity to the security risk equation by expanding the attack surface for threat actors to target mission-critical systems, many of which are legacy systems running outdated operating systems.

Unfortunately, with the evolving threat landscape, many manufacturing organizations within the Life Sciences sector have been subjected to cyberattacks, including ransomware. The result of these incidents can have major consequences and business impact.

In late 2020, Favera, a pharmaceutical manufacturer headquartered in Luxembourg, announced that it was the victim of a cyberattack that caused its operations to come to a halt. While it is unknown how long it took the organization to restore operations, this incident had an adverse effect on its manufacturing and supply to consumers.

And let's not forget the NotPetya attack on Merck in 2017, which was reported to result in $1.4B in losses for Merck.

What's at stake

Downtime from a cyberattack is costly and unproductive. However, it's not only a financial or intellectual property impact, but also a community impact. Trillions of products (including medicines and vaccines) are delivered to hospitals and the global market annually to support our loved ones – moms, dads, sons, daughters and so on. When you think about the broad consumption of these products, our daily lives depend on the mission of Life Science companies to ensure supply reliability and product quality.

These manufacturing operations are essential to our economy. Sadly, many threat actors are motivated to carry out cyberattacks for various reasons – financial gains, espionage or competitive advantages – because they understand what's at stake and how vulnerable many Life Sciences manufacturing facilities are to sophisticated threats, and modern-day tactics and techniques.

Steps to mitigate risk

Fortunately, several steps can be taken to mitigate the risk of cyberattacks and improve your overall cybersecurity posture. Following are some recommended action areas, based on recurring exposures seen in Life Sciences cybersecurity assessments. As you read through the questions below, reflect on your organization's current practices and where you may be in the maturity of your cybersecurity journey.

- How are you bringing together IT and OT stakeholders? – You must share domain knowledge and experience from both worlds to evaluate and mitigate risk. Use a Cybersecurity Framework such as NIST to identify gaps in your IT/OT security posture using a cross-functional team (IT Staff, Security SMEs, Control Engineers, and third-party trusted partners). Use this framework to develop or maintain a unified strategy that addresses the converged IT and OT environments.

- How are you prioritizing security gaps? – You must be efficient with risk reduction decisions to get the greatest return on risk avoidance investments. Use a risk-based approach to prioritize those gaps and develop a strategic roadmap for closing the gaps based on criticality levels or the asset owner's risk tolerance. Not all ICS vulnerabilities share the same risk level; align on risk.

- How are you protecting home field advantage? – You must have a defendable architecture specific to your OT/ICS environment. Many attacks focused on OT often start in the IT environment and then navigate to OT. Implement a modern cybersecurity architecture that incorporates leading practices such as:

    - Industrial Demilitarized Zone-FW/IT-OT Network Segregation and Micro Segmentation for safeguarding the OT perimeter and high value, vulnerable assets within OT – see this CISA example.
    - Identity and Access Management to enforce access and password policies
    - Multi-factor authentication to enhance the security of remote access connections
    - Endpoint device protection to enhance data integrity and security
    - USB security controls to enforce removable media policies

This allows you to leverage a layered defense strategy to help keep out unauthorized users.

- How are you maintaining situational awareness? – You can't effectively respond to threats if you don't know the status of your OT/ICS environment. Be sure to deploy continuous threat monitoring controls to detect anomalous or suspicious activity in your OT network. Keep asset inventory updated and establish a baseline that alerts the security team when unauthorized devices or users come on the network.
- How are you preparing for the handling of incident responses? – Your ability to respond decisively to security incidents is determined by your organization's readiness. Establish a business continuity plan that focuses on operational resiliency and perform tabletop exercises to pressure test those incident response playbooks ahead of "game day." Role play through situational questions such as:
    - Can the plant be isolated and run in a state of autonomy? If so, how long?
    - Does the plant personnel know what production lines to run or focus on during a state of isolation?
    - What key stakeholders are required and authorized to make critical and timely decisions during a security breach or incident?
    - What specialized OT/ICS resources are on retainer for incident response investigations and remediation activities?
    - If wiped out, how long does it take to recover or rebuild from an attack versus paying a potential ransomware fee?

You play how you practice, so be prepared.

How are you driving cultural awareness? – Your biggest threat, unintentionally in many cases, comes from within the organization. Hold regular cyber awareness training for personnel, including activities such as password hygiene and phishing email exercises.

Reducing business and cybersecurity risk must be a priority of all life sciences organizations. Implementing network segmentation, deploying threat detection services and creating an endpoint security strategy for secure, centralized management of portable media in the OT environment are a few of the steps to take to better secure an organization's network. This will help improve product quality, reduce losses and risk and optimize production operations. A win-win for any life sciences firm.

About the Author

Travis Tidwell, business development lead, Rockwell Automation. Travis has over 14 years of experience in the automation industry. In his current role he is responsible for helping Rockwell Automation customers find ways to increase the security posture of their industrial control systems environments through a combination of strategic and tactical approaches.

Building A Layered Plan for Battling Cybercrime

By Kimberly White, Senior Director, Fraud and Identity, LexisNexis® Risk Solutions

As interactions with customers evolve over time, businesses need to keep pace of all the ways in which bad actors can inflict havoc through cybercrime. In many industries, organizations continue to merge digital and physical services within an omni-channel ecosystem. Routes to purchase are increasingly converging with merchants replacing or combining in-store experiences with digital offerings. This is especially relevant today, as the pandemic permanently altered the way customers interact with businesses with increasing emphasis on digital transactions.

The changing dynamics around customer interactions create a hospitable climate for cybercrime to flourish. Well-networked cybercriminals are adept at leveraging innovative threat vectors to relentlessly target key points across the customer journey. Cybercriminals will leap at the chance to exploit any vulnerabilities in a security system, which begs the question: How can a business protect itself and fight back?

Identity Trust in New Account Creation

One of the biggest sources of cyberattacks target newly created accounts, which are attacked at as high a rate of any other transaction type in the customer journey. According to research, fraudulent account creations – a fraudster creating an account using someone else's credentials and payment details – impact one in five adults. Understanding the markers of fraud at the outset can help keep these types of vulnerabilities properly protected. As cybercriminals use stolen, compromised or synthetic identities to create new accounts, identity trust plays an integral role in an organization's strong cybercrime defense. The ability to rapidly recognize good, trusted customers and quickly determine the validity of the customer credentials contributes to a seamless and secure account opening experience.

This includes getting to know the behavioral patterns of the customer base, which allows for the quick identification of any aberrations in behavior. However, looking at both the physical and digital aspects of identities is also crucial.

Combining digital and physical identity capabilities gives businesses a vast view of the consumer so they can quickly pivot against new threats and create a better customer experience. Customer experiences work best when there is a minimum amount of friction for the customer to make their purchases while keeping assets safe. That is the gold standard of security.

Shore Up Unsecure Payment Points with Behavioral Biometrics

Digital commerce saw a massive uptick amid the height of the pandemic and at the same time, the risk behind digital payment points also increased. Cybercriminals are taking the opportunity created by the digital payment revolution to cash out and monetize stolen credentials. A strong payments defense rooted in identity trust is essential as consumers rely on digital payments throughout omni-channel ecosystems.

One tool to help detect and block attacks is the use of behavioral biometrics, which looks at interactive gestures, such as how an individual types on a keyboard, moves a mouse, holds a phone or taps a touch screen, and compares those characteristics with known digital behavioral traits common to fraudsters, bots and trusted users. The technology is proven to help detect and block automated attacks and suspicious transactions.

Implementing solutions with behavioral biometrics strengthens payment fraud prevention since it combines digital identity intelligence with global transaction insights simultaneously with the transaction. Businesses can improve transaction security and refine personalization with immediate risk intelligence that helps confidently differentiate between a trusted customer and a cyber threat.

The Challenge of Hyperconnected Fraud Networks

Research continues to show a strong pattern of cross-organizational, cross-industry and even cross-regional fraud. Hyperconnected networks exploit the same lists of stolen identity data across multiple regions and industries. Networked fraud remains a highly nuanced threat that easily evades traditional fraud prevention tools like static point solutions.

By combatting fraud networks with cross-industry cooperation, businesses can experience a shared view of fraud that includes intelligence relating to online behavior, transaction trust and risk, global block lists, allow lists and watchlists, as well as targeted industry models. By leveraging a collaborative approach, one organization can block an entity confirmed as high-risk by another organization before further transactions process, improving fraud prevention and adding a layer of protection against networked attacks.

The Consistent Rise of Bot Attacks

Bot attacks are widespread, showing little discrimination for what industries they will invade. They represent a cheap, quick and effective method of initial attack that enables identity testing at scale, providing the opportunity for cybercriminals to validate and rapidly monetize stolen credentials. Proactively detecting bot attacks without disrupting legitimate customer interactions or adding unnecessary friction to key customer touchpoints takes a delicate balance.

It is necessary for organizations to set a balance between strict identity protections to protect customers and creating too much friction in the customer experience. It is possible to keep customers happy while also keeping them safe from bot attacks by leveraging a unified picture of identity informed by network intelligence and targeted visibility into risk signals that indicate bots and aggregators.

Preventing Cybercrime and Protecting Customer Affinity

The complex and constantly changing cybercrime climate challenges businesses to balance interaction speeds with fortified security and a seamless experience at every point of the customer journey. Trusted customers will not compromise on an efficient, secure and effortless interaction every time. Consistently delivering optimal, omni-channel customer experiences provides a competitive advantage in a crowded digital marketplace.

A dynamic, multi-layered fraud prevention strategy protects your business in a rapidly evolving cybercrime environment. Building a cybercrime strategy on the foundation of a unified, risk-based identity view enables a business to deliver personalized, more secure transactions for trusted customers while more accurately detecting and preventing cybercrime threats. Businesses can fully capitalize on the opportunities of a well-connected omni-channel ecosystem by starting with establishing identity trust.

About the Author

Kimberly White, Senior Director of Fraud and Identity at LexisNexis® Risk Solutions, is responsible for commercial market strategy for identity verification, fraud analytics and identity authentication with a focus on new account opening and onboarding workflows. With over 20 years of experience in developing product strategy and managing product roadmaps, Kim's expertise includes corporate strategic planning, understanding market needs and building out robust fraud and identity capabilities for financial institutions, retail/e-commerce, and other commercial markets. Prior to LexisNexis Risk Solutions, Kimberly worked at Fiserv, where she developed product strategy for walk-in bill payment solutions. Kimberly is a graduate of Miami University in Oxford, Ohio and Emory University.

You can learn more about LexisNexis Risk Solutions at risk.lexisnexis.com.

Can Cloud Telephony Services with Military Grade Security Enable Organizations to Create High Brand Value?

By Shubham Patidar, Research Consultant at Fact.MR

In today's technology driven world, the workforce is spread out between those working remotely and those working in offices, with some planning on returning to their office full-time and others remaining on a hybrid or remote model for the foreseeable future. While several companies worldwide have remained invested in the on-premises calling system, the reality is that, today, the shortest way to communicate is often through a stable internet connection.

Companies are thus investing huge sums in the development of a unified communications system with a cloud calling feature. Adapting their communication systems to this new technology can potentially improve or even future-proof the line of communication in and outside of an organization.

Cloud calling, often referred to as cloud telephony, helps in making a company's overall phone system cost less. It provides voice communication services primarily through a third-party host. It is gradually

replacing the need for traditional enterprise telephone systems, including private branch exchange across the globe.

Cloud telephony services further frees organizations from the burden of purchasing and storing stand-alone hardware such as handsets and private branch exchange boxes. It also sets the stage for equipping complementary unified communications as a service (UCaaS) features such as artificial intelligence (AI)-enabled customer support, keyword and voice analysis, interactive voice response (IVR), and call center capabilities.

Organizations nowadays are utilizing cloud telephony services to better connect their teams and make their employees more satisfied, engaged, and focused in their roles. The term 'cloud telephony' signifies a multi-tenant access model, with subscribers paying to utilize a provider's pool of shared and commoditized resources.

As per Fact.MR, a leading market research firm, the global cloud telephony services industry is projected to reach a valuation of US$ 51.5 Billion by the end of 2032 and exhibit growth at a CAGR of 9.5% from 2022 to 2032. Surging need to reduce phone bills and the overall teleconferencing cost in an organization is expected to bode well for the industry.

All cloud telephony platforms utilize voice over internet protocol (VoIP) technology. However, cloud telephony poses a security risk to an organization's confidential data owing to the possibility of VoIP hacking. It mainly occurs because of the requirement of an internet connection for using the cloud calling feature.

Which Are Some of the Common Techniques of VoIP Hacking?

VoIP systems can face unique security risks due to their different setup and high dependence on the internet, as compared to the conventional telephone system. Below are some of the common types of VoIP hacking that a user should be aware of:

- **Social Engineering:** It leverages human interaction instead of VoIP system technicalities. Poor execution of social engineering campaigns is one of the major factors that promotes this type of hacking. Various organizations, especially in emerging economies often fail to provide their employees with education regarding the risk of fraudulent phone calls made by hackers by disguising their caller IDs. Hackers often use tricky means to generate confidential information about a specific target and can utilize it later for malicious acts.
- **Toll Fraud:** As international calls are expensive to make, potential attackers place those calls and the bills are charged to the company's account. In toll fraud, attackers mainly target system users and admins with phishing scams to gain unauthorized access to an organization's VoIP system. They usually leave a voicemail to a department in an organization questioning them about information like bank details. If the employee passes the verification codes, attackers can easily get access.
- **Unauthorized Use:** It involves using an organization's phone network to call other companies or individuals pretending to be someone else. Attackers mainly use robocalling and auto-dialing

software with an organization's cloud telephony system. Those who answer to the phone ID would receive a pre-recorded message, thereby compelling them to do specific things.

- **Spoofing:** The majority of people use their caller IDs, however, it might not be the ideal way to know from where a particular call is coming from. Sometimes, an attacker can call an organization by using a fake caller ID and take advantage of the trust that an employee places on a familiar phone number. Attackers can then use the fake ID with another hacking technique like social engineering.
- **Eavesdropping:** Adoption of insecure networks, which is characterized by the lack of Transport Layer Security (TLS) and Real-time Transport Protocol (SRTP), could enable hackers to keep their eyes on an organization's network. It would help them to gather crucial information about the organization, its clients, and other aspects. By gaining the information, they can sell the organization's intellectual properties to rivals, access its customers' data for selling, and blackmail the organization with sensitive data.

Renowned and start-up companies operating in the global cloud telephony space are striving to develop cutting-edge technological tools and services to help protect organizations against the aforementioned hacking techniques. Besides, some of the leading organizations are placing their own security teams to perform cybersecurity services, including the protection of cloud calling features.

Checkmarx Launches Checkmarx API Security for Protecting APIs

In August 2022, Checkmarx, a pioneer in the field of software security based in Israel, launched a new API security solution named Checkmarx API Security. It correlates and prioritizes vulnerable data from various AppSec engines. Every cloud-hosted, modern web, or connected mobile application exposes and uses APIs. These are used to call application functionality and to gain access to data.

It further creates a large attack surface, thereby leading to a rising number of publicized API breaches and attacks. The new solution addresses numerous issues related to security in the software development lifecycle, including cloud calling. It helps in discovering zombie and shadow APIs, eliminates the requirement of additional API-specific tools, and finds out APIs in source code to fix and identify problems.

FCC Chairwoman Jessica Rosenworcel Proposes Restrictions on Ringless Voicemails

Jessica Rosenworcel, chairwoman of the Federal Communications Commission (FCC), proposed restrictions on ringless voicemails in February 2022. The new norm would require callers to gain a consumer's consent before providing a ringless voicemail, which is referred to as a message left in the mailbox without ringing their phones.

As per Rosenworcel, ringless voicemail can lead to frauds like robocalls, as well as be invasive. Thus, it needs to be put under stringent consumer protection norms. The proposal came in after phones in the U.S. received more than 50 billion robocalls back in 2021. The number was significantly higher than that of 2020, in which only 4 billion robocalls were received by consumers.

Worried About Those Random Robocalls? RoboKiller Unveils New Call Confidence API

In May 2021, RoboKiller, a provider of customizable call blocking services, headquartered in New York, unveiled Call Confidence API, its new enterprise robocall prevention technology. Launch of this solution would enable companies of all sizes to tap into the same call blocking technology that have protected more than one million Americans from financial losses worth US$ 150 million due to phone frauds.

Call Confidence API would further help companies to strengthen their networks and provide robust defense features to join the fight against dangerous and illegal phone scammers. The solution utilizes machine learning technology to accelerate the mitigation of robocalls for companies vulnerable to such calls. It provides a plug-and-play solution and is specially designed with ease-of-use, speed, as well as privacy in mind.

Is the Future of Cloud Telephony Bright?

As the cultural diversity of a specific region calls for multi-language support for businesses, cloud telephony would help to ease the task by allowing representatives to transfer customers' calls to various language specialists. It would also enable freedom of geographical equation, thereby making customers feel more connected to a brand.

Thus, no matter where a business is set up across the globe, companies can easily route calls coming from customers to language specialists. But, this potential of cloud telephony has not been used to full extent till date. More companies are likely to eliminate geographical constraints and focus on offering a better experience to their customers in the next decade by using cloud telephony services.

Apart from that, key cybersecurity software solution providers are anticipated to offer military grade data security which would surpass compliance requirements. These solutions would hold the key to meeting stringent norms as industries such as banking and financial services are consistently facing strict communications regulations. Also, by shifting towards a cloud telephony system in future, companies can take a leap forward in terms of meeting regulatory compliance and ensuring data security.

About the Author

Shubham Patidar is an experienced research consultant at Fact.MR, He is a Client Partner at Fact.MR, with a proven experience in market research & consulting industry and has been closely working on technology vertical.

Crack The Code

Cybersecurity Workforce Certificate Program

By Stephen Patrick, Marketing Coordinator at the University of Louisville

According to the Identity Theft Resource Center 2021 Data Breach Report, there were 1,862 data breaches last year, with more than 80 percent revealing sensitive personal information. The demand for qualified cybersecurity professionals is high, but there are not enough skilled people in cyber for the openings. There are 1,053,468 employees working in cybersecurity in the U.S. as of February 2022. (Cyber Seek). As of February 2022, there are 600,000 job openings in the cybersecurity industry, meaning only 68 percent of jobs are filled. (Cyber Seek).

The Cybersecurity Workforce Certificate Program is taking these issues head-on through an innovative online curriculum. Awarded a total of $8.3 million in grant funding from the National Centers of Academic Excellence in Cybersecurity, UofL and its Digital Transformation Center (DTC) are leading a coalition of universities to deploy the next generation of cybersecurity tools and professionals.

The Cybersecurity Workforce Certificate Program received an initial $6.3 million grant to back the research and curriculum development in 2020. For the curriculum, UofL partnered with the University of Arkansas Little Rock, the University of North Florida, the Kentucky Community and Technical College System – Bluegrass Community and Technical College and Owensboro Community and Technical College, and a coalition liaison from the City University of Seattle.

Photo Cred: Photo Cred: UofL Cybersecurity

This coalition has developed an extensive and robust collection of modules covering the foundational concepts needed for any cybersecurity role and introducing innovative topics such as post-quantum cryptography. Industry partners helped to build hands-on learning activities integrated with the curriculum, including a Capstone project inspired by actual scenarios faced by the industry partners. The resulting program incorporates the subject matter expertise from leading academics. The result is an extensive curriculum filled with valuable learning materials.

During the first two years, the coalition piloted the online learning modules with a test group of about two hundred students across numerous cohorts. Student feedback is used to refine the curriculum, labs, and other learning activities.

In 2022, UofL and the collation received an additional $2 million to add six more colleges and universities to the coalition: Kentucky State University and Simmons College, both historically Black colleges and universities (HBCUs); The City College of New York, Kennesaw State University, Hood College, and Northwest Missouri State University. Each school in the coalition is a National Security Agency - designated National Center of Academic Excellence in Cyber Defense and contributes interests, experience, and skills aligned with cybersecurity systems.

Photo Cred: Photo Cred: UofL Cybersecurity

The certificate leverages technology industry micro-credentials from Microsoft, IBM, and Google, gamification, and direct learning with use cases from industry partners to teach artificial intelligence, blockchain, and other innovative aspects of cybersecurity. University of Louisville's Digital Transformation Center leads the curriculum development for the online program. The program is piloting the six-month instructor-led certificate program. When completed, it will be available open source.

“As technology continues to become more of an integral piece of our everyday lives, a strong cybersecurity industry and workforce are the most important protections we have to make our financial and healthcare systems secure,” said Sharon Kerrick. She is a principal investigator on the NCAE-C grant, associate professor, and assistant vice president of the UofL Digital Transformation Center. “We can fill that need with this focused, accelerated curriculum that prepares diverse students of all backgrounds for careers in cybersecurity.”

Photo Cred: UofL Cybersecurity

“It’s great that we’re getting to know our colleagues at neighboring universities — we’re working together, and sharing ideas,” said Richard Maiti, an assistant professor of computer science at Kentucky State University, who serves as the lead for the project at his institution. “This is a terrific opportunity, and it’s helping to bring cybersecurity awareness and training to everyone — our students, professionals, and folks in the community.”

Students are already graduating from the program. Kelly Kramer graduated from the University of Louisville in 2012 with a bachelor's degree in psychology and landed a job in law enforcement as a data analyst and legal assistant. But he grew interested in cybersecurity, where his interests in psychology, technology, and protecting people mixed.

"This program has taught me quite a bit about securing not only those essential entities like hospitals, businesses, government agencies, but also ourselves," said Kramer, who now plans to return for his master's degree in computer science. "It is a complex web of networks, nodes, servers, databases, and much more. We need people to understand each of these if we are to effectively secure them. I do not doubt that this program will open opportunities for myself and others."

JT Corcoran graduated from UofL in 2014 with his bachelor's and master's degrees in computer engineering and computer science and returned for the program. He joined the U.S. Air Force and spent seven years on active duty, working in data analytics, cyber incident response, and network architecture planning. As Corcoran's service ended, he started looking at new career opportunities.

Photo Cred: UofL Cybersecurity

"Since I had a prior background in cybersecurity, many of the topics were familiar but I haven't done some of these things in a while," said Corcoran, who now works as a healthcare security analyst. "The certificate provided a nice refresher on doing things like writing security system rules, configuring network infrastructure, integrating cloud services, and conducting forensics in a lab environment. The inclusion of newer technology topics like blockchain and post-quantum cryptography was fantastic to help brainstorm new ways of innovating in the security space."

The cybersecurity industry is one of the fastest-growing fields in the world. As we rely on technology more every day, educational innovators like this coalition of NCAE-C schools are here to prepare the next generation of the cybersecurity workforce! If you are interested in breaking into the field of cybersecurity and want the opportunity to gain knowledge across multiple domains, this might be the program for you."

More information on the Cybersecurity Workforce Certificate Program is available at louisville.edu/education/nsacybersecurity.

About the Author

Stephen Patrick: Marketing Coordinator at the University of Louisville.

Stephen completed his bachelor's degree in Communications & Marketing. He was an intern assistant in the University of Louisville Sports Information Department. During college, he worked as a Personal Banker at Stock Yards Bank. After graduation, he moved to Nashville, TN. He severed as a Corporate Partnership Coordinator at Tennessee State University. He has over six years of sports journalism experience, writing for several sports media outlets.

Stephen Patrick can be reached online at Stephen.Patrick@Louisville.edu and at our company website

https://www.louisville.edu/education/nsacybersecurity/

Cyber Talent Recruitment: The Best Defense Is An Earlier Offense

By Cynthia Jenkins, Chief Marketing Officer (CMO), Skillsgapp

According to cybersecurity expert, Gary S. Miliefsky, “There will be a global shortage of exactly 5 million cybersecurity jobs worldwide by January 2023.”

Amid an era of unprecedented ransomware attacks, data breaches and supply chain intrusions – the volume of cyber intrusion activity globally soared 125% last year over the previous – what is a company to do in order to shore up their cyber defenses and further, do so during the tightest labor market in the industry’s history?

One significant resource, a game-changer in addressing the cyber/IT skills gap, will be innovative technology; the kind that seeks to connect students to careers in cybersecurity, earlier in the workforce life cycle.

The use of simulation will also be important; mobile outreach, particularly to rural populations; and interactive, gamified apps; these tools will deliver an engaging, skills-based experience, a curriculum that can grow with a student, from soft-skills to bankable hours toward certifications.

Virtual training addresses the highly unique needs of our upcoming generations and leverages the many changes in our society that have taken place over the past decade, exacerbated by the COVID-19 pandemic.

Using technology to allow virtual skills development takes advantage of the shift in our culture - The Entertainment Software Association reports that Americans spend an average of seven hours a week playing online games with others. At a time when only 5% of our high school students study computer science due to lack of funding and/or lack of set standards in cyber/computer science curriculum, this medium serves as a powerful, scalable conduit to students, including importantly those being left behind in these most basic skills, especially young women and students of color.

According to the Pew Research Center, 95% of 13- to 17-year-olds have access to a smartphone, and a similar share (97%) use at least one of seven major online social platforms. The worldwide health crisis of 2020/21 has only fueled that number and validated technology as a viable, teachable medium, as well as prompted a renewed focus on increasing broadband coverage in rural areas.

If there's one thing we've seen illustrated in the past two years, it's that those in regions of the country with lower broadband reach are disadvantaged when it comes to virtual education. Fortunately, we now have not only renewed focus and knowledge about that disparity, but there are also tools – some of which were used by public school systems around the country – to help counter that disparity and supplement broadband access.

The U.S. military is already taking advantage of the use of technology and the mobile gaming trend.

Indeed, one of the most revered workforces in the world uses gaming for tactical training, upskilling, soft skills, and for recruitment. "America's Army Proving Grounds" is the official game for the U.S. Army that lets players try out virtual missions and maneuvers that echo true-to-life Army scenarios.

If the U.S. Army can complete 'Missions Impossible' in headsets, the cybersecurity/IT industry can employ interactive educational technology to help our next workforce generation develop real-world work skills through interactive, digital experiences that will engage with industry and expose users to existing opportunities. Augmented reality can also be used as a more cost-efficient venue for training, apprenticeships, and stackable credentialing.

The warm-body recruitment approach of today simply isn't sustainable. To meet the crisis at hand in safeguarding our cyber defenses and repopulating our workforce in the process, focus needs to shift to the workforce pipeline – and thinking early in that workforce pipeline, starting in middle to high school.

Our up-and-coming cyber workforce craves career awareness and ultimately, guided access to pathways and industry. Technology is the answer.

Funding is needed to support broader computer science and cyber programing, in-class career learning driven by industry, and funding supported by the government, yes. But there also needs to be an open-minded approach to leveraging novel technology, both in and out of the classroom, as this is a digital generation that learns best via the 'Internet of Things' (IoT) and by doing things with their hands.

About the Author

Cynthia Jenkins is Co-Founder and Chief Marketing Officer of Skillsgapp, the developer of Cyber Watchdog and other workforce development and career awareness mobile games designed for middle- and high schoolers+ with regionalized cyber pathways, apprenticeships and job opportunities, based on a player's location and proficiencies.

Contact Cynthia at https://www.linkedin.com/in/cynthiapjenkins/ or cynthia@skillsgapp.com.

How Can Businesses Build Customer Confidence In A Digital Economy?

The importance of developing business-customer relationships with digital trust.

By Peter Boyle, Chief Technical Officer, Burning Tree.

Online shopping is becoming the norm within the retail market. Whilst this presents many opportunities for businesses to expand and thrive, it also means that organisations must focus on a new aspect of customer relations: building digital trust.

The pandemic dramatically accelerated the UK's proportion of online retail sales, which reached a record high of 35.2% in January 2021. And that was only the beginning; lockdowns were a catalyst, but digitisation is not slowing down in the post-pandemic world. Consequently, many companies continue to evolve the online shopping experience for customers.

The decline of in-person shopping means that online user experiences influence consumers' buying decisions more than ever. Most people are aware of the growing threat of scams and cyber attacks. As a result, establishing digital trust helps users decide which companies will keep their personal information safe.

'Digital trust' describes the confidence online users have in the ability of processes, people and technology to create secure digital transactions, dividing the dependable services from the corrupt ones.

So, gaining the trust of digital customers is non-negotiable in the modern world. But how can businesses develop digital trust — and what will happen if they do not?

Attracting loyal customer bases through digital trust

When people make a purchase or interact with an online retailer, they demonstrate their digital trust in that business. However, the quality of the service is no longer defined by how an interface looks or how easy it is to navigate.

Customer expectations have evolved with digitisation. Driven by device proliferation and improved internet connectivity, modern online shoppers expect to encounter seamless digital processes from sign-in to purchase — particularly since the pandemic, which increased the number of people using online services regularly.

Today, customers are more aware of how their data is used and stored and base their shopping behaviours on a provider's ability to ensure security. The Okta Digital Trust Index (2021), which surveyed 13,000 office workers, found that 88% of people in the UK were unlikely to purchase from a brand they did not trust. And according to a Retail Week report on the 20 most-trusted UK retailers, 58% of consumers are highly conscious about their safety when shopping online, citing identity theft as a significant concern.

Plus, with most businesses working online in some capacity, the government is introducing regulations for using technology to manage digital identities. An updated UK digital identity and attributes trust framework was announced earlier this year to make sharing digital identities between users easier and safer, allowing more control over what personal information is available to different services and organisations.

There are several ways businesses can generate a loyal digital customer base — from inviting positive customer reviews to providing excellent customer service. But when it comes to digital trust, three main factors make people in the UK more likely to trust a brand: its service reliability, tried-and-tested security policies and quick response times — all of which can be facilitated by successful digital transformation.

Developing cyber security to support digital trust

Cyber security is an essential consideration for organisations undergoing digital transformation, which involves implementing technology to automate processes, encourage a more cyber-aware business culture, increase security and refine user experiences. As such, retailers must protect data from a cyber breach to remain compliant and secure digital customers.

According to Okta's survey, 47% of UK people permanently stopped using a firm's services after hearing of a data breach. As such, IT professionals are harnessing advancements in artificial intelligence and machine learning to support existing traditional threat models and automate risk management to reduce the overall probability of falling victim to a cyber attack.

Many organisations are also taking a 'zero-trust' approach to cyber security, which means that no network activity is trusted immediately. Every device, service, application or user connected by a network must go through a robust identity and access management process to gain a least privileged level of trust and

associated access entitlements. A zero-trust framework helps bolster cyber security and minimises the likelihood of a breach.

Effective customer identity and access management (CIAM) solutions also enable organisations to capture and interpret customer profile data to inform customised user experiences whilst controlling secure access to services and applications. A robust CIAM solution may involve implementing multi-factor authentication (MFA), self-service account management and single sign-on (SSO) to minimise friction, increase engagement and develop trust in business processes over time.

Implementing cyber defences is integral to building digital trust. Still, having a robust cyber security system should be a fundamental requirement within every organisation — no matter its business goals. As the threat landscape worsens, cutting corners can lead to significant reputational and financial damage. So, ensuring cyber security should be an urgent priority — not an afterthought.

About the author

Peter Boyle is the chief technical officer (CTO) at Burning Tree: a specialised information security company operating globally. He is responsible for creating a suite of security products to complement Burning Tree's existing consulting capability. Under Peter's direction, Burning Tree is creating a product suite that helps companies overcome many of the complex security challenges we see today — without incurring the overhead of an in-house security team.

Peter joined Burning Tree from BT, where he spent 20 years working in information technology — including eight years as the head of identity and security services. In this role, he was responsible for the design, development and operation of a range of platforms covering identity lifecycle management, privileged user management, single sign-on (SSO), authentication, security information and event management (SIEM) and threat detection.

Peter can be reached on LinkedIn (https://www.linkedin.com/in/peterjpboyle/) or via Burning Tree's website (https://burningtree.co.uk).

How Cloud-Based Services Minimize the Impact of Incident Recovery

Few organizations are able to continue operating after being hit by ransomware, let alone be able to quickly get services back online. Those few who can are likely assisted by cloud-based services as those systems tend to remain unaffected.

By Jeff Chan, Technical Advisor, MOXFIVE

Recent data shows that nearly 70% of organizations now host more than half of their workloads in the cloud, with overall cloud adoption growing 25% in the past year. With this increase in the adoption of cloud-based services, organizations are well on their way to moving existing services from on-premises to the cloud. One of the biggest and most notable benefits for organizations making this shift is that the security risk and IT management gets transferred to the vendor. Organizations can significantly reduce the amount of time they spend managing infrastructure, updating software, and upgrading hardware by transferring these tasks to their vendor, who is then responsible for ensuring that services are up, systems are updated, and Service License agreements (SLAs) are met. What's more, cloud-based services can provide a significant benefit when dealing with a ransomware incident.

In the event of a ransomware incident, cloud-based systems tend to be unaffected, since these services and the servers hosting them are not running on the organization's domain/network. In my experience, only a few organizations have been able to continue operating even after being hit by ransomware or

have been able to quickly get services back online within a matter of a couple of hours/days. Those few were likely assisted by the number of cloud-based services they were using.

Lessons from a Law Firm

In 2020, a law firm was tasked with restoring its impacted environment, which contained a couple of on-premises Exchange servers (email) and a document management system. Unfortunately, their backups were targeted by the threat actor and these backups were impacted in such a way that trying to recover data from them required an extensive amount of time. For this law firm, their email servers and document management system were critical as their core business relies on email communications and contracts stored on those systems. Restoring their email servers to a functioning level took approximately 7-10 days, increasing the firm's stress as they were unable to operate for those days and had to resort to other methods to connect with their clients.

A year later, another law firm of relatively the same size was impacted by ransomware. Fortunately for them, they recently migrated their email services from on-premises to Microsoft 365 and were therefore able to continue operating as usual. Roughly 80% of their business was up and running immediately after the incident happened, and only a handful of non-critical systems were impacted by the ransomware. Having these cloud-based solutions minimized their business impact, which allowed the law firm to keep calm throughout the response efforts knowing that they would still be able to operate and run their business.

Building Off a Solid Foundation

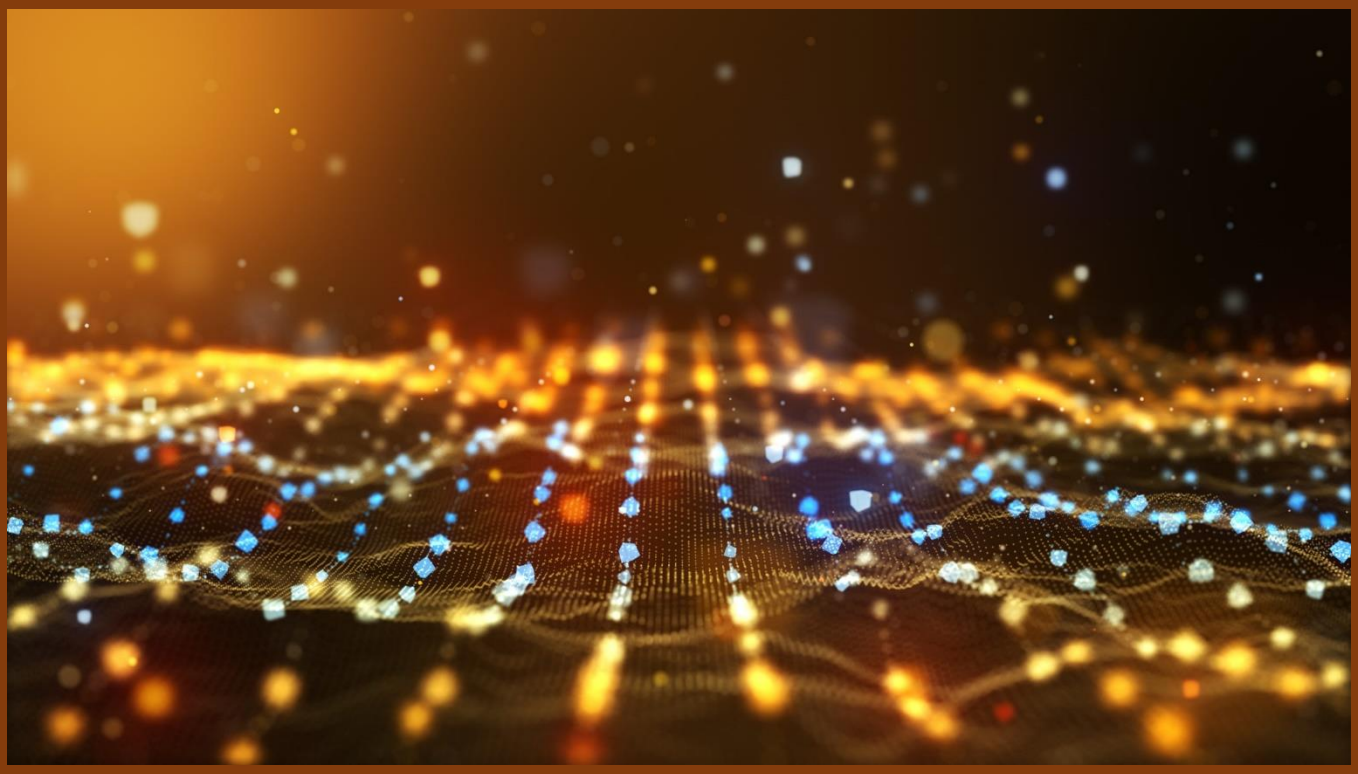
It's clear that cloud-based services have their benefits, but it is also important to secure the data in those services. These services are still vulnerable to attacks and threat actors can log into these services and get creative with the information and services to which they are exposed. So, when you're considering going to a cloud-based service, make sure to implement a few cybersecurity basics, such as:

- Enforcing a strong password policy.
- Setting up Multi-Factor Authentication (MFA) using a software or hardware token.
- Enhancing logging capabilities and regularly monitoring logs.
- Limiting the number of users with administrative roles.
- Implementing IP whitelisting and geo-blocking, if possible.

When you consider making a move to a cloud-based service, it's important to understand why you are doing it and if it makes sense for your organization. In most cases, it's simple: You let someone else manage your services so that you don't have to, it makes it easier to scale as needed, and allows your organization to focus on what matters. And if you ever get impacted by ransomware, you can more confidently trust that these applications will keep functioning, minimizing the stress of recovery.

About the Author

Jeff Chan is a technical advisor at MOXFIVE who is a technical cyber security leader that has helped build incident response teams and has led a large number of digital forensics and incident response investigations. As a technical advisor, Jeff has assisted clients in managing incidents and recovering their networks from cyber security attacks. Jeff can be reached online at his LinkedIn profile at https://www.linkedin.com/in/jeffrey-chan-h/ and at MOXFIVE's website https://www.moxfive.com.



How To Guard Critical Infrastructure Against the Sophisticated 'Golden Ticket' Attacks

The Powerful 'Golden Ticket' Attacks are Surging in Popularity – What You Need to Know

By: David Levine, Director of Solution Architects, Remediant

Golden ticket attacks aren't anything new to the cybersecurity industry, but the latest surge in successful attacks from the Chinese-speaking APT group, TA428, and other cyber espionage gangs, have served as a hard reminder for all on just how powerful these attacks can be. The incidents have also highlighted what aspects of an organization's cyber health and readiness need to be prioritized.

It's never a convenient time to experience a breach, but reducing the time it takes to detect the breach and the privilege sprawls an organization has can make a huge difference in how effective one is. As recorded in Verizon's 2022 Data Breach Investigation Report (DBIR), the use of stolen credentials was one of the top ways attackers succeeded, and key among the culprits is privilege misuse, of which 80% is caused by privilege abuse, which is what lies core to the sophisticated golden ticket attack techniques.

The name says it all

The golden ticket concept arises from the Kerberos authorization technology used by Microsoft. Kerberos runs on a Key Distribution Center (KDC) that uses tickets to authenticate all parties, verifying their identity through nodes. The authentication process uses conventional shared secret cryptography that prevents attackers from reading or altering packets moving laterally across the network.

Every time the KDC authenticates a user, it issues a ticket granting ticket (TGT) with a unique session key and timestamp for how long the session is valid. Once authenticated, the TGT serves as proof that the user is legitimate, allowing them to access other resources within the environment. Each TGT is encrypted with a KRBTGT password hash, which is the so-called golden ticket.

If an attacker gains access to that hash, they can create a TGT and impersonate any user for any amount of time, giving them unfettered access across the domain. From there, they only need four pieces of information:

- The Fully Qualified Domain Name (FQDN) of the domain
- The Security Identifier (SID) of the domain
- The username of the account they plan to impersonate
- The KRBTGT password hash

And, depending on how an organization manages privileged access, attackers can either be successful – or be stopped in the middle of the attack. If they are successful in obtaining each one, attackers have a golden ticket to carry out data breaches, ransomware attacks, and more.

What makes this attack so powerful and concerning is how attackers can continue abusing an identity and moving laterally across systems with Kerberos tickets, even after the account has been flagged as compromised and its credentials have been reset.

Strategies to defend against golden ticket attacks

Golden ticket attacks are one of the most egregious examples of these trends. With a golden ticket in hand, hackers can appear as any user or be granted the permissions of any role in Active Directory, giving them free rein over your environment.

While there is no way to completely prevent golden ticket attacks, there are precautions you can take to close off this entry point from attackers. This includes:

1. **Reduce the number of privileged administrators.** The fewer there are, the less privileged account exposure you risk. You can also implement “Just Enough Admin” and “Just in Time” access for administrators to further limit privilege for those accounts and contain any attacker who gains access to them.

2. **Control endpoint privileges.** No regular user should ever have standing administrative rights on their device. At the same time, administrators shouldn't be allowed to log on to end-user devices. That way, even if an attacker gains access to an endpoint, they won't have the privileged credentials they need to expand the scope of their attack.

3. **Minimize standing privilege.** Built on the principle of least privilege, Zero Standing Privilege (ZSP) is a new approach coined by Gartner that aims to eliminate all standing privilege and deliver only the minimum privilege required for the minimum amount of time. Adopting a Zero Trust Privileged Access model that includes ZSP and JITA can mitigate the risks of golden ticket attacks.

With geopolitical tensions at its height, critical infrastructure and supply chain organizations in particular need to be vigilant in containing the risk of stolen credentials and privilege abuse. In fact, the 2022 IBM Cost of a Data Breach Report found that almost 80% of critical infrastructure organizations studied don't adopt zero trust strategies, even as "concerns over critical infrastructure targeting appear to be increasing globally over the past year." Of the breaches against critical infrastructure organizations, 28% were ransomware and destructive attacks aimed at disrupting global supply chains. From standing privilege granted to internal users to access given to partners and other third parties, you can open yourself up to not only compromised credentials, but lateral attacks once attackers gain access to your environment.

Looking ahead, organizations need to take the proper steps to eliminate standing privilege and cut off attackers' ability to move about their environment, as it may be our best move for tamping down increasingly bold attacks.

About the Author

David Levine CISSP, has over 20 years of experience in technology and cybersecurity and has published articles and blogs in these fields. David has held information security leadership roles at public traded companies, SMB's, and startups.

David is currently the Director of Solution Architects at Remediant, in this role he leads Remediant's Sales Engineering team and works closely with both the sales and engineering teams. He is responsible for the adoption and implementation efforts that secure and protect lateral movement and privileged access which is of utmost importance to both corporations and its customers. David has held many networking and ethical hacking certifications (sadly due to time constraints, some have expired).

Is Your Security Log 'Bathtub' About to Overflow?

By Ozan Unlu, CEO and Founder, Edge Delta

Security Log Data - More Data Doesn't Always Mean Better Protection

A major issue that security operations teams face is the aggressive speed at which vulnerabilities are being exploited, coupled with massively increasing data volumes (relating to security events) being generated across current infrastructures.

Security logs can be extremely useful for helping identify or investigate suspicious activity, and are a cornerstone of every traditional SIEM platform. But the fact is that current infrastructures are generating security logs at a rate faster than humans or even machines can analyze.

Consider this: it would take a person about one 8-hour work day to read 1 megabyte of raw logs and events, a thousand people for a Gigabyte, a million people for a Terabyte, and a billion people for a Petabyte. Some of the organizations we work with create close to 100 petabytes of data per day. Security operations teams are drowning in data and the tide is only going to get higher. These teams desperately need a better way to manage, analyze and make sense of it all. But how?

The Limitations of SIEM Systems

Today's SIEM systems - where security logs are traditionally routed, indexed and prepared for analysis - are quite advanced, but they do have their limitations. Certain systems, particularly older, on-premise ones, can be painfully slow when it comes to querying data and delivering the required information,

especially when maxed out on events per second (EPS). This is certainly not ideal given that attackers only need seconds to exploit a vulnerability. Visibility into threats - both emerging and existing - in as close to real-time as possible is essential.

Additionally SIEM pricing models can be problematic, as price often inflates massively as data volumes increase, while security budgets are only increasing incrementally. Here, it's important to remember that all security log data is not created equal. Certain logs are typically the most likely to contain meaningful information, while other logs may contain information helpful for event correlation.

An example of this would be an intrusion detection system that records malicious commands issued to a server from an external host; this would be a primary source of attack information. A firewall log could then be reviewed to identify other connection attempts from the same source IP address, reinforcing that the IP address in question is in fact likely to be a malicious actor.

Intelligent event correlation is one of the most powerful features of SIEM systems, and the richer and more comprehensive the data, the better the results. Security operations teams therefore find themselves facing a dilemma. They can include the majority (or all) log data - including a high volume of logs with little to no value - which often leads to an overstuffed SIEM that eats through their budget. Or, they can make predictions on what logs they really need while neglecting others, which may keep the team in-budget but creates significant blindspots and vulnerabilities. Such an approach may be deemed too risky since threats can be lurking anywhere.

Finding A Balance

The "centralize and analyze" approach to SIEM evolved at a time when organizations prized one true copy of logs in one highly secure location, often totally separated from production environments and completely inaccessible to hackers, malicious insiders and other employees. Given the significant rise in the number and variety of cybersecurity threats, combined with the volume of security logs being generated, such an approach is no longer optimal from a speed or cost perspective.

A new approach is needed that entails analyzing all data at its source - separating where data is analyzed from where it is stored. Some call this approach "Small Data" - processing smaller amounts of data in parallel. Once logs are analyzed at their source, they can then be relegated as higher-value (and routed to a higher-cost, lower volume SIEM repository) or lower value and routed to a lower-cost storage option). Additionally, when analytics are pushed upstream, security operations teams can sidestep indexing for the moment and identify anomalies and areas of interest even faster than with an SIEM alone, which is critical in the constant race with adversaries.

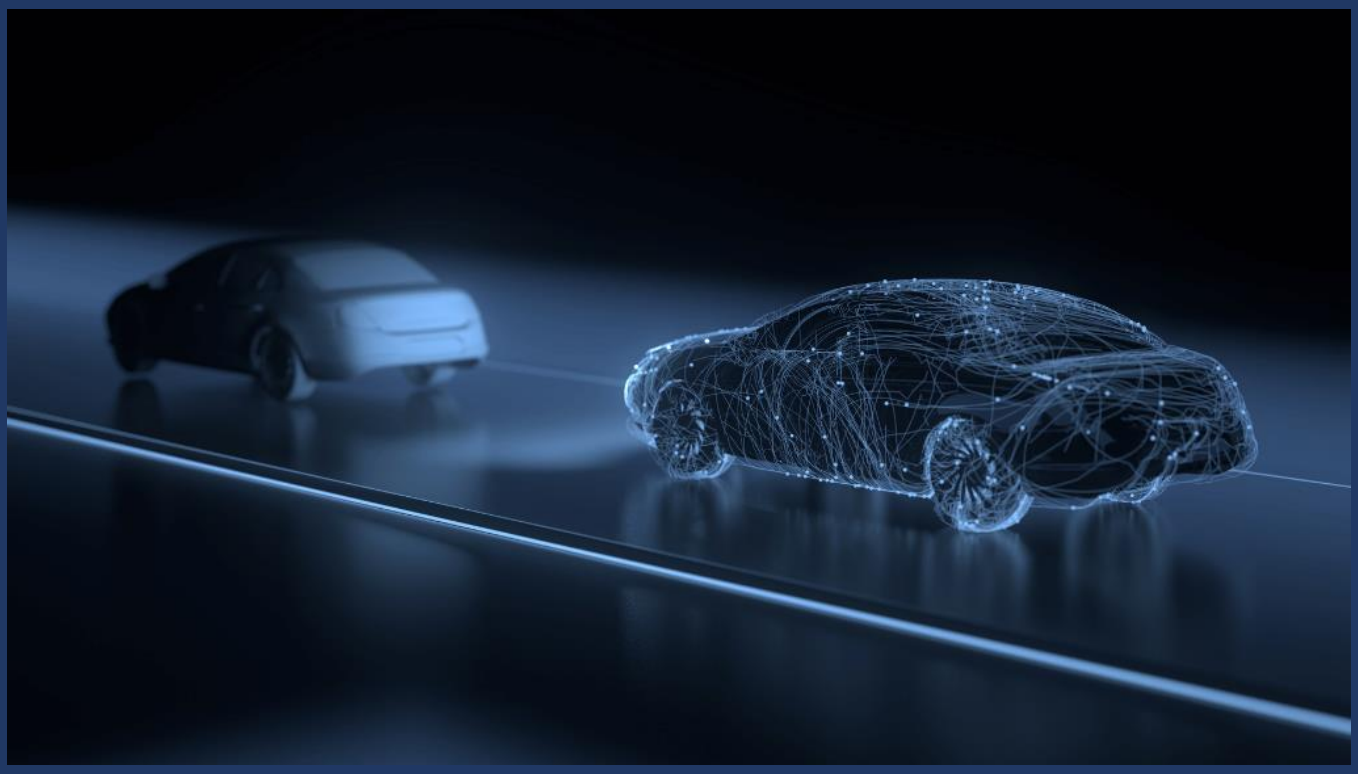
Today, this can be achieved in a way that maintains maximum security, availability and confidentiality of logs. Enterprises can therefore afford to have eyes on all their data while not compromising the security benefits of an SIEM.

Conclusion

In the coming years, cybersecurity threats will only escalate, and security teams must be able to expertly harness and leverage their log data in order to stay one step ahead. Older methods of data ingestion and analysis, which may have worked well as recently as a few years ago, are in need of modification to meet this new reality. There are ways that security operations teams can have it all - visibility into complete datasets combined with a budget preservation - but it may require some new approaches.

About the Author

Ozan Unlu, CEO and Founder, Edge Delta. He can be reached online at ozan@edgedelta.com and at https://www.edgedelta.com/



It Isn't Your Daddy's Oldsmobile Anymore

By Dan Shoemaker, Professor and Distinguished Visitor IEEE

There is no situation where you are more vulnerable to a cyber-attack than when you are in your automobile. Are you surprised? If so, you still view your car as a transportation device. But today's cars aren't like your old man's. They're built around a complex array of microcontrollers and integrated circuits that enable all the wonders of the modern driving experience. And due to that thirst for digital technology, the automobile business has become one of the world's primary consumers of microchips.

Your vehicle is a self-contained local area network. So, logically, every access point requires the same network security authentication and authorization processes. Likewise, your car interacts within a diverse electronic cyber-ecosystem. That makes it a prime target for exploitation. Over-the-air software updates of vehicle systems, GPS satellite connectivity, hands-free cell phones, onboard diagnostics, and even your remote keyless entry system are all legitimate points of entry. Yet, there are no guards posted at those gates.

You are probably familiar with the general shape of access control on a network because you use passwords to authenticate your systems. That is not the case with an automobile's external interfaces. For instance, the interface between your cell phone and the functionality that enables hands-free calling or your onboard entertainment package are not firewalled. And so, exploits like RFID relay attacks, cell tower spoofing, hacks of OBD-II ports, or Software Defined Radio attacks pose a credible risk.

Controlling access to your vehicle's internal systems is vital to driving safety because your car depends on tiny electronic control units (ECUs). These ECUs are nothing more than embedded logic installed to perform a single operation, like braking. A controller area network bus (CAN-bus) ties the car's ECUs into a complex system. That system enables every aspect of your automobile's digital functionality, from entertainment to throttle control. It should be clear that explicitly designed and implemented countermeasures are necessary to protect these digital components from unauthorized access. Otherwise, a malicious third party could take remote control of your car. That would be a dangerous condition in a parked vehicle. It is a subject of extreme concern if the car is doing seventy miles an hour down a local freeway.

Accordingly, adopting a standard, systematic approach to monitoring and controlling the interactions between the vehicle and its digital ecosystem is vital. There have been whack-a-mole attempts at addressing the problem, such as immobilizers and discussions of purpose-built PKI for authentication. But the fact is that the industry has always concentrated more on spreading the net to enable greater access rather than devising ways to control it. That's because features sell cars. So dangerous functionality, like onboard internet, has always gotten precedence over implementing a proven set of best practices for stopping cyberattacks.

But that is going to change. In January of 2021, the International Standards Organization (ISO) promulgated a comprehensive set of standard best practices for Road Vehicle Cybersecurity Engineering (ISO/SAE 21434). These practices establish a formal and systematic cyber security management system (CSMS). Specifically, ISO/SAE 21434 describes a systematic way to protect the vehicle from design, development, production, operation, maintenance, and decommissioning risks. That advice encompasses all internal connections, embedded systems, and external interfaces.

Realistically, the prospect of an OEM adopting an organization-wide CSMS wouldn't be worth discussing. Because in a world of profit, the requirements of ISO 21434 are far too costly. However, compliance with 21434 is tied to a United Nations Economic Commission for Europe (UNECE) regulation called UNECE R-155, "Uniform Provisions Concerning the Approval of Vehicles with Regarding Cyber Security and Cyber Security Management Systems." Cyber security management systems involve practical control behaviors that ensure that all known cyber threats are addressed. R-155 mandates that every OEM must provide audited proof that they have implemented a functioning Cyber Security Management System (CSMS).

UNECE R-155 comes into effect in July of 2024. After that date, the countries that make up the UNECE will require certification of a correctly configured CSMS to grant vehicle type approvals. Those approvals are critical because the OEM would not be able to sell their cars if they didn't have them. Of course, this deadline could change as the OEMs jockey with the UNECE, and It should also be noted that this mandate is for Europe only. Still, this initiative provides a commonly accepted standard definition of what each OEM needs to do to safeguard their products in this digital age.

Full and Systematic Vehicle Cybersecurity

So, what does systematic automotive cybersecurity look like? Well – first of all, it's a process. In effect, the activities within this process satisfy the stated intentions of the standard. The standard imposes five global conditions. First, there's the requirement for overall governance, which is stipulated in Clause Five. Governance is a general term that describes the coordination of the entire effort. In the case of 21434, we are talking about creating a comprehensive framework of cybersecurity policies that both align with the organization's business purposes and define the organization's solution. These policies regulate the internal and external actions undertaken in the assurance process.

Procedures are the specific means to implement a governance process. These must be tailored to each policy. These procedures represent the organization's management solution. The requirements are itemized in Clause Six of the standard in the form of specific outcomes which will satisfy one of the particular criteria of the process.

Finally, there are the everyday operations that must be performed in an end-to-end fashion in the lifecycle. Requirements for this are specified in Clauses Nine through Fourteen of 21434. They are explicit actions that turn a defined procedure into specific activity in the local setting. These practices may differ as settings and products vary. But each activity will implement some integral aspect of the process. The outcomes of these actions are audited and documented to demonstrate compliance.

Two significant outside factors are also addressed. These are specified by the final three Clauses of the standard. First, the risk management process identifies threats, analyzes risks, develops mitigations where necessary, and communicates the findings across the organization. This is specified in Clauses Eight and Fifteen of the Standard. Finally, Clause Seven species best practices to address supply chain risk issues and is essentially a new feature in any standard for cybersecurity.

But wait… There's More?

Still, UNECE R-155 isn't the only regulation the OEMs will need to comply with. The other one is UNECE Regulation No. R-156. This regulation accompanies R-155, and it will be enforced in the same fashion. UNECE 156 requires the presence of a comprehensive software update management system (SUMS). For what ought to be obvious reasons, over-the-air (OTA) updates are a particular target for R-156 assurance. The SUMS manages in-vehicle software updates under the R-156 criteria. That requirement applies to any vehicle that allows software updates, which is essentially every car today.

In essence, R-156 stipulates the creation of a documented baseline of software configuration items (SWCI) for every applicable initial and updated software version utilized by a vehicle type. The items in that baseline must be uniquely identified and labeled.

What Does This All Mean?

It should be evident that any efforts to improve the cybersecurity of automobiles will introduce time-consuming and expensive new wrinkles. So, the obvious question is, what's the point of doing it? If this were 1957, or even 1997, there wouldn't be much reason for wasting your valuable time. However, programmed logic controllers are everywhere in your vehicle, from software-defined radio (SDR) to the CANbus and its network of vehicle ECUs. And that isn't even to mention the prospective world of self-driving vehicles. Your automobile is a complex digital ecosystem where failure in any onboard device, for instance, an unauthorized OBD or RFICD access, could lead to disaster. Hence, there has to be a well-defined and highly organized effort to counter potential cyberattacks in this brave new world of digital technology.

About the Author

Dan can be reached online at dan.shoemaker@att.net, or Dan Shoemaker| IEEE Computer Society

Long-Term Impacts A Data Breach Can Have on Your Business

Ways To Protect Your Business from A Data Breach

By Grant Gibson, Executive Vice President, CIBR Ready

The average data security breach takes less time to pull off than it does to prepare a cup of coffee.

While the main focus of any organization who experiences a hack is solving the issue quickly and addressing their employees, it turns out there are a number of long-lasting effects that can cause potential damage to your business. These may include a hit to company reputation, revenue loss, data loss, and disruptions in operations.

As the risk of cyber security attacks and data breaches increases each year – as highlighted by recent news headlines – it is imperative to learn about the possible long-term impacts they can have on your business and how to prevent them.

Loss of property

When a data breach occurs the hacker can gain access to company-sensitive files that may include financial information, personal details, or confidential documents such as contracts. Many times, they will

steal the files and the business will lose the fundamental information they need to run smoothly. If a backup does not exist, it can take months, or even years, to rebuild the documents.

In addition to stealing information there have been many accounts of hackers tricking employees into transferring company funds.

Halt of operations

Data breaches are almost always unexpected and cause a disruption in operations if a mitigation plan was not arranged beforehand. Work may not be able to resume as normal without the critical data that was stolen. Since it can take some time to recover or rebuild data, the business may have to pause working conditions until it is resolved.

Hit to company reputation

Nothing truly disappears on the internet. If a business faces a data breach, it may attract negative publicity and decrease the trust customers have in the company. In the long term this might impact potential new business opportunities, talent recruitment and overall dependency. This is why it's so important to do everything possible to prevent a breach in the first place, but if you do suffer a breach, transparency is key. Inform your customers immediately of the breach. Once you know exactly what data was compromised, share this information as well. Rebuilding a company's reputation after an incident like this can take a great deal of time and patience.

Loss of business and revenue

Reputational damage could also lead to a loss of customers and, in turn, a decrease in sales. With customers having less trust in the company, you will likely lose business and as a result, lose revenue. The business will also lose revenue by having the extra expense of remedying the data breach. Add to this the potential legal fees and compensation to customers and you can see the detrimental long-term effects a data breach can have on your business. So how can businesses prevent these risks in the first place?

Educate employees

Not everyone is aware of cybersecurity safety tips, so it is critical to ensure everyone is on the same page with best practices within the company. In fact, according to a study by IBM, 95% of cyber attacks are caused by human error. Host a brief, refresher lesson every so often to make sure employees remember the safety tips and use them in their everyday tasks.

Encrypt data and update software regularly

Data encryption is when data is translated to a unique code or language that requires a key to understand it. A password can also be used with data encryption. Even when a data breach occurs, the hackers will not be able to understand the data without the key. Your company can decide who has access to the key, which reduces the risk of hackers gaining the key and increases accountability when/if something goes wrong.

Updating your software regularly will also ensure that you have the best and most reliable systems. Using older software makes your equipment vulnerable to these attacks. There are also programs that check your software to make sure everything stays up to date.

Create an emergency plan

Having an actionable plan in place for a potential cyber attack ensures all employees know what to do to solve the situation properly and efficiently. Being transparent and informing customers what could happen with their information also helps the customer place trust in your company.

No matter how small or large your business, you should take every step to prevent a data breach, and this includes preparing for the worst. From financial loss to reputation management, the long-term fallout of a data breach can be devastating—especially if you don't have safeguards and a recovery plan in place. To bounce back from the possible long-term impacts of a data breach, it is important to identify what went wrong and implement policies that prevent this from happening again.

About the Author

Grant Gibson, Executive Vice President, CIBR Ready. He has more than a decade of experience in the cybersecurity industry and is the Chief Information Security Officer at CIBR Ready, a cybersecurity think tank headquartered in the Triangle. Gibson also serves as chair of National Initiative for Cybersecurity Education where he provides a voice of leadership to emerging Cyber technology education standards in the United States. He is a proud veteran of The United States Marine Corps, serving as a critical Communications Chief and pioneering IT instructor. Grant can be reach at https://www.linkedin.com/in/grantgibson1/ and at our company website https://cibrready.com/

Getting Ahead Of The Latest Threat By Perception Point

By Karen Krivaa, Chief Marketing Officer

What is Perception Point?

Perception Point was founded in 2015 by three innovators who served in elite cyber units in the Israeli Intelligence Corps. They initially developed and patented a technology focused on Zero-days and N-days; highly dangerous advanced persistent threats (APTs), which are extremely hard to detect and even harder to prevent. The HAP™ (hardware-assisted platform) was born. HAP is a dynamic scanning engine (next-gen sandbox) that detonates content on Windows and macOS, leveraging CPU Tracing to, in near real-time, detect malware and zero-day attacks at the exploit stage, in a deterministic manner without relying on known signatures, or historical data.

Perception Point leveraged this game-changing technology as just one of its multi-layered advanced detection engines along with isolation capabilities to build a comprehensive SaaS solution that isolates, detects, and remediates any content-borne attack across an organization's main attack vectors, including email, cloud collaboration apps and web browsers.

Perception Point has been built as one platform that detects and prevents all threats including phishing, BEC, ATO, malware, ransomware, APTs and zero-days and spam, well before they reach enterprise users. Cloud-native by design, Perception Point is deployed with a few clicks in just minutes, with no change to the enterprise's infrastructure, and requires very little work on the side of enterprise security teams. The company offers a significant value-added service through its managed Incident Response, which is included as part of the solution at no additional cost, and boasts an expert team that serves as a force multiplier to an enterprise's SOC team.

Perception Point supplies unparalleled enterprise-grade cyber protection for organizations of any size, covering the main attack vectors threatening enterprises today, all without disrupting business continuity or changing the way people work.

Perception Point is rapidly growing its customer base, and is externally validated by numerous third parties. In 2021, the company reported that it tripled its annual recurring revenue and customer base for 2 years in a row and was recognized by Gartner for the third time running as a leading Integrated Cloud Email Security Solution (ICES). In June 2022, SE Labs awarded Perception Point an AAA rating for email security services protection, ranking #1 among several competing security providers. SE Labs tested a range of email security services from well-known third-party security vendors and email platforms and the results found that Perception Point achieved a 'remarkable' 100% Total Accuracy rating, detecting every threat featured in the test, and returning 0% false positives.

What is Perception Point Capable of?

Cloud migration and digital transformation trends began changing the way companies do business and how people communicate, with 5–20 different communication channels being utilized on average by enterprises. This was supercharged over recent years by the start of the COVID-19 pandemic and the introduction of the hybrid work era that has driven enterprises to adopt a range of modern SaaS and cloud-based tools including email, cloud collaboration apps and storage to solve various issues that come with the decentralized workspace. The accelerated deployment and adoption of these tools, along with the need for remote access to organizations' sensitive data, has not allowed security teams to catch up. Many organizations are blind to the potentially malicious content that can be uploaded and shared to their networks, and, at the same time, they are not protecting their sensitive data from managed and unmanaged devices. When combined with the increasingly sophisticated and aggressive tactics of threat actors, Perception Point was compelled to develop an advanced solution to better safeguard the organization.

As a one stop shop for the isolation, detection, remediation of all threats across the organization's main attack vectors - email, web browsers and cloud collaboration apps, Perception Point provides unparalleled protection to reduce breaches, lowers IT friction and through its managed service reduces the SOC resources required in the organization - all while ensuring user productivity.

Perception Point uniquely provides seven layers of next-gen detection capabilities, including the aforementioned HAP™, which operate against any type of attack via text, files and URLs across the main attack vectors: email, the web, and collaboration tools. This results in not only the best detection

rate in the market, but also the lowest false positive rate. The system dynamically scans 100% of content (including embedded files and URLs) at an average scan rate of 10 seconds at an unlimited scale, compared to legacy sandboxing solutions that can take up to 20 minutes and cannot dynamically scan all content.

The HAP™ is a patented next-gen sandbox technology which leverages Intel's Processor Trace to achieve unprecedented visibility into advanced attacks. All content is unpacked and dynamically scanned without tampering with files. HAP uses CPU tracing as opposed to application behavior and signatures in order to accurately detect APTs and zero-days in near real-time on both Microsoft and Mac – a duality that other solutions have not been able to achieve.

Fueled by this seven-layer advanced detection system, patented isolation technology and a managed incident response service, Perception Point can isolate, detect, and remediate all attacks across both email, collaboration channels, and web browsers.

The SaaS-based Advanced Threat Protection System for Email, Cloud Collaboration Apps as well as the Advanced Browser Security solution are entirely cloud-native from their original design. This provides the speed that customers require, even at scale.The capability to create on-the-fly rules and logic, and automatically update the system to deal with new threats, requires no effort on the part of the customer. The user-friendly nature, as well as the speed, scale and accuracy of Perception Point, is key to its product offering.

The goal of security teams is to protect their organization as well as the company's customers; however, this needs to be balanced with daily business continuity and user productivity. Perception Point's speed and transparent nature ensure that employees or customers do not have to wait for an email or for a file to arrive via a collaboration channel, or experience web browsing delays. Online services that allow third party uploads of files and who promise "real-time" service cannot afford to use inefficient and slow threat protection.

In March 2022, Perception Point acquired Hysolate, a next-gen web isolation platform. This allowed the company to release the Advanced Browser Security solution in July 2022. The solution fuses patented next-gen web isolation technology and Perception Point's unmatched, enterprise-grade multi-layer detection engines, and due to Perception Point's focus on usability has the ability to be installed on all standard Chrome, Edge and Chromium-based browsers. This combination delivers the unprecedented ability to isolate, detect and remediate threats from the web while also securing access to sensitive corporate apps via an isolated, trusted Chrome or Edge browser - preventing data loss by design on both managed and unmanaged endpoints. The availability of the Advanced Browser Security solution has allowed Perception Point to become a one-stop-shop for isolating, detecting and remediating all threats across an organization's top attack vectors – email, web browsers, and cloud collaboration apps.

With the oft-mentioned talent shortage that has plagued the cybersecurity industry over the past decade and the constant need for companies to reign in their outgoings and cut costs, especially in the unique economic circumstances of 2022, enterprise Security Operations Center (SOC) teams are frequently overworked and overburdened - they lack the resources to deal with the challenges they face at the required speed. Perception Point has always emphasized that a first-class customer experience is key, and the company saw a real need for tools to bolster enterprise security operations. Therefore, the

company developed a 24/7 managed Incident Response service, included with all Perception Point offerings, that efficiently analyzes, manages and remediates incidents using AI, ML, and human-powered analysis – a lifeline which provides some breathing room for understaffed and overworked cybersecurity teams. The service is an extension of SOC teams, and as a result Perception Point can reduce SOC team resources by up to 75%. Cyber experts analyze incidents to ensure that if something bypasses the system it is immediately remediated across all protected channels. Any update related to new threat intelligence is immediately uploaded so that it can be intercepted the next time it is encountered. End-users can even upload any file or URL that they think may be malicious to be checked by the system and the Incident Response service.

What Does the Future Look Like For Perception Point?

Currently Perception Point covers advanced email security, web browser security, cloud storage security (on Dropbox, OneDrive, SharePoint, Google Drive, S3 Buckets and more), security for Microsoft Teams and the ability to protect proprietary channels via an API. It is available through the Salesforce AppExchange to provide Salesforce security, and the AWS Marketplace.. However, going forward we continuously expand the security coverage offerings through additional integrations and availability on other major marketplaces.

We believe that as attackers become more sophisticated, our solutions need to keep up to prevent attacks. Thus, we are investing in innovative methods, ML and advanced algorithms to maintain the highest detection accuracy in the market. We continue to invest heavily in Mac-based threats as Mac-specific vulnerabilities grow more frequent.

From a business perspective the company has shifted to a partner-first strategy across the globe. The company plans to triple their revenue for the third year in a row in 2022.

About the Author

Karen Krivaa possesses a strong high-tech background and over 20 years of experience in product and portfolio solutions marketing and corporate marketing management. Karen's executive vision and belief in "team" are the core tenets that drive the company's strategic marketing planning and execution, as well as awareness and customer acquisition efforts across all channels. Prior to joining Perception Point, Karen held leadership positions in companies including RADVISION, Alvarion, NICE, Applied Materials and GigaSpaces. Karen holds an M.Sc in Applied Chemistry and MBA from the Hebrew University of Jerusalemcan be reached online at https://www.linkedin.com/in/karen-krivaa-314505/ and at our company website https://perception-point.io/

Low-To-High-Side Development in The Public Sector

Low-to-High-Side Development

By Marc Kriz, Strategic Account Leader of National Security Programs, GitLab

The stay-at-home orders put in place at the start of the COVID-19 pandemic were a catalyst for the rapid – and previously unprecedented – adoption of remote work in the public sector. This was particularly challenging for the intelligence community, and other departments working in primarily classified, or high-side environments.

For decades prior, software development in the public sector could only occur on-site. When the stay-at-home orders were put in place, government leaders were forced to either slow down development by utilizing a reduced team of essential personnel, until all teams could return back to the office, or adjust to the new way of working – through low-to-high-side development enabled by the adoption of DevOps technology and culture.

Government agencies varied broadly in their approaches to implementing remote work. The agencies that focused on low-side – or unclassified – development were able to keep their missions going, and found an increased ability to develop code on the low side much faster than they could ever before.

As remote work continues to solidify its place as the new way of working, it's critical to create new processes that allow developers to work remotely while still being part of the development process. Let's walk through how to bring low-to-high side development to life, and the tools and organizational shifts necessary to do so.

Why Implement Low-to-High-Side Development?

Low-to-high development is critical to improving speed-to-mission, developer productivity and experience, and most importantly, creating more innovative products, all while remaining secure by design. Many government agencies today work across a number of classified and siloed networks, which can make collaboration extremely challenging, and at times, nearly impossible.

As these organizations attempt to scale, each point solution tool must be configured, managed, troubleshooted, and maintained in order to work with the other point solutions tools within that toolchain. With each duplication, toolchains become even more complex, turning toolchain management into its own time consuming, and cost prohibitive task. These legacy tools and processes oftentimes result in siloed teams, poor collaboration, and increased bottlenecks – ultimately slowing delivery time and halting results.

Adopting a consolidated, singular end-to-end software development platform can enable faster low-side development. This approach allows developers to stay in one interface throughout the cycle and get more work done without having to rely on disparate tools, stitched together to make a disjointed toolchain and inefficient software development cycle. A comprehensive software development platform also enables developers to collaborate within the solution with government leadership and program management, keeping everyone on the same version of the truth. All of this can be accomplished within distributed teams, without needing to be on-site.

Best Practices for Low-to-High Side Development

A typical low-to-high side environment has one team of developers, UX/UI designers, and project managers working on the low side. They are able to build out the initial code, create issues, and collaborate in a non-classified environment. From there, they are able to pass the work over to the classified environment, or high side, within the same platform to finalize the work. By using a consistent toolchain across environments, all relevant context to the code is passed over from the low side, including artifacts, versioning, audit trails, reviews, and testing results.

Typical application segmentation leads to segmented environments that are similar, but built through different processes. Although this works in theory, in practice it is made challenging when each environment has the same parent organization, resulting in redundancies and inefficiencies. In these

situations, organizations often double up on work, leading to a loss of productivity and difficulty collaborating – and as organizations grow, and expectations on speedy software delivery grow steeper, the challenges grow as well.

Organizations should seek out end-to-end solutions that have security baked into every step. By integrating security capabilities into the development workflow, developers can be alerted immediately to new vulnerabilities in every developed line of code. Many security professionals have been made to believe that development velocity is the enemy of security. In some cases, this is true. But by bringing security close to the developer, teams likely can produce more secure code even more efficiently than sending code to a third party scanner. A single source of truth allows developers to drive their mission forward while ensuring that security professionals have more visibility into any security risks that may arise throughout the development process.

Enabling Telework Through Low-to-High Side Development

As the effects of the pandemic begin to slow, some agencies have pushed the intelligence community to return to working high-side and in-person once more, despite the new level of efficiency and productivity enabled by telework and low-to-high side development. While the widescale adoption of remote work has been embraced by the private sector, many in the public sector have been hesitant to embrace telework beyond the short-term.

By forcing people to return in person, organizations risk losing out on top talent for the sake of geography. Unlike the years prior to the changes the COVID-19 pandemic necessitated, agencies could seek out the brightest talent from all corners of the country. The return to the office could lead to turnover like that the Great Resignation that occurred in the private sector. Government agencies are competing with all other organizations to win talent, not just other public sector organizations.

Low-to-high side development is a proven method that allows developers to focus on work that drives their missions forward – not managing complex toolchains or completing redundant work. But the greatest shift of all in the next stage of remote work and development is a mindset shift.

It's critical that government leaders prioritize a mindset of innovation, collaboration, and transparency alongside the adoption of new development processes and technologies – including remote work. The public sector is at a turning point – US Federal, State and Local governments can either revert to the pre-pandemic methods of software development, or identify seamless, real-time development processes that deliver software efficiently and securely, and allow teams to deliver truly innovative solutions.

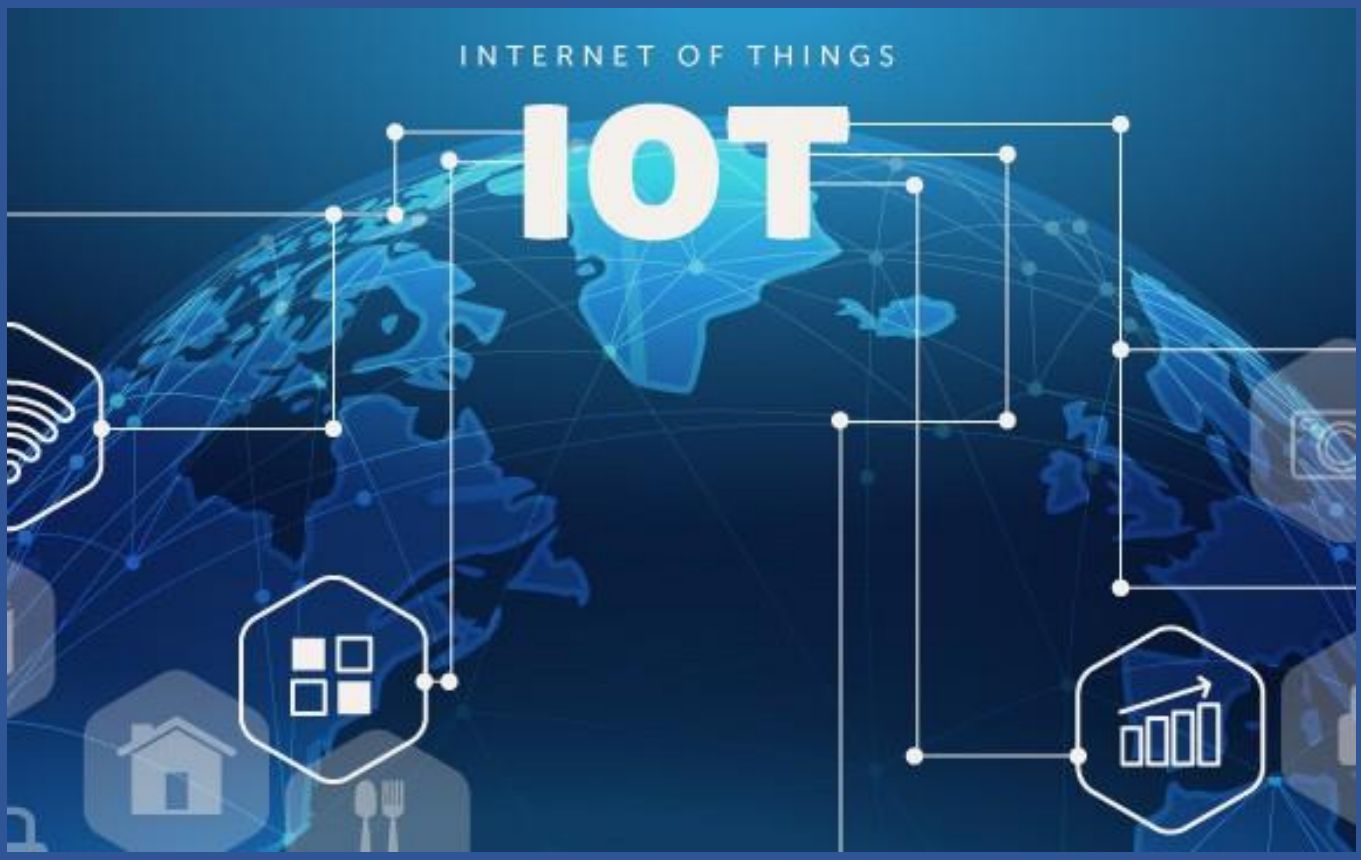
About the Author

Marc Kriz is a Strategic Account Leader of National Security Programs at GitLab Inc., the DevOps platform. GitLab's single application helps organizations deliver software faster and more efficiently while strengthening their security and compliance.

Since joining GitLab in 2018, Marc has been focused on driving innovative, end-to-end DevOps transformation in the National Security Community. As a technology specialist and trusted advisor to the U.S. Intelligence Community, he works with government agency clients and industry partners to assess and solve complex challenges that support the mission of protecting the nation's citizens, infrastructure, and data.

Prior to joining GitLab, Marc supported National Security programs at Cloudera, SAS, and HP. As an early employee at Compaq Computer, Marc was fundamental to launching, building, and leading the company's successful Midwest channel sales program.

Marc holds a B.A. from Eastern Washington University.



Overcoming Security Hurdles for IOT Projects

By Phil Beecher, CEO and President, Wi-SUN Alliance

Five years ago, Wi-SUN Alliance published its first Internet of Things (IoT) 'state of the nation' report.

At the time, we were not surprised to see security as one of the main concerns among survey respondents (IT decision makers who are IoT adopters in UK and US organizations), with the majority ranking security as one of their top three challenges when rolling out IoT. But attitudes – and barriers to adoption – are changing.

This year we revisited the study to see how attitudes and adoption patterns have changed within organizations across a range of different industries, from energy & utilities and telecommunications to construction and government.

The message is loud and clear, IoT is now a bigger IT priority than ever across all sectors. More than 90% agree they must invest in IoT technologies over the next 12-18 months, to help gain competitive advantage, reduce operational costs, and create business efficiencies.

Looking at the two studies over a five-year period, it's clear that there are more companies not just thinking about the technology, but also planning to roll out IoT initiatives. These include more established uses cases for security and surveillance, distribution automation and advanced meter infrastructure. But it's encouraging to see growing enthusiasm for other IoT applications designed for smart cities, including traffic management, smart parking, and electric vehicle charging.

So, with the market maturing and a growing range of IoT solutions and devices available, organizations are becoming more ambitious and open to the idea of planning and deploying services and applications. Such projects, however, can remain challenging.

Fewer security worries, but data privacy concerns grow

Security remains a challenge for some organizations, but it's becoming less of a concern five years' on. Respondents ranking security as one of their 'top three challenges when rolling out IoT' fell from 58% in 2017 to 24% in 2022.

The number of respondents viewing it as a technical challenge also fell, from 65% in 2017 to 42% in 2022, indicating fewer concerns, but still highlighting it as an issue. Organizations might be less worried about security, but it is still on their risk list.

While security is seen as less challenging than it used to be, there are growing fears over data privacy.

IoT projects like smart metering, streetlighting and smart city applications using hundreds and possibly thousands of devices and sensors, have the potential to generate huge amounts of data. Even if this information is secure, handling it responsibly represents a privacy risk. Managing large volumes of data is technically difficult, especially when regulators interpret it as sensitive personal information. Organizations who mishandle or misuse it risk running into compliance issues.

Data privacy regulation was ranked the second-highest political, economic, or social challenge for IoT adopters, with 36% placing it in their top three just behind the need to reprioritize spending due to Covid and ahead of budget cuts resulting from the pandemic.

Fears over big data have jumped to 19% from 11% placing it in their top three IoT rollout challenges in the last five years, and one in four respondents citing regulatory concerns.

This is no surprise given the focus on data protection in recent years. Since our first study, stricter privacy laws have put pressure on organizations to protect sensitive data, including the introduction of the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA) and other privacy regulations.

There's evidence of a growing number of attacks targeted at IoT devices, applications, and services in recent years, leading to the launch of denial of service (DDoS) attacks. Mirai is perhaps the most well-known IoT attack. Dating back to October 2016, it took advantage of insecure IoT devices, such as CCTV and routers, to launch a massive DDoS attack. Astonishingly, it's still used today by malware developers to attack vulnerable systems, from manufacturing to critical infrastructure.

The journey to IoT is maturing, with organizations becoming more ambitious in their thinking and their approach. It is now a bigger priority than ever across all the sectors, and the scale of what is being planned over the next few years is encouraging.

What is clear is that this journey isn't over and there is still some way to go to true IoT maturity. Obstacles remain and organizations must work to overcome them.

To see the full Wi-SUN Alliance report.

About the Author

Phil Beecher is President and CEO of Wi-SUN Alliance. Since 1997, Phil has played a key role in the development of communications standards including Bluetooth, WiFi, and IEEE and the specification of test plans for a number of Smart Utilities Network standards, including Advanced Metering Infrastructure (AMI) and Home Energy Management Systems.

Wi-SUN Alliance can be reached on Twitter at: @WiSunAlliance and on LinkedIn at: https://www.linkedin.com/company/wi-sun

Patch Zero Days In 15 Minutes Or

Be Breached

By Randy Reiter CEO of Don't Be Breached

Patch Zero Day Software Bugs in 15 Minutes Before the Hackers Arrive

Domestic and International hacker groups are now targeting Zero Day vulnerabilities within 15 minutes of their public disclosure. A Zero Day vulnerability is a recent discovered software bug that hackers can use to attack and compromise application or operating system software. The term "Zero Day" refers to the fact that the software vendor just learned of the software bug. This means the software vendor has "Zero Days" to fix the issue. A Zero Day attack occurs when hackers exploit the software flaw before software development teams have a chance to apply a fix for the software vulnerability.

Most organizations cannot apply software patches to production software within 15 minutes of public disclosure of a Zero Day to prevent hacker attacks that can result in data breaches and ransomware attacks. Palo Alto Networks reported in 2022 that hackers typically start scanning for Zero Day vulnerabilities within 15 minutes of the Zero Day being announced. Once a Zero Day software bug has been publicly announces a fix may not be released immediately. Hackers are aware of this and begin initiating cyber attacks immediately. As a result Zero Days are are big business for both cyber criminals and government-backed hacking teams.

Most Recent 2022 Data Breaches

August 2022. A hacker publicized 22 million QuestionPro email addresses and other data. The same hacker previously successfully breached the FBI and Robinhood.

July, 2022. A hacker posted 5.4 million Twitter accounts for sale on a hacker forum. A few days earlier another hacker posted 69 million Neopets (virtual pet website) accounts to the same forum. In both incidents hackers exploited Zero Days to scrape confidential data from websites.

July, 2022. Hackers stole 20 gigabytes of sensitive data from Marriott International. The sensitive data included flight information and credit card numbers.

July, 2022. Massachusetts-based Shields Health Care Group disclosed they were breached in March 2022. The continental data stolen by hackers included names, social security numbers, medical records, and other sensitive personal information.

Conventional approaches to cyber security may NOT prevent Data Exfiltration and Data Breaches. In 2020 the DHS, Department of State, U.S. Marine Corps and the Missile Defense Agency recognized this and all issued requests for proposals (RFP) for network full packet data capture for Deep Packet Inspection analysis (DPI) of network traffic. This is an important step forward protecting confidential database data and organization information.

Zero-day vulnerabilities that allow hackers to gain system privileges are a major threat to all organizations encrypted and unencrypted confidential data. Confidential data includes: credit card, tax ID, medical, social media, corporate, manufacturing, trade secrets, law enforcement, defense, homeland security, power grid and public utility data. This confidential data is almost always stored in DB2, Informix, MariaDB, Microsoft SQL Server, MySQL, Oracle, PostgreSQL and SAP Sybase databases.

How to Stop Data Exfiltration and Data Breaches with Deep Packet Inspection

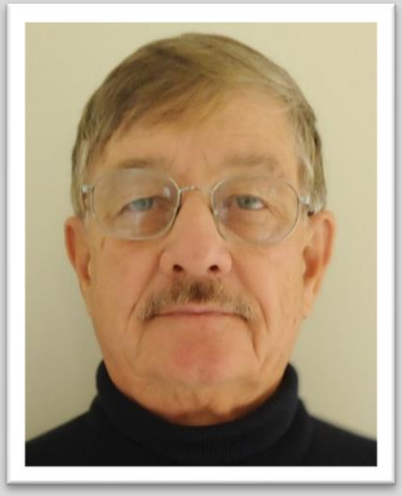
Protecting encrypted and unencrypted confidential database data is much more than securing databases, operating systems, applications and the network perimeter against Hackers, Rogue Insiders, Government-backed Hacking Teams and Supply Chain Attacks.

Non-intrusive network sniffing technology can perform a real-time Deep Packet Inspection (DPI) of 100% of the database activity from a network tap or proxy server with no impact on the database servers. The database SQL activity is very predictable. Database servers servicing 1,000 to 10,000 end-users typically process daily 2,000 to 10,000 unique queries or SQL commands that run millions of times a day. Deep Packet Analysis does not require logging into the monitored networks, servers or databases. This approach can provide CISOs with what they can rarely achieve. Total visibility into the database activity 24x7 and 100% protection of confidential database data.

Advanced SQL Behavioral Analysis from DPI Prevents Data Exfiltration and Data Breaches

Advanced SQL Behavioral Analysis of 100% of the real-time database SQL packets can learn what the normal database activity is. Now the database query and SQL activity can be non-intrusively monitored in real-time with DPI and non-normal SQL activity immediately pinpointed. This approach is inexpensive to setup and has a low cost of operation. Now non-normal database activity from Hackers, Rogue Insiders or and Supply Chain Attacks can be detected in a few milli seconds. The Security Team can be immediately notified and the Hacker session terminated so that confidential database data is not stolen, ransomed or sold on the Dark Web.

About the Author



Randy Reiter is the CEO of Don't Be Breached a Sql Power Tools company. He is the architect of the Database Cyber Security Guard product, a database Data Breach prevention product for DB2, Informix, MariaDB, Microsoft SQL Server, MySQL, Oracle, PostgreSQL, and SAP Sybase databases. He has a Master's Degree in Computer Science and has worked extensively over the past 25 years with real-time network sniffing and database security. Randy can be reached online at rreiter@DontBeBreached.com, www.DontBeBreached.com and www.SqlPower.com/Cyber-Attacks.

Privacy Enhancing Technology Is Crucial for Cybersecurity When Hybrid Working

Ivar Wiersma of R3 discusses the cybersecurity issues presented by the "new normal" and how these challenges can be overcome.

By Ivar Wiersma, Head of Conclave, R3

The practice of hybrid working has been one of the few positives embraced by employers and employees alike in the wake of the pandemic. The ability for employees to work from the office but also from home when needed has allowed for flexibility in most sectors and a general increase in wellbeing.

However, while this new model has fostered greater flexibility, we must also be wary of the issues surrounding privacy and data sharing that it has uncovered, which have the potential to stifle innovation and slow post-pandemic growth.

New normal, new problems

The “new normal” poses several new challenges for cyber security since many businesses have found ways to operate virtually.

Although stay at home restrictions have eased, many companies still allow their employees to work remotely. This has increased the demands and requirements on data storage on the cloud, data security and privacy concerns. With remote working becoming a new norm, online data sharing has become the main mode of working.

At its core, the main challenge that we face today is the inability to technologically enforce what and how third parties are using the data once it is made available in the public domain.

Allowing employees to work from home heightens the need to ensure that the data shared is kept secure, confidential and tamper proof.

To prevent any tampering of confidential data, many businesses simply do not share their confidential data with partners. This is a key challenge for businesses in the post-pandemic world.

In Q1 of 2020, when widespread “work from home” schemes were first implemented, there was a 17% increase in the number of data breaches. This further underlines the importance of ensuring the security of user data for many businesses today.

Catering to growing demand

Information sharing offers great opportunities for companies to build more efficient and resilient business models. However, many businesses are still hesitant to share their data as the space remains difficult to control once the data is made available.

With 75% of the world’s population projected to have their personal data online by 2023, user data security will not only become a responsibility of businesses but a priority for those companies who wish to thrive post-pandemic.

To cater to this online transition, businesses have ramped up their partnerships to collaborate digitally in a distributed environment.

However, this digital world brings with it a host of security risks. Some common causes of cyber breaches include using applications that are riddled with vulnerabilities which threaten the integrity and security of classified information owned by enterprises.

To prevent such threats, it is in the firm’s best interest to adopt programs that protect their classified data while it is at rest, in motion and in use. To do so, it is important that firms deploy a security-by-design approach, whereby applications and services are designed to protect privacy first.

Potential solutions to these issues

One possible solution for companies who wish to enhance the security of their complex enterprise structure could be to adopt confidential computing.

This privacy preserving technology encrypts data while it is still in its processing stage, enabling firms to securely aggregate their datasets to solve shared business problems without revealing the raw enterprise data to anyone.

Additionally, it secures the processed and consolidated data from multiple databases as well as the insights generated from them, disallowing access from any party and minimizing the risk of data manipulation.

This new form of data processing can protect policymakers and relevant stakeholders from data breaches, since raw data is not being distributed or made available to external parties. In fact, many enterprises are starting to realise the benefits of adopting confidential computing in today's distributed work environment.

A report published by Everest Group, for example, forecasts that the confidential computing market could grow from US1.9 billion in 2021 to US$54 billion by 2026.

Alongside confidential computing, a "zero trust" approach could also be used to compliment the protection it provides and strengthen its impact. A 'Zero trust' security model requires that a transaction be verified for it to be successful to prevent any security breaches. This implies that all transactions made – even if from within the network - must be verified. Between 2020 and 2026, the market is expected to grow from US$19.6 billion to US $51.6 billion.

However, one challenge of the 'zero trust' architecture includes the strict requirements of a 'zero trust' network and its implementation. Some of these requirements include ensuring network security, infrastructure security and identity security. But we can expect this to be made easier thanks to emerging technologies that are keeping up with the demand for enhanced security.

Looking ahead

With the rise of remote work and a hybrid cloud environment, traditional networks are increasingly unable to keep up with the ever-growing security needs of firms.

If firms wish to effectively adapt to this "new normal" of hybrid working and promote growth in a post pandemic world, confidence in data sharing must improve. To effectively accomplish this, privacy-enhancing technology like confidential computing should be the answer.

About the Author

Ivar Wiersma is the head of Conclave, R3's confidential computing platform. Before R3, Ivar started ING Wholesale Banking's Innovation department and led the Blockchain and Advanced Analytics teams. Ivar can be reached online at "Ivar Wiersma" on LinkedIn and at our company website: https://www.r3.com

Protecting Government Data at The Intersection of Zero Trust and Open Source

By Rick Vanover, Senior Director, Product Strategy, Veeam

As the federal government continues its emergence from the pandemic, its information technology strategy is being influenced by two compelling, but divergent trends—zero trust and open source.

Thanks in part to the White House's 2021 Executive Order on Improving the Nation's Cybersecurity, the most prominent of these trends may be zero trust adoption. But some fear cybersecurity gain could be weakened by the growing popularity of open-source software.

According to the 2020 Federal Source Code Study, 80% of the more than 6,800 federal software projects listed on Code.gov are open source, allowing developers to innovate quickly, lower cost for deployment and provide more vendor choice.

Open source's crowd-supported approach to innovation could improve cybersecurity but the transparency of the source code can allow attackers to creatively inject malware. A 2020 research paper entitled the "Backstabber's Knife Collection," detailed 174 malicious software packages "used in real-

world attacks on open-source software supply chains," between 2015 and 2019 to highlight the challenges that the software applications face from potential breaches.

While the open-source community is adept at monitoring and quickly patching vulnerabilities, the diffuseness of open-source packages means that when an attack occurs, it can spread quickly before being detected. Once those open-source software applications are breached, it becomes difficult for a zero-trust architecture to combat the attack because the software infected with malware has already been accounted for in the IT environment.

And while zero trust can help secure legitimate points of access and limit data exposure, it cannot itself recover compromised data in the event of an attack. Zero Trust is an architecture, a design, a mindset – not a foolproof copy of data, nor a single product.

To prepare for the potential impact of attacks on open-source supply chains, agencies need to think beyond traditional zero trust methods to put in place defensive strategies that account for the complete supply chain and a strong data protection plan should a breach occur.

Protect the entire software supply chain

The dependency on open-source software is not expected to ebb, especially in the public sector, where the federal government continues to see its value in innovation.

That means in addition to zero trust protections, IT officers also need to incorporate cybersecurity efforts against possible software supply chain attacks. This could include steps like requiring a software bill of materials (SBOM) to provide IT personnel with data on the components of a software product.

It also requires strong cyber hygiene from IT managers, including frequent patching and updating of software components across the enterprise to protect against possible vulnerabilities.

Safeguard your data

To combat an attack that may have already occurred, IT managers need to ensure their data is also protected.

As we discovered with NotPetya, a strain of malware first identified in a 2017 attack on Ukraine, the attack itself was originally thought to be ransomware installed in a legitimate software update that merely left users unable to access their data. However, it was ultimately found to be a fast-spreading wiper attack that irretrievably destroyed data on infected computers and globally caused $10 billion in damages.

Because of the inherent risk of these threats, it is vital for enterprises to implement a data backup strategy that is reliable, verified and tested and can be deployed across all mission-critical workloads.

That means taking steps like ensuring that a backup's integrity is verifiable from the moment it is made and quickly retrievable in the event of such an attack. Backups must also possess resiliency from attack

— either by being stored on removable drives, protected in hardened repositories, secured with end-to-end encryption or safeguarded by ransomware remediation capabilities.

Without full visibility into the software supply chain, it may be difficult to identify vulnerabilities. While efforts to secure the software supply chain are ongoing, having an expansive data protection strategy across on-prem, in the cloud and within other software-based systems is a critical failsafe and therefore the most comprehensive form of protection.

Zero trust remains an important strategy in helping defeat potential cyberattacks, but it is only one strategy to be deployed against increasingly sophisticated adversaries. To help ensure that government is resilient in the face of such threats, it is imperative that it has at its bedrock a strong data protection strategy.

About the Author

Rick Vanover is an expert in intelligent data management and backup. In his role at Veeam, Rick sits at the crossroads of many types of storage. Whether it is storage systems, critical application data, data in the cloud or data anywhere in between, Rick has experience in the data management practice as IT practices change with new technologies. Follow Rick on Twitter @RickVanover.

Protecting The Enterprise in The Digital Era

What Organizations Need To Know In The New Workplace

By Anurag Lal, President and CEO, NetSfere

Over the past two years, the entire globe has experienced a takeoff in the digital era - specifically within the enterprise. Naturally, cybersecurity concerns have advanced alongside these developments, and a myriad of issues and concerns, especially regarding data and privacy, continue to rise to the surface. As the workplace becomes increasingly decentralized with remote and hybrid work becoming the norm, cybersecurity must move to the forefront, becoming a top priority for enterprise leaders.

Pre-pandemic security efforts are no longer adequate in maintaining the utmost protection of company information. In order for organizations to fortify the role cybersecurity plays in both their digitization efforts and the overall success of their business, there are crucial elements that must be considered and reflected – and acted – upon.

Employees are your weakest link.

Almost 100% of all data breaches within organizations are a result of human error. With employees no longer under the same roof, IT control becomes increasingly more difficult for enterprises with employees across not only multiple Internet networks, but in many instances, different states. Additionally, with the

growing popularity of BYOD (bring your own device) policies, security levels are more likely than not significantly lower than in a traditional, pre-pandemic office setting as IT cannot fully control personal devices to the same standard. Employees are accessing company emails, websites and other materials on their personal cell phones and laptops that have little to no protection compared to their work devices.

How do we ensure that remote and hybrid employees and their work are protected equally? The answer is simple: education.

It is up to enterprise leaders, IT and human resources departments to continuously supply and deploy educational materials for employees on cybersecurity best practices. Additionally, it is important to note that trends in phishing scams are becoming considerably more sophisticated, appearing more discreet and often targeting new channels, like SMS. It is the employer's responsibility to equip its employees with the knowledge to distinguish such attacks, report them to IT and not interact or engage with them. Companies should also consider a course or class on the matter, repeating it annually and/or with new hires to ensure cyber safety is a priority for each team member.

Implement the necessary tools and systems to protect data at every level.

Your employees may have all the tools they need to engage safely at work, but that alone is not enough.

Any platform or channel where sensitive data, information, plans, documents, records and other confidential files are shared must be protected at every entry point. There are many types and tiers of encryption floating around, but end-to-end encryption absolutely is the gold standard. With the message being decrypted only on the device of the sender and recipient, the chance of an attacker accessing information is depleted. This is vital in the remote era when employees are communicating on digital channels like email and instant message, especially when using their personal devices. Industries like healthcare and finance are more susceptible to attack due to highly sensitive and valuable personal information and records as well as outdated and inefficient systems. In light of recent events overseas, these sectors, among many others, should consider deploying fully encrypted, compliant collaboration channels, ensuring that information is being exchanged securely and end-users are protected as well.

It is also worth enterprises considering adopting a zero-trust framework to further limit employee access to company information and decrease the risk of a human error-related breach. This model requires network users to be verified at every entry point and gives them access to only what is required to perform a task or role. With a zero-trust implementation, unverified users are immediately denied entry to the network, providing a sophisticated level of security to the enterprise.

The digital technologies and best practices being implemented by enterprises today are shaping their futures for a safer, more efficient and successful tomorrow. It will pay off in multitudes to take a proactive approach to the protection of your company and teams. Invest in your employees. Safeguard your company data, devices and communication channels. Take no risks.

About the Author

Anurag Lal is the President & CEO of Infinite Convergence Solutions. With more than 25 years of leadership and operating experience in technology, mobile, SaaS, cloud and telecom services, Anurag leads a talented team of innovators who are transforming everyday messaging technology into secure, highly scalable communication platforms that can be leveraged across a variety of markets and segments. Appointed by the Obama administration, Anurag also previously served as a Director of the U.S. National Broadband Task Force (part of the Federal Communications Commission). A frequent contributor on wireless connectivity, broadband and related security issues, Anurag has received various industry accolades, including recognition by the Wireless Broadband Industry Alliance in the U.K. for exceptional individual contributions to the wireless broadband industry. Anurag can be reached on LinkedIn at https://www.linkedin.com/in/anuragl. For more information about NetSfere, please visit https://www.netsfere.com/.

Source Code Protection Market

Do we need backup software for DevOps ecosystems?

By Marta Przybylska, Marketing Manager, GitProtect.io / Xopero Software

Today, the software is the driving force of the world, and developers are game-changers. There are approximately 40 million people that are involved in writing code or programs. Thus, the real revolution is happening on the other side of our screens. And with thousands of startups coming up worldwide, the demand for developers and source code is soaring.

Data is compared to Oil in the 18th Century driving the digital economy more than ever. And developers are responsible for generating most of the data processed daily. How many? Well, this number grows at an exponential rate. In 1992 it was 100 GB generated daily, in 97' - 100 GB per hour and today it reaches the number of 50 000 GB per... Second.

Source code, as an Intellectual Property is one of the most crucial business assets. When it comes to startups, tech or software development companies - is a key factor of a company valuation. There is no wonder that businesses put more and more effort and expenses into cybersecurity. However, there is one area software development companies cannot underestimate. Protecting the source code itself.

Market potential

GitHub claims to have over 56 million registered developers, including 72% of Fortune 50 companies. It makes it “the largest source code” globally. GitLab estimates its users for more than 30 million while Atlassian’s Bitbucket reached 10 million business users.

Software developers use version control systems like Git and hosting platforms like GitHub, Bitbucket, and GitLab on a daily basis. Those are places where code is created, hosted and where the development teams spend thousands of hours to write, support, and improve projects. Can you imagine how much it would cost tech companies to lose access to such valuable data? And is it even possible?

Source code, even if hosted within such reliable hosting, might get unavailable or lost. While those services are considered accessible and proven, no service provider can ensure customers with 100% availability.

Ups, something went wrong...

Downtime and outages are one of the reasons. For example, in June 2020 GitHub experienced a major outage that lasted for hours and impacted millions of developers. In 2017 the huge outage happened to GitLab.com and made its services unavailable for hours. The company lost some production data that was unable to recover.

How about cyberattacks? In 2019 most of tech media reported that attackers were targeting Bitbucket, GitHub and GitLab accounts, wiping code and commits from many repositories leaving behind only a mysterious ransom note.

Finally, we have to mention the nightmare of every IT administrator and cybersecurity professional – human errors. Branch deletion, synchronization problems, or some intentional malicious behavior - that’s just some of the developers’ mistakes (intentional or not) that can put source code in danger or wipe it out.

Shared responsibility

Like most SaaS providers, also GitHub, GitLab, and Atlassian rely on shared responsibility models. Those define which security duties are handled by the service provider and which belong to the organization. In a nutshell: version control systems providers are responsible for maintaining the infrastructure and making sure data is available and accessible. Companies as users are responsible for protecting their GitHub, GitLab, or Bitbucket data in general.

While there is a lot of management, monitoring, code quality, and security apps available in both the Atlassian and GitHub marketplace, there is a big niche when it comes to backup software.

Source protection today

So, how do companies handle repository backup today? Generally: they don't at all. And if so, there are usually DIY methods based on git-clone commands and self-written scripts. Some businesses rely on snapshots of their local git instances. But those approaches have their limitations - high-long-term costs of script administration, no backup verification, no automation, and no restore guarantee which could potentially make backup useless in case of any event of failure.

The source code backup market is still crawling - the first backup solutions start to appear as a result of internal development teams' needs. However, there are also some established and experienced backup vendors, that discovered and decided to develop this niche, making it the most professional backup software for GitHub, GitLab and Atlassian environments.

Considering Intellectual Property value and GitHub and Atlassian's emphasis on adequate data protection, we might foresee that GitHub, GitLab and Atlassian backup, in the footsteps of Microsoft and Google Workspace, will become another, key data protection field.

About the Author

Marta Przybylska, Marketing Manager at GitProtect.io/Xopero Software. From the very beginning of her career, she has been associated with the IT industry and technology startups. For over 3 years has been related to the cybersecurity market – working at Xopero Software, a backup vendor on the project code named GitProtect.io – the most professional, fully manageable GitHub and Bitbucket backup software (available on both GitHub Marketplace and Atlassian Marketplace). Company websites: https://xopero.com/ and https://gitprotect.io/

The Implications of Zero Trust for Data

By Julius Schorzman, Director of Product Management, Koverse, Inc., an SAIC Company

Zero Trust is a hot topic in network security. For those not familiar, zero trust is the “never trust, always verify” premise applied to every device, with an eye to protecting the corporate network. In many ways, this architectural approach represents the ultimate security posture.

That said, most zero trust approaches today have a flaw. Two, actually: people and data.

The people flaw might be colloquially termed “the insider threat problem.” In short, how do you protect against rogue actors (or good actors that have been phished)? With the right credentials, that actor has the keys to the kingdom.

The data problem is even more pernicious: how do you protect PII, confidential and classified information without creating data silos? Most larger companies today use some form of a data lake where they ideally collect and physically co-locate *everything* – structured and unstructured, batch and continuously streaming, classified and unclassified, basically all sorts of complex data. There is no way to block, say, a social security number contained in a piece of unstructured data without blocking (siloing) the whole file. These data silos can wreak havoc on analytics, data science and artificial intelligence (AI) initiatives, especially in sectors with a heavy dose of sensitive data, such as financial services, life sciences, healthcare, and of course government.

The problem with previous approaches to zero trust is that it's applied at a network and file level not the data level. In that sense it's a blunt instrument; you either have access or you don't, the data itself is insecure. The irony is that zero trust pushes for perimeterless security, yet what to establish a bolt-on zero trust perimeter around your data storage, and then slice that data up to try to maintain the appropriate level of security.

Let's examine what this means in regard to people and data access.

The People Problem

You may think with zero trust, your data is locked down, and that highly confidential data is safe. But is it? Only authorized users have access, after all. And those authorized users include all your database administrators, your helpdesk staff or any of which may be on contract, and thus be more transitory than typical employees and subject to less scrutiny. Any of these people (employees or contractors) could be phished. Or have a virus on their computer.

Still feeling safe?

Even with zero trust, there can still be issues in configuration and policy management. Anyone who's dealt with common cloud security policies knows these can be onerous to apply to a large and varied set of data and services. An administrator sets up a new cloud database, only to discover it can't communicate with the policy engine or web servers. The natural inclination is to just change settings to "allow" … and now everything works, but your data is open to the internet. Are you certain that all those loopholes have been closed?

The Data Problem

Regardless of zero trust, for most organizations today, data is secured by segmenting it – in other words, creating data silos. Again, this is a blunt, all-or-nothing approach, especially when it comes to unstructured data.

Take a spreadsheet, for example, where two workers, Bob and Alice, need access. Both have credentials and are working from a trusted device. Alice is authorized to view all the data in the spreadsheet, even the confidential information. Bob, however, doesn't have clearance to see the sensitive data, so he needs to work on a copy of that spreadsheet with that information removed. Now you have two copies of the same file. Even worse, once Bob updates the spreadsheet, now someone has to reconcile those changes. This happens over and over across the organization.

Having to silo confidential information can have a significant impact on data science, analytics, and AI, particularly if this data is of mixed sensitivities. Either it becomes off-limits to the people and algorithms that could use it, or the organization has to effectively duplicate storage, management, AI/ML pipelines, etc.

Integrating Zero Trust at the Data Level

The traditional network-centric approach to zero trust does not address these issues. But what if we implemented zero trust, along with attribute-based access controls (ABAC), at the data level instead? What would this look like?

All data would have security labels applied on write, i.e., immediately protected at ingestion. The system should be able to handle all data types – structured or unstructured, streaming or static – in their raw forms, retaining the data's original structure to ensure greater flexibility and scalability.

Attribute-based access control allows resources to be protected by a policy that takes users' attributes and credentials into account, not just their roles, and can allow for more complex rules. And if ABAC is used to protect data at a fine-grained level, it ensures that data segregation is no longer necessary. Unlike the more common role-based access control (RBAC), which uses course-grained roles and privileges to manage access, ABAC is considered the next generation of access control because it's "dynamic, context-aware and risk-intelligent." These access controls can be applied at the level of the dataset, column, attribute-based row, document/file, and even individual paragraphs. In this scenario, people see only the data they need (and are authorized) to see, even if they're looking at the same file.

Let's look at our earlier examples through the lens of zero trust for data. A data analyst could upload sensitive information that would be immediately labeled. Even the database administrator would not be able to view this information – they can manage the system resources, but not view the confidential data therein. Zero trust.

It gets even more interesting when considering the spreadsheet being managed by our friends Alice and Bob. Only one copy of the spreadsheet exists; both Bob and Alice can be looking at it and working on it, but each see and have access to only the data appropriate to their credentials. Technically, Bob would not even know he's not seeing all the data. Again, zero trust.

The Implications of Zero Trust for Data

So, what would this mean for an organization and its data?

First, that data – *all* data, across mixed sensitivities – would be better protected. Because silos are eliminated, all data can be co-located, improving efficiency, and making information immediately available for use. Because we've now got fine-grained control, we can even apply this zero trust and ABAC to search, so that all data, regardless of sensitivity, can be readily indexed and found; users only see the results they're authorized to see. And data scientists can focus on the objectives for their AI and analytics work, instead of the infrastructure.

If this sounds like fantasy, it's not. It's actually the approach that prominent three-letter government agencies use when they have to work with data of mixed sensitivities. That zero trust for data is now making its way into commercial and government organizations of all types, and it promises to have a major impact on how we work with – and protect – data going forward.

About the Author

Julius Schorzman is Director of Product Management for Koverse, Inc., an SAIC Company, which empowers customers to use data to gain understanding and drive mission-impacting decisions and actions. He is an experienced product management executive with a proven track record in product development and knowledge management for high growth enterprises.

Julius can be reached online at https://www.linkedin.com/in/schorzman/ and at our company website https://www.koverse.com/

Threat Modeling: Bridging the Gap Between Developers and Security Architects

By Stephen de Vries, Co-Founder and CEO of IriusRisk

The application security world is known for friction between security and development teams. However, this tension can be eradicated through a development security strategy to bring developers and security architects together: threat modeling.

Protection before it's too late

Threat modeling is the act of conducting security analysis before a system is finalised, or even built, to detect weaknesses and vulnerabilities in the design of the system and to plan for mitigating insecure design. It's looking left and right on the street before crossing, rather than checking for cars when you're in the middle of the road – looking for threats is better done sooner rather than later.

Threat modeling can traditionally be done manually using a whiteboard, running as a workshop where security experts show the product team which practices to avoid or embrace to enhance security. It can

also be done through integrated tools that run the process at scale, across teams and users. Automating threat modeling means developers will be notified of the security gaps during the development process, so changes can be made immediately, as opposed to retrospectively when the product is fully developed.

Threat modeling is an excellent engineering practice as it allows organisations to start security left, building a product that's secure by design to make the process from ideation to launch much smoother. Developers aren't always security experts, so by doing this they can learn to look for some of the weaknesses that regularly appear in the design phase, which has a positive impact on the security culture within an organisation.

Businesses that integrate threat modeling to their product development process have the potential to obtain better quality software and reduce costs as well: fixing finished software is expensive, especially if they have been in production for several years. Threat modeling is a way to identify technical debt that you may not want to take on, as well as a way to identify risk.

Business benefits: Collaboration and team learning

As benefits become more obvious, a growing number of companies are adopting threat modeling as a software development practice. It's especially important for businesses that are growing fast, for whom building a secure product is a top priority: companies don't want to lose the secure culture they spent so much time and effort creating.

Threat modeling as a practice also brings development and security teams together, enabling easy collaboration. This type of collaboration – as opposed to security teams acting as a bottleneck to release products after testing – has great advantages for cyber teams, but also for the product engineers themselves. Security teams can't consistently look at every piece of code that's been written, which is why empowering the development team is crucial to scale security practices. Threat modeling essentially allows companies on a fast-growth journey to grow their security practices as they do, ensuring their products remain secure by design.

Learning is a big aspect of collaboration through threat modeling and we see it very clearly in our clients. Developers are not expected to be security champions, but there are great benefits from the security team explaining retrospectively what worked and what didn't. Once the mistake is understood, it can be avoided. Multiply this by dozens or even hundreds of common security mistakes in the development process, and a business can save massive amounts of time, money and resources by avoiding discovery of these changes at a later stage.

However, this is where we find a challenge: developers don't always want to invest in doing threat modeling and be able to see the benefits. Developers aren't always aware of the consequences of not integrating threat modeling into the development process, or the benefits of doing so. The solution is to make developer teams aware of the many benefits of thinking about security from the very beginning and starting security left.

What's next for threat modeling?

Threat modeling is already part of the development process in many businesses and we'll continue to see it grow and become a common industry practice. Beyond threat modeling for security issues and cyber attacks on the system, we will see it be applied to prevent conflict, trolling, bullying and even AI biases. In the future we will have a more integrated security process that will give development teams a chance to think about the implications of the decisions they are making for user's security inside and outside the platform.

We will continue to see threat modeling develop to become as frictionless and easy to implement as possible, even as a company grows and the technology is used at scale across a product portfolio. More and more organisations are integrating threat modeling with their existing tool kit, which works around standard developer flows.

The current momentum around threat modeling is not just a trend. As more businesses adopt threat modeling as a practice and the security and financial benefits become more obvious, it will evolve from a 'nice to have' to a must in application and software development, bringing engineering and security teams closer together and helping businesses scale securely.

About the Author

Stephen de Vries is the Co-Founder and CEO of IriusRisk. He has a diverse technology background starting as a software developer, firewall engineer, penetration tester and software security consultant. Stephen has over 20 years' experience in information security; the last six dedicated to building a threat modeling platform. He was a founding leader of the OWASP Java Project and contributor to OWASP ASVS and Testing projects, and contributor to the Threat Modeling Manifesto.

Stephen can be reached online at @stephendv and at www.iriusrisk.com

Top 10 Actions to Repel and Recover from Active Directory Attacks

By Sean Deuby, Director of Services, Semperis

Active Directory is foundational to on-premises and hybrid identities that are everywhere in enterprise environments and the cloud today. It is also key to a zero-trust security architecture. As a result, it's a primary target of a cyberattack: Security company Mandiant says that Active Directory is involved in 90% of attacks that it is called in to investigate.

Here are 10 actions to take now to protect your organization against Active Directory attacks.

1. Implement good identity lifecycle processes

Protecting identities and access in your environment is essential to maintaining a secure environment. There are some incredible tools out there to help with this, but you can improve your identity lifecycle processes with something as simple as a calendar. Set review dates, audit access, and run a regular process to:

- Remove inactive users and computers
- Regularly review privileged access, especially paths to Tier 0 accounts and systems
- Regularly update service accounts with long, strong, random passwords

These actions help avoid attacks such as Kerberoasting, which enables attackers to elevate their privileges by gaining access to passwords for service accounts on the domain.

2. Adopt trust security

Consider how best to establish trust in your environment. Within a single forest, all domains trust each other, and you can escalate from one compromised domain to all the others. An Active Directory Forest can be used to create separate areas of trust and access control. Implementing selective authentication forces, you to make security decisions about who has access rather than using a “trust everyone” approach. To be successful, keep the following in mind:

- Ensure SID filtering is active across all trusts between Active Directory forests.
- Consider enabling selective authentication to create a “default deny” trust rather than a “default allow”.

3. Prioritize backup and recovery

Backup and recovery plans and processes are essential to implementing a solid recovery plan. Make sure that your plan is documented and practice it annually, at least; there is no IT procedure whose success depends more upon constant practice than disaster recovery. Time is critical in a crisis, and that’s not the time you want to be relying on an outdated process (or worse, your memory) to restore your critical systems. Most IT professionals document steps they plan to take during regular maintenance windows. Why would you have anything less in place to use when disaster strikes? Doing a dry run also helps ensure that you are correctly following the supported backup methods required by services like Active Directory. (Pro tip: screenshots are not the thing to use here.) Fixing a faulty process is always easier when you are not in crisis mode. Here are some essentials to keep in mind when considering your backup and recovery process:

- Back up every domain, especially the root.
- Back up at least two domain controllers per domain.
- Test your backups regularly. This means actually recover AD from them; “backup successful” messages are not tests.
- Use supported backup methods. Virtualization checkpoints or snapshots don’t count.
- Ensure backups are malware-free.
- Don’t forget to keep offline copies of backups. Offline storage is essential to protect your backups from malware and ransomware. Many an attacked organization has found that its online backups were also attacked and disabled.
- If administration of your backup application is AD integrated, have a “break glass” emergency access method for when AD is unavailable.

4. Consider your Kerberos security

Kerberos (the primary security protocol used in AD) attacks are on the rise. Here are some steps to take to enhance your Kerberos security:

- Every Active Directory Forest has a KRBTGT account that's used to encrypt user Kerberos ticket-granting tickets (TGT). Protecting the KRBTGT account is an essential piece of protecting the security in your AD environment. Annually reset the KRBTGT account in every domain to mitigate Golden Ticket attacks. My colleague Jorge de Almeida Pinto maintains a widely used KRBTGT reset script.
- Take advantage of recent Kerberos security enhancements and patches. For example, upgrade your Windows Server 2019 domain controllers to take advantage of AES encryption over the older RC4 encryption algorithm (post-upgrade steps are required).
- Remove Service Principal Names (SPNs) assigned to admin accounts. This step eliminates a favorite Kerberoasting path to domain dominance.
- Eliminate unconstrained delegation, which gives a compromised server the ability to act widely on behalf of unsuspecting users.

5. Deter lateral movement

Deterring lateral movement helps prevent an attacker from moving through systems from computer to computer or across forests. Take these steps to make lateral movement more difficult:

- Where possible, remove local administrator rights from client user accounts. For some users, this action might require a privileged access management (PAM) solution.
- Implement local administrator password solution (LAPS) on all member servers and client computers.
- Restrict local administrator group membership to the smallest number possible.

6. Actively manage privileged users and group security

In light of recent highly publicized malware and ransomware attacks, organizations should actively manage who has privileged access in AD and enforce least privilege across the forest. Although explaining why access rights must be reduced can be difficult, the change is essential for good governance. Here are some steps to take:

- Minimize privileged group membership. Operators should not require Domain Admin rights.
- Remove administrative permissions granted to service accounts. Applications should not require Domain Admin rights.
- Delegate least privilege access to the lowest level required.
- Monitor for permission changes on the AdminSDHolder object. (If you see a change here, the account has likely been compromised.)

7. Secure your dependencies

As you think about the security of your environment and Active Directory, consider all the abstraction layers and how they are secured. Each one of those layers expands your attack surface, so take the time to understand how they are protected and consider adding security to them. Take these steps to get started:

- Limit hypervisor admin privileges.
- Restrict access to storage that contains copies of the Active Directory .dit database file, such as backups and IFM (install from media) AD copies.
- Audit management tools and services with elevated access.
- Evaluate PAM tools.

8. Harden your domain controller

In addition to the other functions it performs, your domain controller provides the physical storage for the Active Directory database. Just as abstraction layers can be abused by an attacker, so can your domain controller. If your domain controller is compromised, your Active Directory forest is considered untrustworthy until you can restore a clean backup and ensure that the gaps that led to the compromise are closed. Take these steps to harden your domain controller:

- Upgrade your domain controllers to a minimum Windows Server 2019 OS level with AES encryption configured.
- Remove unnecessary server roles and agents.
- Disable the Print Spooler service on all domain controllers.
- Consider using server core to reduce the DC's attack surface.

9. Harden privileged access

Hardening accounts that have privileged access reduces AD's attack surface and lessens the likelihood of potential compromise of these accounts. Here are some steps you can take to protect privileged accounts:

- Implement an MFA service designed to support AD.
- Use separately named admin accounts and lock them down for administration purposes only.
- Create break glass accounts to use in case of emergency.
- Deploy a tiered administrative model, focusing on protecting access to Tier 0 accounts and systems.
- Use a PAM solution to enable just-in-time access to privileged accounts.
- Use privileged access workstations that are specially hardened to limit the potential for being used as an attack entry point.

10. Monitor for unusual activity

You can't secure what you can't see! Monitoring is essential for understanding shifts in your security posture and finding the earliest indicators of compromise. Consider these aspects when developing your monitoring strategy:

- Implement a security incident and event management SIEM) solution with user and entity behavior analytics (UEBA) capabilities.
- Monitor privileged groups for membership changes.
- Watch for access control list (ACL) changes to sensitive objects.

Prevention and the path to recovery

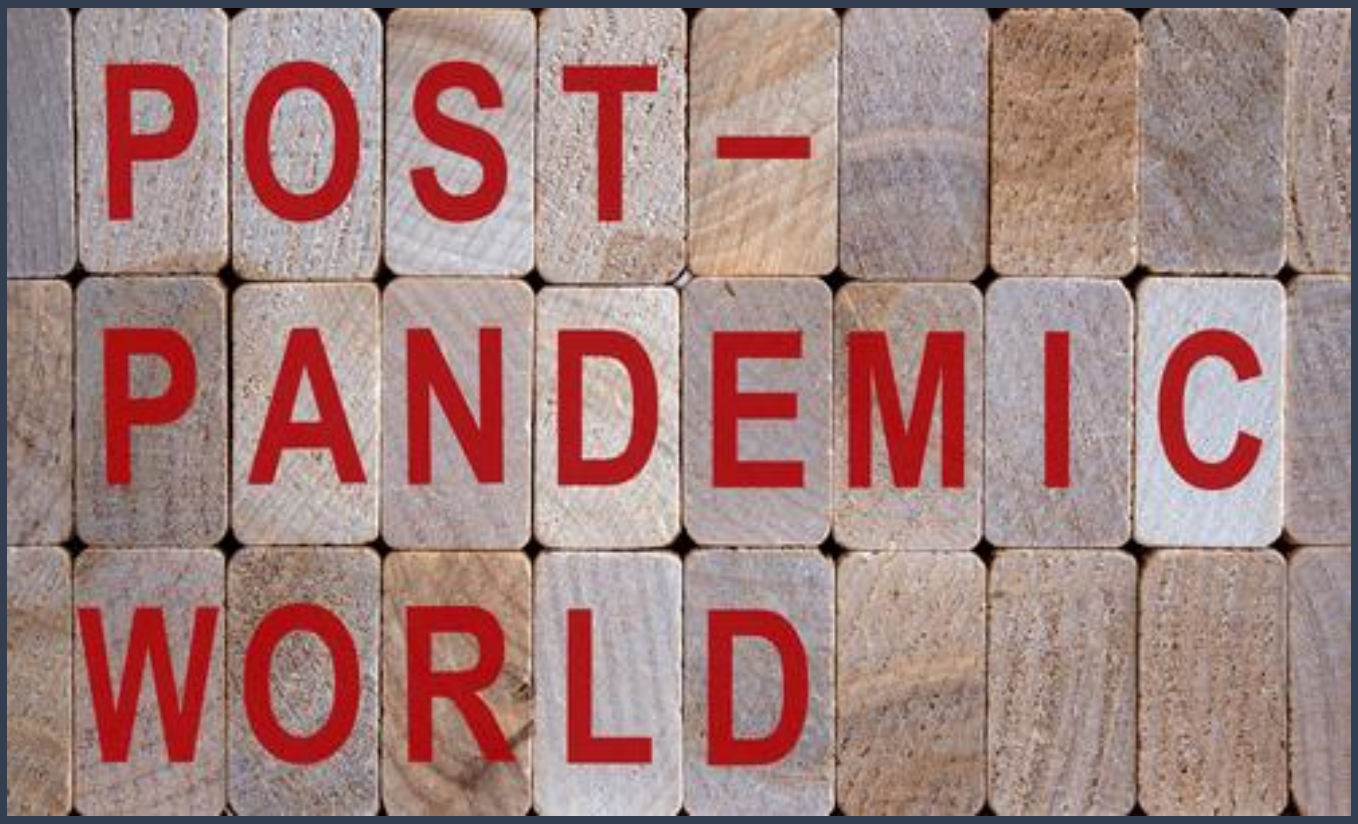
With these 10 actions, organizations of any size can significantly reduce their attack surface and protect their Active Directory instances. Why is securing Active Directory so important? It's central to establishing and maintaining trust in your environment. It's also central to attackers gaining control. Successful attacks center on an attacker's ability to steal AD credentials or compromise an AD account with malware. Once they have that, they can escalate privileges to gain access to anything in your systems. Anything you can do to prevent that access and ensure that you have a path to a faster recovery if something does happen is well worth it.

One quick and painless way to assess your AD security stance is to download and run the free Purple Knight utility. The tool doesn't require any special permissions, giving you an "attacker's view" of your Active Directory—and any gaps that might admit malicious actors. You get an overall security score as well as individual scores across several categories, including Kerberos, Group Policy, and account security. Plus, Purple Knight returns a list of security indicators—both indicators of exposure and indicators of compromise—so that you know where to focus efforts to beef up your defenses.

Anything you can do to prevent malicious access to AD and ensure that you have a path to a faster recovery if something does happen is well worth the time spent.

About the Author

Sean Deuby brings 30 years' experience in enterprise IT and hybrid identity to his role as Director of Services at Semperis. An original architect and technical leader of Intel's Active Directory, Texas Instrument's NT network, and 15-time MVP alumnus, Sean has been involved with Microsoft identity since its inception. Since then, his experience as an identity strategy consultant for many Fortune 500 companies gives him a broad perspective on the challenges of today's identity-centered security. Sean is an industry journalism veteran; as former technical director for Windows IT Pro, he has over 400 published articles on AD, hybrid identity, and Windows Server. Sean can be reached online at seand@semperis.com, @shorinsean and at https://www.semperis.com/.



Top Trends in Cyber Security Post-Pandemic

By Suchita Gupta, Associate Content Writer, Allied Market Research

Cyber security is a fast-moving sector as both cyber security providers and hackers go toe-to-toe with each other. With new threats, security providers come up with innovative ways to prevent such attacks. For the last two years, the world was battling and coping with the global Covid-19 pandemic, but this trying period was particularly helpful to cybercriminals. During the pandemic, various companies including tech giants such as Microsoft experienced sophisticated cyber-attacks of all time. Global adoption of remote working, digitization of society and organizations, and increased transition of our lives to the digital world have created uncountable opportunities for phishers, scammers, hackers, and extortionists. According to Allied Market Research, the global cyber security market is projected to garner $478.68 billion by 2030, registering a CAGR of 9.5% from 2021 to 2030. So, let's look at the most significant trends in the cyber security sector that are bound to make difference in the coming years.

1. Growing threat of ransomware

During the pandemic, many companies struggled due to ransomware attacks. What's more, as per the UK National Cyber Security Center, the ransomware attacks in the first quarter of 2021 were three times that of in the whole of 2021. This trend is expected to continue in the future. The growth of digital

environments and penetration of the internet and the internet of things (IoT) in developing countries are major factors behind such statistics.

Ransomware involves infecting devices with the virus that creates restricted access to the user with unbreakable cryptography and threatens to destroy the file and other data unless a certain ransom is paid. In such cases, untraceable cryptocurrency is used. Moreover, hackers may threaten to publish private information, which can compromise the organization and make it liable for fines.

2. Risk in cloud services and cloud security threats

Cloud vulnerability will continue to be a concern in the future and a major cyber security trend. Rapid adoption of work-from-home following the pandemic increased the need for cloud-based services and infrastructure tremendously. But there are some security implications for organizations that may have been overlooked.

While cloud services are flexible and offer an array of benefits including scalability, cost-saving, and efficiency, they are the main target for cybercriminals. Misconfigured cloud settings are backdoors for cyber-attacks and cause data breaches and unauthorized access, account hijacking, and insecure interfaces. Data breaches in an organization could cost millions to the company. Along with this, organizations face numerous network security and cloud security challenges, such as:

- Cloud migration issues
- Dealing with potential entry points for hackers
- Ensuring regulatory compliance
- Insider threats

3. Social engineering attacks to get smarter

Social engineering attacks such as phishing are not a new threat to use but they have recently become more troubling, especially during the global adoption of remote working. Now, attackers target people connecting to their employer's network from home as it is an easy target. Along with traditional phishing attacks on employees, there is increase in whaling attacks that target executive organizational leadership. Moreover, SMS phishing has gained prominence due to the popularity of messaging apps such as Slack, Skype, and WhatsApp. These apps make it easy for attackers to trick users into downloading malware onto their phones.

Over the last two years, another variation has gained traction- voice phishing. Hackers pose as IT staff such as customer service representatives and trick users into offering access to important credentials and access to internet tools. Voice phishing has cost millions to various companies, especially financial institutions and larger corporates.

These are a few trends in the cybersecurity industry. Such threats will only increase in the future and create challenges for IT professionals. There is a dire need to develop counter-attacking technologies to

improve cybersecurity. As the connected world is clearly the future cybersecurity must evolve with time and companies must invest heavily to improve their security solutions.

About the Author

Suchita Gupta is an explorer, musician and content writer. While pursuing MBA, she found that nothing satisfies her more than writing on miscellaneous domains. She is a writer by day and a reader by night. Besides, she can be found entertaining her audience on social media platforms. Find her on LinkedIn & Instagram.

Suchita Gupta can be reached online at https://www.alliedmarketresearch.com

https://www.linkedin.com/in/suchita-gupta-0b818b202

Trust in The Future of Electronic Healthcare Data Management and Security

By Coley Chavez, Chief of Staff and Compliance Officer of Genomic Life

Healthcare data is defined as “any information, which relates to the physical or mental health of an individual, or the provision of health services to the individual.” This data stems from several sources, including but not limited to electronic health records (EHRs), medical imaging, genomic testing, medical devices, and claims data. The acceleration of technological improvements in healthcare throughout the past decade has enabled millions of practitioners and patients to convert their healthcare data into useful, actionable information.

However, considering prevalent cybersecurity attacks, there has been increased scrutiny of healthcare data security management and measures in an ever-changing healthcare landscape. Earning an end-user's trust is paramount to adopting innovative healthcare solutions.

The Landscape

Security and privacy are essential foundations when it comes to protecting healthcare data. How an organization commits to this is critical, especially regarding data sharing.

The migration of electronic healthcare data stored to a cloud-based architecture has created a significant shift in how businesses must proceed with managing and protecting their end-user's sensitive information. Robust privacy and security policies and certifications must replace traditional security measures for protected data that organizations previously managed on-premises.

A Culture of Compliance

Companies managing sensitive data must adopt a culture of compliance when developing their security and privacy programs. This initiative should start with the company's risk management framework. Leadership needs to set the bar high, as does the investment in technologies that ensure the privacy and security of the data.

We utilize third-party audit organizations to test and validate our compliance program's security and privacy controls. Companies that don't look holistically at their security and privacy measures upfront will have difficulty implementing the long-term.

Buy-in for compliance must come from the top. A company's board of directors, the executive management team, and the organization must create a culture around compliance. Without buy-in from the top, it is challenging to implement proper safeguards.

As healthcare data breaches have been occurring more frequently and on a larger scale, these cybersecurity issues have reminded us that not all companies hold data security and privacy with such high regard. Despite the increased adoption of innovative cloud-based technologies, the healthcare industry still lags behind most other industries when it comes to data security and privacy management. This is mainly due in part to the challenges presented by the complex nature of healthcare data and budget limitations.

The End-User

Health information is worth much more on the dark web than someone's financial information. With that additional information, a hack can manipulate things such as medical services and IRS tax audits. As such, the end-user is rightfully looking at who is managing their data and what regulatory framework is in place to protect their most sensitive information. Companies that don't adhere to these frameworks increasingly run the risk of facing consequences that are severe and expensive.

As this paradigm shift in healthcare data security continues to take place, the most successful data management companies will adopt a modern risk framework that emphasizes a culture of compliance that ultimately builds more trust with their end-user.

Solutions

Paramount to this new regulatory framework for data security is an agile-based compliance program that can meet the different needs of each stakeholder.

Our stakeholders- employers, employees, and benefit brokers - have different requirements. We must look at how we apply our agile-based, rigorous compliance program to meet their needs at varying levels.

As Genomic Life's compliance officer, when our company signs on with a new client, I meet with their security and compliance team to explain our current risk management program and the measures we have to safeguard their stakeholders. There are numerous layers of responsibility we must account for in rendering our services, and the comprehensive compliance program I'm describing allows us to plan for these layers as they occur more effectively.

In Conclusion

All companies that manage sensitive customer data must invest in their overall compliance programs and demonstrate compliance through verification with the highest certification bodies, such as HITRUST, offering comprehensive cybersecurity management and evaluations. Companies that manage your data should be trusted, but as the end consumer, it's crucial that you also verify.

Electronic data management is constantly evolving, requiring leaders to review their policies and redefine governance, risk, and compliance programs to ensure the highest level of privacy and security measures. This step fortifies the trust, but verify mandate.

About the Author

Coley Chavez is the Chief of Staff and Compliance Office of Genomic Life. He works with the CEO, Executive Management Team and Audit Committee, and leads a team tasked with aligning the organization's operations and technology platforms in order to help deliver the sciences of today for the medicine of tomorrow.

Prior, Coley held leadership and executive roles at Chord Health, OncoSec Medical, Inovio Biomedical Corporation, Genetronics, Inc., BTX, Abnology, Sangart Inc., Ziff Davis, and Harte Hanks Market Intelligence.

He is a HITRUST Certified CSF Practitioner (CCSFP, #59200) and architects agile-based compliance solutions. He has received certifications from San Diego State University and the Certified Technical Institute (CTI) for Computer Sciences and focused-based information technologies. Coley has been involved in the HIT community working with the Life Sciences Information Technology Global Institute (LSIT), HIMSS, further promoting and developing industry Good Informatics Practices (GIP) for the Digital Health, Life Sciences, and the Health Tech industry for over 20 years.

Coley has a degree in Finance from the University of New Mexico and was a member of the UNM Football team.

Coley Chavez can be reached online at https://www.linkedin.com/in/coleychavez/ and our company website is https://genomiclife.com.

Understanding The True Financial Risk of Ransomware Attacks

By Mark Guntrip, Senior Director of Cybersecurity Strategy at Menlo Security

The European Union Agency for Cybersecurity (ENISA) recently defined today's threat landscape as the "golden era of ransomware". Ransomware has become one of the biggest cybersecurity threats facing organizations today in any industry and any market – and unfortunately, it is only likely to get worse.

According to research that Menlo Security recently undertook, a third of organizations (500+ in the US and UK) said they experience ransomware attacks at least once a week, with 9% experiencing them daily. Over half (53%) of respondents to our survey admitted that their company has been the victim of a ransomware attack in the last 18 months.

The shift to remote and hybrid working models has expanded the attack surface, opening up a host of new vulnerabilities, attack vectors and entry points into the corporate network.

Combined with this is the development by attackers of new and ever more sophisticated techniques. We have seen a surge in attacks known as Highly Evasive Adaptive Threats (HEAT), designed to bypass detection from traditional security tools like sandbox analysis and phishing detection solutions.

A tool to make money

Cybercriminals see ransomware as a proven and effective tool to make money, and lots of it, with pay-outs totaling as much as $40 million. The financial effects of ransomware are certainly becoming more pronounced, with more attacks targeted at supply chains and critical infrastructure, causing widespread disruption. The Cybersecurity and Infrastructure Security Agency (CISA) reported in February 2022 that it is aware of ransomware incidents against 14 of the 16 US critical infrastructure sectors.

Despite all the warning signs, are companies underestimating the cost of recovering from such an attack?

Industry figures suggest there is an alarming disparity between the perceived cost and the actual cost of recovering from a ransomware attack among security professionals. Our own survey shows that the average perceived cost is $326,531, with insurance pay-outs extending up to an average of $555,971. Industry figures, however, show that the average total cost of recovery from a ransomware attack was $1.4 million in 2021.

It was encouraging to see that three-quarters of respondents have cyber insurance, although one in four (24%) do not have any insurance or don't know if they do.

So, with current insurance pay-outs unable to cover even half of the average cost to recover from ransomware, many firms will be under huge financial pressure if they are hit, particularly smaller businesses that may lack the resources and expertise to manage it.

Our research also highlighted some other serious concerns, notably that threats are outpacing security teams.

When we asked security professionals what keeps them awake at night, 41% said they worry about ransomware attacks evolving beyond their team's knowledge and skillset, while a similar percentage (39%) worry about them evolving beyond their company's security capabilities.

Their biggest concern, however, is the risk of employees ignoring corporate advice and clicking on links or attachments containing malware. In fact, they worry more about this than they do their own job security, with just a quarter worried about losing their job.

Ransomware demands – to pay or not to pay?

There is also some debate in the industry around how best to deal with ransomware demands according to our research. One in three security professionals said they were worried about paying a ransom demand and not getting their data back, but 65% would still pay.

Interestingly, around a third said it was down to their insurance company to pay it, and around one in five (18%) said the government should pay. More than a quarter (27%) of security professionals would never pay a ransomware demand.

Paying a ransomware demand clearly depends on an organization's level of preparedness. Do they have the right processes in place and strong backup and recovery? If so, they won't need to pay it. According

to our report, however, less than half (45%) of businesses implement a data backup or recovery plan as the first step in the event of a ransomware attack.

This could result in an organization being unable to function as normal, access data, or worse, the impact and damage is likely to bring down the business. If this is the case, that's when the business needs to seriously re-evaluate its options. Now is the time to re-examine security infrastructure to make sure attacks can be prevented before they even happen.

About the Author

Mark Guntrip is Senior Director of Cybersecurity Strategy at Menlo Security, responsible for articulating the future of threats to security leaders around the world. Prior to joining Menlo Security, Mark has been security strategist at Proofpoint, Symantec, Cisco, and several other leading cybersecurity providers.

Using Identity for Access Is a Huge Cybersecurity Risk

Why FIDO's proposal to use identification for cyber access opens more security vulnerabilities for threat actors to exploit

By Julia O'Toole, Founder and CEO of MyCena Security Solutions

In recent months, the Fast Identity Online (FIDO) Alliance has announced its commitment to supporting passwordless authentication across all of its products. The group – consisting of technology companies such as Apple, Google and Microsoft – has been planning this approach for nearly a decade and is expecting to implement it across platforms later this year.

FIDO initially began work on a system that lets users log in to their online accounts without using a password – instead utilising a PIN, biometric, iris scan or voice recognition. Now, FIDO believes it can provide better protection over legacy multi-factor authentication and better protection against malicious phishing attacks.

Rather than relying on users to remember their passwords directly, they would instead be stored on the user's device or cloud sync service associated with their operating system. Their phone becomes the access point to their work domain – access authenticated via inputting their PIN, or by using fingerprint or face identification.

FIDO hopes to reduce the reliance on passwords and give users a way of keeping their credentials to hand, as they move between devices. However, this overriding regard for convenience above security could potentially be leaving vital data vulnerable to threat actors.

Why identity and access are not the same

FIDO's approach exposes a misguided confusion between identity and access. In essence, someone's identity is composed of fixed non-changing properties such as legal identity, work or studies credentials and biometrics. Your legal identity gives you certain legal rights such as the right to live in a country, to receive benefits and to travel to certain places, while your work and studies credentials give you the right to work in certain regulated professions such as doctors or lawyers. Biometrics, such as your face, iris and fingerprint are hardcoded visible – therefore non-secret – characteristics that you can't change.

None of the data connected to these attributes is hard to get, from leaked databases such as the entire 45 million Argentinian digital ID database to photographs such as this benevolent hacker recreating the fingerprint of the current president of the EU Commission. What makes using identity particularly dangerous is the permanence of the theft. Once stolen, data cannot be unstolen. You can change a password, but you cannot change who you are.

On the other hand, people have long invented the concept of keys to grant access to certain places. The concept is simple: as long as you have the right key, you can open a certain door. It is completely independent of your identity, as keys can be transferred, shared or changed. In the physical world, you can have as many keys as you have doors to lock, ensuring that losing one key only requires changing one lock.

Don't use a single key for everything

In the physical world, people do not use a single key for all their doors. It would be extremely unsafe to have one single key to access everything from their house to their car to their office... since losing it would mean losing everything in one swoop. But in the digital world, people have been advised to use a single master password, biometric or PIN to access their digital assets. FIDO's proposal is another illustration of the push to trade resilience for convenience. If people follow that advice, it means one attack could cause the loss of all of their accounts and data at once.

A lifetime of risk for a moment of convenience

When you start mixing biometrics and single access things get worse. Imagine that you use your identity biometrics to access everything you own. Biometrics are a unique combination of 1s and 0s, which by the nature of digital information can be stolen. Not only would a thief be able to access every account you have, but the unique biometrics data is permanently stolen - since you can't change who you are. That means you will never be able to fully control your "digital identity" ever again. Any time in the future, that data you innocently gave away for access may be used without you ever knowing it, putting you in potentially illegal situations without your knowledge.

Never make your own keys – physical or digital

When it comes to managing access keys in the real world, it is a straightforward process.

Companies give keys to employees, landlords to tenants, car dealers to car buyers. No one thinks they need to become a locksmith and start to cut out their own keys – keys are just received and used. The misconception starts when we moved to the digital world and people believed they had to make their own keys. It is both inefficient and unnecessary. As much as you don't need to make and cut out your keys, you don't need to create or remember passwords. After all, a password is just a digital key.

The only difference between a physical and a digital key is the absence of physical obstacles to stealing a digital key. In the physical world, a thief needs to be in reach of the key to steal it. But in the digital world, a thief can be located anywhere in the world and phish or guess your digital keys or passwords. So the question should be how to ensure those keys aren't stolen. The answer lies in history: make them secret.

Solution: encrypt all digital keys!

As narrated in The Code Book: The Secrets Behind Codebreaking by Simon Singh, people throughout history have used cryptography to keep secrets. For digital keys, the best way to keep passwords secret from anyone, including the user, is to encrypt them from creation, distribution, storage, use, to expiry - since you cannot leak what you don't know.

Passwords keep the same properties as keys: they are flexible, changeable, discardable and can work for anything. By encrypting all digital keys, you remove the threat of human errors over credentials, which represent 82% of all data breaches according to Verizon's Data Breach Investigations Report 2022. Not only would it remove the risks of weak and reused passwords, but it would also prevent hackers from stealing or buying credentials from current and former employees as well, as was recently the case at two dozen major natural gas suppliers and exporters.

There are different ways to manage encrypted passwords for different needs. In the business world, companies can distribute end-to-end encrypted passwords for every system to all of their employees into a digital fortress with multiple levels of security. By utilising end-to-end encryption, they remove passwords from the control of employees, who can only use them as keys to open doors without the need to know or see them. Not knowing passwords means employees cannot give them away in a phishing attack – which represents 83% of cyber-attacks according to the Office of National Statistics in 2021. Not knowing passwords also means employees not forgetting passwords, which saves organisations money on password resets and productivity.

Not your keys, not your data

In reverse, when companies let employees create and control the keys to their data, they do not control the keys to the data. Not controlling the keys to the data means not being able to control and protect the data. Hackers know that and how easy it is to get to any employee to phish or guess their keys, which

explains why data breaches are so common. Only companies that encrypt their access can fulfil their legal obligation of custody, possession and control of their data, since only they have full control of the keys to that data.

Increased physical risks

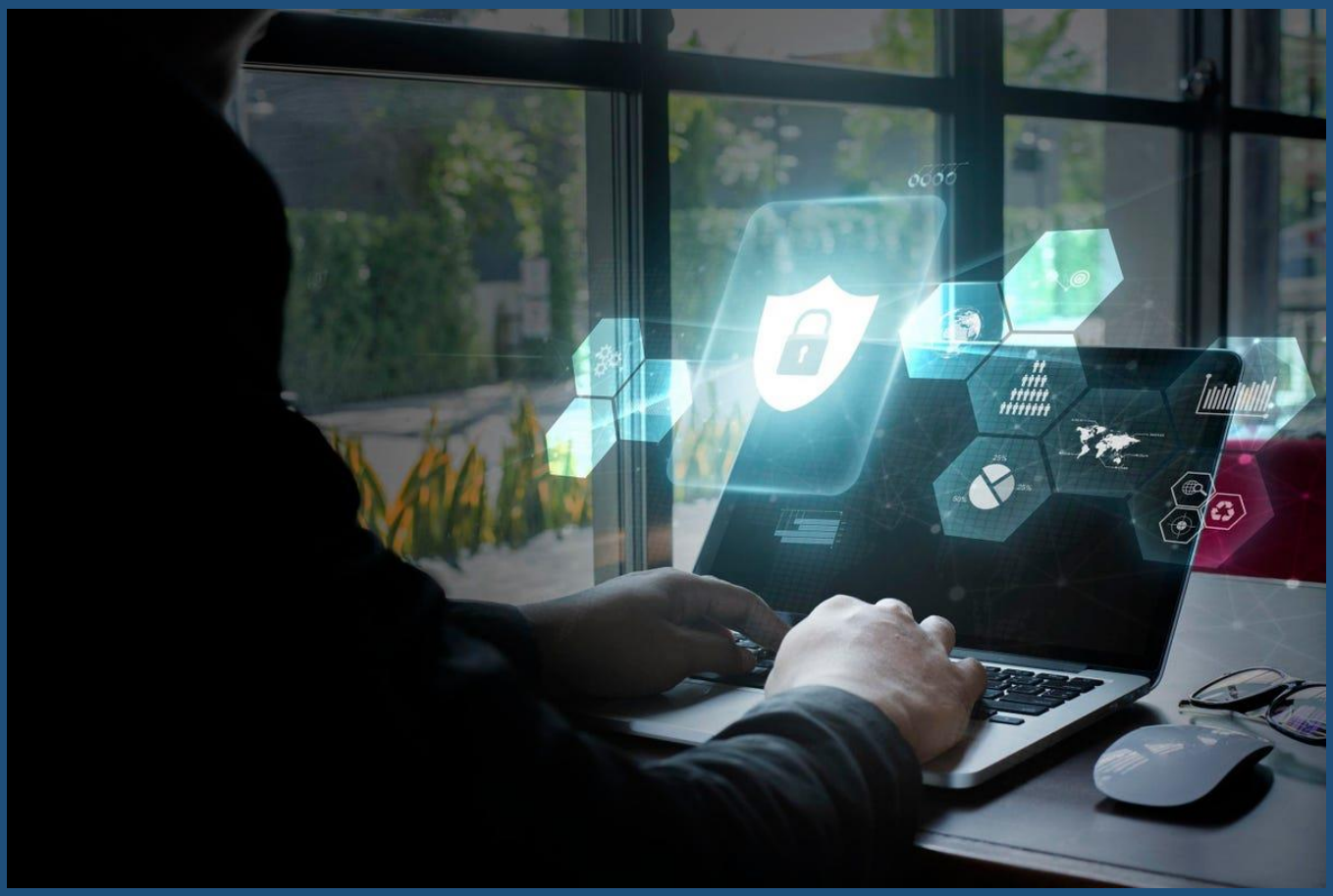
Of the issues stemming from FIDO's proposal, none has more chilling implications than the risks that spill over to the physical world, which makes anyone with a portable device become an obvious target for criminals. Many cases of physical assaults in the city of London have been reported where people were threatened with knives to give their fingerprint and face ID to open their devices. Should everyone use their identity on their mobile device to open all their accounts, anyone walking in the street becomes a target wallet for criminals.

As we have learned from the last decades, a lot of new technology that seems convenient at first often hides oversized, unforeseen and uncalculated risks. FIDO's proposal of using identity for access can directly affect people's security and well-being. Fortunately, we have now accumulated enough experience and data to know better and do proper risk assessments before blindly going all in for the next shiny new object. If we have learned anything from our early mistakes with the internet, it is that convenience often hides a flipside you discover when it is too late. Let's not make the same mistake when there is so much at stake.

About the Author

Julia O'Toole, Founder and CEO of MyCena Security Solutions, a breakthrough solution to manage, distribute and secure digital access. An inventor and author of several patents, Julia uses maths, neuroscience and technology to research and design simple yet innovative solutions for complex problems. Julia's areas of research and expertise include cybersecurity, collaboration and search. Julia founded MyCena in 2016, which has since become a market leader in segmented access management and safe password distribution. With its ground-breaking patented security system, MyCena protects companies from the risks of password error, fraud and phishing, loss of command and control, ransomware, and supply chain cyberattacks.

Julia can be reached online at (julia@mycena.co , linkedin.com/in/juliaotoole,) and at our company website http://www.mycena.co



What We Have Learnt Building a Global Security Conscious Culture

By Nicola McCoy, Chief Information Security Officer at RSM International

The growing cyber risk is impacting global businesses of all shapes and sizes as 'bad actors' develop more sophisticated and coordinated attacks. Building a comprehensive cyber defence has never been more important. However, it requires an understanding of the inner workings of an enterprise, the breaking down of departmental silos, and analysis of the organisation's entire supply chain, and this is not always simple.

Achieving this in a company that operates in multiple jurisdictions or has a group or network structure for example can be complex and increases the need for transparency of interdependencies and differences across operating jurisdictions. In short, creating a security conscious culture across a varied global network, like the one I represent at RSM International, presents some unique challenges and risk management responses.

Cyber security professionals must look beyond purely technology threats and think holistically about the 'capabilities' that underpin how they operate and deliver work to their clients to identify high priority risks.

By capabilities, I mean the people, processes, technologies and supplier relationships that enable a business to run and grow. Once you have a true understanding of these fundamental elements, interdependencies, risks and impact, you can assess where the threats and weaknesses among them lie and balance where you need to remediate and invest.

The transformation era

At RSM, we talk a great deal about the '*The Transformation Era'*: a time when businesses, governments and communities are focused on post-COVID-19 recovery through digital-first, data-driven technological solutions. As a global organisation, RSM has over the years focused on accelerating the transformation of its entire network while supporting clients of our member firms transform for future growth. Today we are building on our existing agility and resilience by putting in place new technologies to deepen our dedication to quality across the more than 860 offices within our growing network of independent firms.

The adoption of new technology and a continuous focus on innovation is the key to all organisations moving forward, yet it also opens up new areas of risk. It is essential that leaders build a security conscious culture and reinforce it constantly though knowledge sharing and best practice. RSM firms around the world are embracing innovations like AI, big data and automation that can help plug skills gaps created by the great resignation, reduce reliance on manual processes to free-up our experts to focus on more exciting project work, and create new possibilities for businesses.

Emerging technologies and the risk of remote working

New technologies enable these possibilities, but they also create access points, data sources, vulnerabilities and gaps that can be exploited by criminals. It is critical that any decision to implement new technology has security front of mind. To ensure growth and competitive advantages it is important not to slow the pace of innovation and instead continue to enhance our business capabilities. It is also important to ensure the appropriate due diligence checks are carried out so that new solutions designed to help a business do not actually end up causing a negative impact instead.

Another technology risk relates to an organisation's people and, specifically, the risk that comes from catering to employees' newly acquired expectations around remote and flexible working. A businesses' digital infrastructure and data risk now extends into people's homes and personal devices; the need for up-to-date and tailored training, as well as the skills to embed robust systems and processes into the organisation, has never been more important if this is not to become an easy target for criminals.

Global risk exposure in the supply chain

Gartner predicts that by 2025, 45% of organisations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021.

Businesses transact with, rely upon and share risk with suppliers every day. But how many leaders in board rooms know what is really happening on the ground? A recent survey conducted by one of our members, RSM UK, revealed that business leaders are experiencing successful cyber-attacks in greater numbers (up to 27% in 2022 from only 20% in 2021). Perhaps even more worryingly, the survey found that a third of business leaders admit their board does not understand the cyber landscape enough.

Data managed or processed by a third party is subject to the same security requirements as information which is directly held; a successful attack further down the supply chain would be a critical governance issue for the client in just the same way as one that occurs closer to home – with the same financial and reputational implications among the investors and clients who hold the company to account.

Any organisation with global offices, affiliates or partnerships must make itself acutely aware of supply chain cyber risk. It should determine its level of exposure; identify the controls it can use for mitigation and make sure these are embedded into supplier contracts. It should also investigate all aspects of its suppliers' procedures and operations, from how they store and secure their data; to how they train and vet the employees who have access to it. Backups, encryption standards, audit trails, incident response plans and business continuity contingencies are among the many factors that should be considered.

Furthermore, building in regular reviews of the supplier, including determining if overdependency on a single supplier, is also key and should be balanced in accordance with the relative impact and criticality of the service they are providing.

Building a universal security conscious culture

What all these examples have in common is the rapid change they are undergoing in terms of how businesses use them to operate and work. Because of this, we have long understood the importance of embedding these changes within our overall risk framework. As a growing global organisation, at RSM, we consider cyber risk across our whole organisation and share best practice through working groups and internal training events to ensure consistency in processes, systems and approach to security.

Those capabilities could be the technology we adopt, the ways in which our employees choose to work or the integrity with which the suppliers who support our operations manage their own systems. They are the things that are required to make an organisation successful. And they are also the areas where we should be looking for risks so we can safeguard against them with robust systems, training, policies and skills.

As a global organisation, RSM's core objective is to bring our team of 51,000 professionals even closer together and to support the provision of cross-border services to clients. While global policies and procedures are fundamental to us working cohesively, true collaboration only comes when the collective shares the same values and vision for the future, as well as best practice like robust cyber defence and security protocols. This is a truly exciting part of my role as the Chief Information Security Officer for one of the world's largest networks of independent audit, tax and consulting firms.

About the Author

Nicola McCoy is Chief Information Security Officer at RSM International, the world's 6th largest Network of independent audit, tax and consulting advisers focused on the global middle market.

Nicola can be reached online on LinkedIn and at our company website RSM Global | Audit Tax and Consulting Services.

Why CSOs Are Decluttering Their Cybersecurity Toolboxes

By Motti Elloul, VP Customer Success and Incident Response, Perception Point

Slashed budgets, staff shortages, and the significant risks associated with legacy cybersecurity solutions – these reasons and more are why Security Operations Centers (SOCs) and Chief Security Officers (CSOs) are considering more efficient, secure systems with streamlined numbers of tools and layers.

The key for CSOs is to find the happy medium between big-tent cybersecurity solutions and the large number of niche hyper-focused cybersecurity features those enterprises require.

Key Problems

Reports indicate that since May 2022, tech startups have laid off nearly 27,000 workers, however, even before today's budget and staff cuts, there was already a chronic staff shortage in the cybersecurity sector. According to studies, "the demand for cybersecurity professionals continues to outpace supply."

There are tangible consequences in the cybersecurity realm to these staff and skills shortfalls – misconfigured systems, risk assessment and management that is either rushed or skipped, slow remediation times that leave systems exposed, and the inability to handle all active threats to the network. In short, SOC teams are increasingly understaffed and overworked – all while facing a rising tide of increasingly sophisticated attacks.

Furthermore, outmoded legacy solutions can leave networks even more vulnerable. There are certainly industries where older means wiser, but in cybersecurity, legacy solutions often cannot keep up with the evolving threat landscape and are not easily integrated with updated tools. In addition, they often have complex configuration and maintenance processes that make management, patches or updates complicated and impractical. According to reports, unpatched vulnerabilities and risky services account for 82% of successful attacks.

The current threat landscape is only growing. The hybrid work era has driven enterprises to adopt a rising number of SaaS and web-based tools to deal with the consequences of a decentralized work environment – messaging apps, file sharing, CRMs, etc. As recent Google Drive and Dropbox hacks demonstrate, there is a rapidly growing number of new attack vectors which malicious actors can exploit. This trend is only likely to continue as new SaaS and web-based tools are developed to optimize the modern workplace, and remote work policies give employees the potential to access sensitive apps from unmanaged and third-party devices. In short, many companies are a lot more vulnerable than they realize.

Big Tent vs. Niche

Understaffed and overworked SOC teams are now facing a new hurdle: System Overload. As cyberattacks grow in sophistication and frequency, the number of cyberdefense tools that security professionals rely on is constantly growing. Reports indicate that some organizations use as many as 45 different tools on average to keep their networks safe.

These hyper-focused security tools may be effective in the fight against the growing sophistication of cyberthreats, but their sheer volume is in and of itself a problem because they are often cumbersome to manage; forcing analysts to waste time toggling between tools. This results in delayed incident analysis and security system maintenance. Furthermore, the disparate nature of these solutions means that analysts are unable to get a holistic view of issues or react quickly to breaches. Those using more than 50 tools ranked themselves as 8% less likely to be able to detect an attack and 7% less responsive when attempting to address it. With staff shortages, SOCs also find it hard to retain the expertise needed to utilize these multiple systems efficiently.

That said, big-tent, legacy cybersecurity solutions are not necessarily the best alternative. It may seem beneficial to have many defense tools within the same platform, but the pinpoint responses of niche solutions to the growing threat-landscape may be lost. In other words, these catch-all solutions can't necessarily keep up with the growing sophistication of threats. 40% of cybersecurity professionals said their current cybersecurity strategy will likely be outdated in just two years, with 37% said it would happen in three.

The Middle Ground

To effectively combat the next generation of cybersecurity challenges, CSOs will need to create an effective middle ground. This industry need has only been accentuated by the current economic downturn, which is forcing many SOCs to cut budgets by providing the most bang-for-your-buck solutions to secure vulnerable systems.

The trick for cybersecurity providers will be to offer a balanced number of solutions that effectively cover a number of threat vectors – not so many that they lose their focus, but enough that clients can reduce their reliance on an unwieldy number of security products. In the long term, more streamlined SaaS cybersecurity systems can not only make it easier for SOC teams to employ, train, and retain their teams, but actually reduce their workloads. Vendors must also strive to create easy to deploy and manage integrated solutions that fit neatly within customers' current systems, and which interact seamlessly with their standard operating systems and business workflows. This ensures that both security team members and general staff can easily leverage the benefits in a frictionless manner. In a similar vein, vendors should provide tools and services that bolster a SOC team's capacity, offering a lifeline for groups that are understaffed and overworked. These could be supported by automated ML- and AI-based platforms and actual cybersecurity experts in a managed SOC service to ease the strain of analyzing and remediating the tide of malicious activity threatening to engulf companies.

Modern streamlined and decluttered cybersecurity solution suites should be hastened in by the realities of the industry's knowledge shortages and today's economic challenges; however, going forward they make the most sense for effective, efficient, and durable SOC teams.

About the Author

Motti Elloul is VP Customer Success and Incident Response at Perception Point. He works with existing customers to educate and help them maximize their product knowledge and solve issues that may arise. Motti focuses on building sustainable customer relationships by optimizing their asset protection and leveraging the value of customer satisfaction. Motti has worked in people-centered roles at Applause, Red Bend Software, and Nuance Communications. He holds a BSc in Software Engineering from the Jerusalem College of Engineering.

Motti can be reached online at https://www.linkedin.com/in/mottie/ and at our company website https://perception-point.io/

Why Cyber-Attacks on The Cloud Are Rising and How to Prevent Them

Increase in implementation of cloud by government and private organizations to improve efficiency and save costs made it the prime target for cyber-criminals. However, taking security measures can enable smooth functioning of cloud and provide many benefits.

By Pratik Kirve, Team Lead - Content Writing, Allied Market Research

It will be strange to learn that an organization, whether it be private or government, is not operating on the cloud in one way or the other in 2022. Why? Because, technological advancements and benefits in terms of cost and efficiency led organizations to shift their resources, operations, storage, and majority of functions on the cloud. Cloud implementation also saves a lot of space needed for physical servers. However, privacy and security issues related to the cloud become a major concern as hackers and cyber criminals eye for vulnerabilities and exploit them in every way possible. There are number of reasons that lead to increase in cyber-attacks on the cloud. Let us have a look at them:

- **Surge in utilization of cloud services**

According to Cisco, nearly 94% organizations across the world utilize cloud services in one way or the other. This statistic shows how cloud has emerged as a viable option for organizations from the past few years. It also highlights that the cloud computing will get even bigger year by year. The data storage on the cloud is estimated to amount to 100 zettabytes by 2025, according to the article published in Cybercrime Magazine by the firm Cybersecurity Ventures. The firm also highlighted that this amount will represent nearly half of the total data generated at that time. With huge amount of data and operations moving to the cloud, it is obvious that attention of cyber criminals will turn toward exploiting vulnerabilities and posing different types of threats.

- **Replacement of traditional VMs with cloud containers**

The replacement of traditional virtual machines (VMs) with cloud containers is one of the major reasons for surge in cyber-attacks on the cloud. Instead of utilizing in-house physical servers and containers, many enterprises are choosing cloud servers and containers for carrying out storage, operations, and other functionalities for saving costs, increasing efficiency, and enabling smooth operations. The speed and simplicity provided by cloud containers made enterprises prefer them for cloud deployments. Traditional VMs can be replaced with cloud containers. However, many security lapses can be incurred during the deployment or replacements. There are high or critical security vulnerabilities in nearly 75% of images in cloud containers, according to the report by Sysdig. With such huge vulnerabilities, the cyber-attacks on the cloud are on the rise.

- **Adoption of remote working culture**

Another major reason that emerged for surge in attacks on the cloud is rise in adoption of remote working. Very few organizations adopted this culture before the Covid-19 pandemic. However, the outbreak of the pandemic became the primary factor for a considerable rise in implementation of remote working or work from home culture in organizations across the world. According to the survey by Gartner, nearly 88% of the total organizations across the globe provided remote working option to cope up with the pandemic. Organization have found that there are many benefits such as lowered operating cost and improved productivity with remote working facility. CoSo Cloud survey highlighted that there was 77% increase in productivity of employees with remote working. The trend of remote working persisted post-pandemic. Nearly 16% of organization adopted fully-remote mode of operation, according to Owl Labs. Though this number is less, it will increase considerably in the coming years. The cloud is the most feasible option for ensuring the smooth operation in the remote working culture. This shows that the cloud adoption will increase as more and more organizations adopt fully-remote culture. It will make the cloud platforms a target for attacks as cyber-criminals will try to exploit vulnerabilities and pose different types of threats.

These major reasons will increase the need for cloud security. Various cloud security measures will be implemented by organizations to strengthen the safety of data, ensure seamless operations, and improve cost-efficiency. The demand for innovative and strict cloud security measures will increase in the coming years. According to the report published by Allied Market Research, the global cloud security market is estimated grow considerably in the next few years, owing to rise in demand for managed security services and surge in dependence on cloud-based services.

Let us now look at major types of cyber-attacks on the cloud and how they can be prevented:

- **Prevention of data breaches**

Data breach is one of the major ways hackers are attacking the cloud. The huge data breach shook LinkedIn in 2012. More than 100 million users were affected. Their usernames and passwords were stolen and put on the internet black market for sale. Similarly, Yahoo reported that nearly 500 million users were affected due to data breach in 2014. This is the result of improper access management and the losses may be irreparable. The simple solution is to introduce multi-factor authentication. Social media companies such as Facebook began this practice. Nearly every social media, banking, and other organizations began implementation of two-factor authentication. Yahoo introduced Yahoo Account Key that eliminated the requirement of password and surged the protection measures.

Organizations need to ensure that that they have a specific access management layout. This implies that the marketing department in the organization does not have an access to the finance department credentials and protocols. This layout will help in ensuring the proper management of access points. Another way to avoid the data breach is to put firewall restrictions in place. This firewall will allow the authorized personnel only and detect the suspicious activities. It is not necessary that the threats will be made from outside sources only. The existing or former employees, partners, and contractors can utilize their ability to carry out various activities such as data loss, data breaches, credential leakage, system downtime, and others. Organizations need to provide access of critical systems to employees based on

trustworthiness and accountability. Moreover, misconfigured cloud systems must be fixed on priority. Regular analysis for providing authorization and validation to certain personnel should be conducted. This will prevent data and financial losses. Moreover, it will maintain the credibility among your customers for keeping their data and information safe from potential threats.

- **Ensuring proper security of APIs**

Application programming interfaces (APIs) allow two applications to connect, interact, and transmit data. These APIs provide an access of software platforms to third parties. Owing to weak authentication at the gateways of these APIs, the sensitive data may become vulnerable to hackers. Many hackers are always focused on exploiting APIs and steal the user data. In June 2021, LinkedIn reported that its APIs were utilized to steal the data of nearly 500 million users. The data was put on dark web for sale. For prevention of such leaks, cloud security providers must ensure that there is an integrated security. Moreover, there must be proper management, monitoring, and security of “front door” of the cloud. There should be avoidance of reuse of API key along with the usage of standard and open API frameworks. The utility programs that override the network, systems, and applications must be restricted. The access to APIs must be segregated and the access to specific users needs to be provided for preventing data tampering and disclosure.

- Awareness and prevention of denial-of-service attacks

Though scalability is one of the crucial benefits of the cloud, it may become a liability if the cloud system is overloaded and stops its operation. This may become one of the crucial cloud security risks. Many hackers are not trying to gain access to the system, but trying to stop the working of the system. This will frustrate users as they will not be able to utilize the system. This type of attack is known as denial-of-service attack (DoS) and it disrupts the workflow. Sony's online PlayStation store was attacked in a similar manner in 2014. The brute force attack was utilized in this hack attempt and the online store was down for nearly a day. Many organizations that have their workloads on the cloud will be attacked in the same way to stop their daily operations.

Such DoS attacks can be prevented in various ways including updating intrusion detection systems, blocking IP addresses, and firewall traffic inspection. The system must be able to determine anomalies when users try to access the system and early warning needs to be provided. On the basis of anomalies in credentials and behavioral aspects, the system can provide early alarm to ensure cloud security. Moreover, the suspicious IP addresses should be blocked. Security teams can also inspect the incoming traffic. The source and destination of incoming traffic can be inspected and firewall can be placed by differentiating the good and bad traffic.

Such security measures can be taken to prevent the cloud systems from hackers and cyber-criminals. The cloud adoption will surely increase in the next years and the need to deploy stringent security measures to prevent different types of attacks will rise consequently. With increased awareness,

competent security teams, and advanced tools at hand, organizations can ward off attacks and ensure smooth functioning of cloud systems.

About the Author

Pratik Kirve is writer, blogger, and sport enthusiast. He holds a bachelor degree in Electronics and Telecommunication Engineering, and is currently working as a Team Lead - Content Writing at Allied Market Research. He has an avid interest in writing across different verticals. When he is not following the updates and trends, he spends his time reading, writing poetry, and playing football. He can be reached at pratik.kirve@alliedanalytics.com

LinkedIn - https://www.linkedin.com/in/pratik-kirve-8213b284/

Why Throwing Money at Cybersecurity Doesn't Work

By Zac Amos, Features Editor, ReHack

Cyberattacks have become more frequent and debilitating as the work gets more tech-centric. With so many advanced and expensive security tools available, companies should be able to protect their online information, right? It's not that simple. Here's why throwing money at cybersecurity doesn't work.

More Money, More Problems

The problem with devoting more finances to cybersecurity isn't the money itself but how organizations use it.

According to a survey from security firm Trend Micro, 42% of 5,000 surveyed companies spend most of their cybersecurity budgets on risk mitigation. Instead of investing in proactive solutions, they are constantly paying for damage control. This finding should come as no surprise, as many employers still neglect cybersecurity awareness training.

Social engineering, malware and other basic attacks remain the greatest threats to most businesses. A larger emphasis on training would be a simple, cost-effective way to combat these risks, yet people continue to ignore their weak points and take action when it's too late.

One reason companies are still undertrained is that they think an advanced cybersecurity infrastructure will do the dirty work for them. The system will stop all threats with no human intervention required. Of course, this misconception is not true. The cyberthreat landscape is always changing, so all systems need regular audits to address their vulnerabilities.

Another problem with throwing money at cybersecurity is a lack of standardization. Using a wide range of tools to manage security threats can lead to operability issues. Collecting data for risk assessment is a key part of cybersecurity, but that task becomes more difficult as more information sources get added to the mix.

More information does not always lead to more accurate risk assessments. Each tool operates independently, so each batch of data is also independent. This structure lacks the centralized intelligence that large organizations need to identify and address risks in a timely manner. Managing a constant stream of alerts is another downside to using many tools.

Moreover, some companies add extra layers of defense just to meet compliance checklists. The security team might not even know a tool's intended purpose. They won't be able to interpret the data correctly if they don't understand how the program works. As the late management educator Peter Drucker once said, "you can't manage what you can't measure."

Cybersecurity Fundamentals

Throwing more money at cybersecurity can lead to an adequate solution, but it needs direction. The real fix is choosing the right investments and learning how to maintain them. Here's what businesses should focus on to improve their cybersecurity.

1. Cloud Storage

Rather than buying a bunch of miscellaneous security tools, businesses should take a more centralized approach with cloud storage. Cloud storage keeps data on one platform, making monitoring and evaluating much easier. The security team can oversee employee information, customer files and financial records from one standard source.

Cloud computing is especially beneficial for remote employees who spend most of their time navigating the web on their own devices. They're more vulnerable to a cyberattack than in-house workers. A cloud storage system can give their information the same protection as the rest of the staff.

2. Automated Analytics

The human presence remains an important part of cybersecurity, but as we've established, people often get in their own way. Thanks to artificial intelligence (AI) and machine learning (ML), businesses can use automated analytics tools to monitor their data and identify security threats.

A detection system with AI and ML constantly gathers insights about its organization's strengths and weaknesses. When a threat emerges, it determines the severity and sends an automatic alert so the security team can address it.

3. Awareness Training

The human part of cybersecurity that businesses need to prioritize is awareness training. A workforce that knows the most common threats and best security practices is less likely to expose sensitive information. Building smart online habits from the ground up is the most surefire way to keep cyberthreats out.

Some job positions need more detailed training than others, so multiple programs might also be necessary. An in-person and online program is the bare minimum.

Most importantly, businesses must understand that awareness training isn't a one-time thing. Cybersecurity is an ongoing responsibility. The programs should be updated frequently to ensure employees know about recent developments in the best habits, tools and other topics that will help them protect their data.

Fundamentals Over Funding

When it comes to cybersecurity, fundamentals will always be more important than funding. A business can throw as much money at cybersecurity as it wants, but it doesn't mean anything without sufficient centralization, analysis and training. These basics will build the foundation of a safe, secure network.

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.

ZTNA and the Distributed Workforce: Hype vs. Reality

By Timothy Liu, CTO & Co-Founder, Hillstone Networks

ZTNA, or zero-trust network access, seems to be one of the hottest cybersecurity buzzwords right now, at least as measured by the coverage it's been receiving. At its core, ZTNA is a fairly straightforward construct that purports to improve security across the board, especially for the distributed workforce. Its basic premise is to eliminate implicit trust in users, devices and other network elements, which will theoretically reduce overall attack exposure including multi-level, multi-phase threats. Is all the buzz warranted, though? At Hillstone, we believe the answer is a resounding 'Yes,' with a few qualifications.

But First, A Look Back

Before examining ZTNA in detail, it's important to understand why this new model is being proposed and promoted. Achieving a means of secure remote access has been an objective of IT professionals almost since the very first data networks were developed. In the early 1990s, several early methods of securing remote access arose, such as SIPP. In the mid-1990s the secure sockets layer (SSL) protocol was released and it became the underlying technology for the enterprise-class SSL VPNs that are still in wide usage today.

(Author's note: Though most in the industry still refer to this type of secure remote access as SSL VPN, technically the technology is now based on transport layer security (TLS), which superseded SSL in about the mid-2000s.)

SSL VPNs are available as stand-alone appliances, as part of next-gen firewalls (NGFWs) and other security products like Hillstone Networks' solutions, and as cloud services. Early in the pandemic, when governments attempted to lock down their populations to prevent the spread of COVID-19, many corporate IT teams turned to SSL VPNs to support workers who suddenly needed to work from home.

Now, however, the distributed workforce has become a reality rather than a phenomenon, and the need to support remote workers in large numbers has brought certain issues and limitations of SSL VPN to the fore, including:

Common Vulnerabilities: Over the years, numerous vulnerabilities in enterprise-class VPNs have become apparent, raising red flags for many cybersecurity professionals. In 2021, for example, multiple U.S. federal civilian organizations faced the potential of data breaches via the Pulse Connect Secure VPN vulnerability. Two years earlier, in response to active exploitations of certain VPNs, the U.S. National Security Agency issued an advisory.

Licensing Costs and Expansion Limitations: Usually, commercial SSL VPNs are licensed per-user and per-capacity, meaning that scaling to support additional remote workers can be expensive both in purchase of licenses as well as in IT staff labor. Physical SSL VPN appliances might also require the purchase of additional modules in order to expand capacity.

User Authentication: Visibility into users and devices that are connected to the network is one of the bedrock principles of cybersecurity. A typical enterprise VPN will perform authentication just once, on initial login and set-up of the VPN tunnel, and then access is granted for all the network resources for which the user is pre-approved. This can create a security risk if, for example, user credentials are stolen by an attacker.

As mentioned, SSL VPNs are in broad use; the market in 2021 was estimated at nearly $5b USD. There's a cost connected with a forklift upgrade to a new secure remote access technology, but with the issues and concerns raised above, many security teams are considering ZTNA as another option.

ZTNA: Basic Definition

At its most basic, the mantra of ZTNA is 'never trust, always verify.' To expand upon that, ZTNA is intended to abolish absolute trust of devices and users and to allow only the minimum access and authorization based on user role, position or other factor. Under ZTNA, authentication is constant and ongoing – a change in the user's or device's security posture can result in revocation of access, for example. If it's executed well, ZTNA can deliver extremely fine-grained visibility and control with improved scalability, flexibility and reliability.

From a technological viewpoint, ZTNA employs a user-to-application approach, rather than the traditional network-centric focus, which completely inverts the concept of authentication. With ZTNA, users and devices are examined at a deeper level – encompassing identity as well as the context of network and application resources being requested.

It's important to note that the user-to-application approach expands security past the network perimeter to any resource connected to the network. This can include cloud applications and resources, for example, or remote physical or virtual applications and data.

Industry analyst firm Gartner has promoted the concept of the secure access service edge (SASE), which includes ZTNA as one of its elements. SASE, another hot topic in the cybersecurity world, consists of cloud-based security infrastructures to serve the new distributed workforce. Two closely related key benefits of SASE are reduced latency and an improved user experience.

A Practical Path Forward

Given the wide adoption and usage of SSL VPN, any conversation about transitioning to ZTNA must account for the older technology. There's just too much current investment in platforms, IT staff time, and education of end-users to simply discard existing SSL VPN solutions. Luckily – and partly by design – ZTNA easily lends itself to a more stepwise approach.

For example, Hillstone's ZTNA solution leverages Hillstone NGFWs as well as the Hillstone Security Management (HSM) platform to overlay ZTNA authentication over SSL VPN capabilities. The combined solution can leverage a wide range of authentication protocols and provides tight controls over users and devices with role- and context-based policy enforcement. Another possibility is to leverage the security capabilities of SD-WAN (another of the elements of SASE) alongside SSL VPN services to serve as a bridge to ZTNA and SASE later.

Conclusion

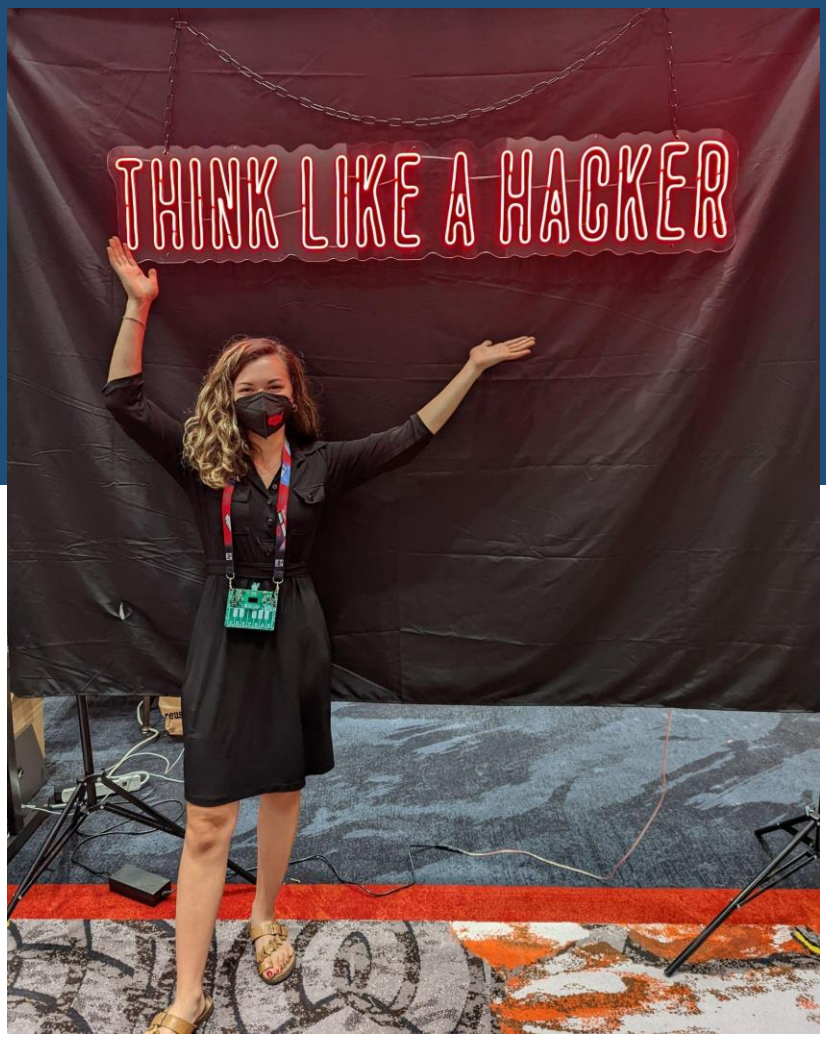
Ultimately ZTNA is a nascent cybersecurity technology – though it seems to be maturing quickly. Development efforts will eventually lead to consolidation and standardization, which will give manufacturers and security pros alike a set of table stakes to shoot for. For now, whether ZTNA is just the latest hashtag or the real deal will depend upon how it's implemented. It will require careful consideration of how it can co-exist with the existing security framework, support and enhance security policies, and better secure and defend the entire network from core to endpoint to cloud.

About the Author

Timothy Liu is Co-Founder and Chief Technology Officer of Hillstone Networks. In his role, Mr. Liu is responsible for the company's product strategy and technology direction, as well as global marketing and sales. Mr. Liu is a veteran of the technology and security industry with over 25 years of experience. Prior to founding Hillstone, he managed the development of VPN subsystems for ScreenOS at NetScreen Technologies, and Juniper Networks following its NetScreen acquisition. Mr. Liu is also a co-architect of the patented Juniper Universal Access Control and holds an additional patent on Risk Scoring and Risk-Based Access Control for NGFW. In his career, Mr. Liu has served in key R&D positions at Intel, Silvan Networks, Enfashion and Convex Computer. He Liu holds a Bachelor of Science from the University of Science and Technology of China and a Ph.D. from the University of Texas at Austin.

Tim can be reached online at @thetimliu and at our company website https://www.hillstonenet.com/

Surviving And Thriving The Hacker Summer Camp: A Cybersecurity Student's First Time Experience With Defcon, Blackhat, And The Diana Initiative

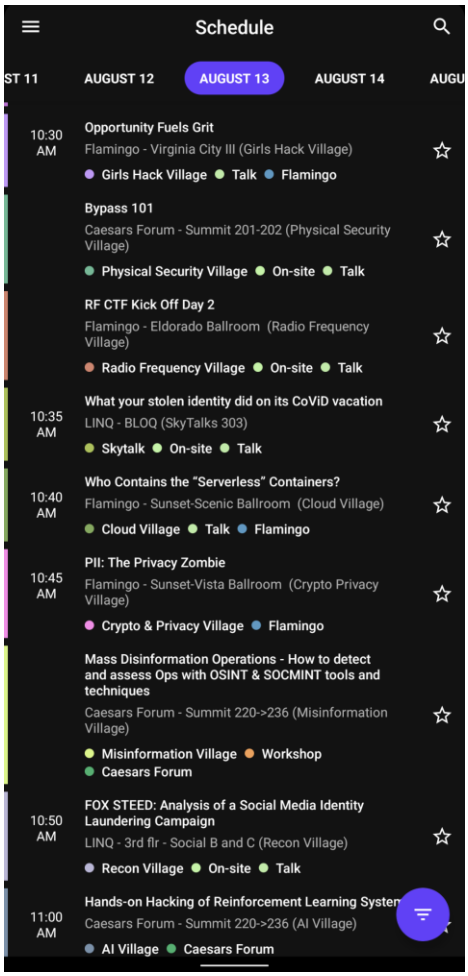


Earlier in August, I experienced my first Hacker Summer Camp - three cybersecurity conferences that ran from August 10th to August 14th. While I didn't make my way to BSidesLV, I attended The Diana Initiative, BlackHat, and DefCon in what turned out to be a whirlwind of a week. From preparing to go through walking the conference floor, I found the whole experience to be an invaluable part of my experience in cybersecurity.

Preparing

Having never been to multiple large-scale cybersecurity conferences within a short time frame, I didn't know what to expect. Even prepping for the conference and trying to come up with a game plan was overwhelming. I watched previous recordings, joined the DefCon Discord community, and did some research on the conferences.

Taking advice from previous attendees, I decided to come up with a list of key items I wanted to get out of the conferences. With so many things going on, it's difficult to do everything, so I knew going into it that I had to pick and choose what to try. I was also advised to not make recorded presentations a priority, as they could always be rewatched later.



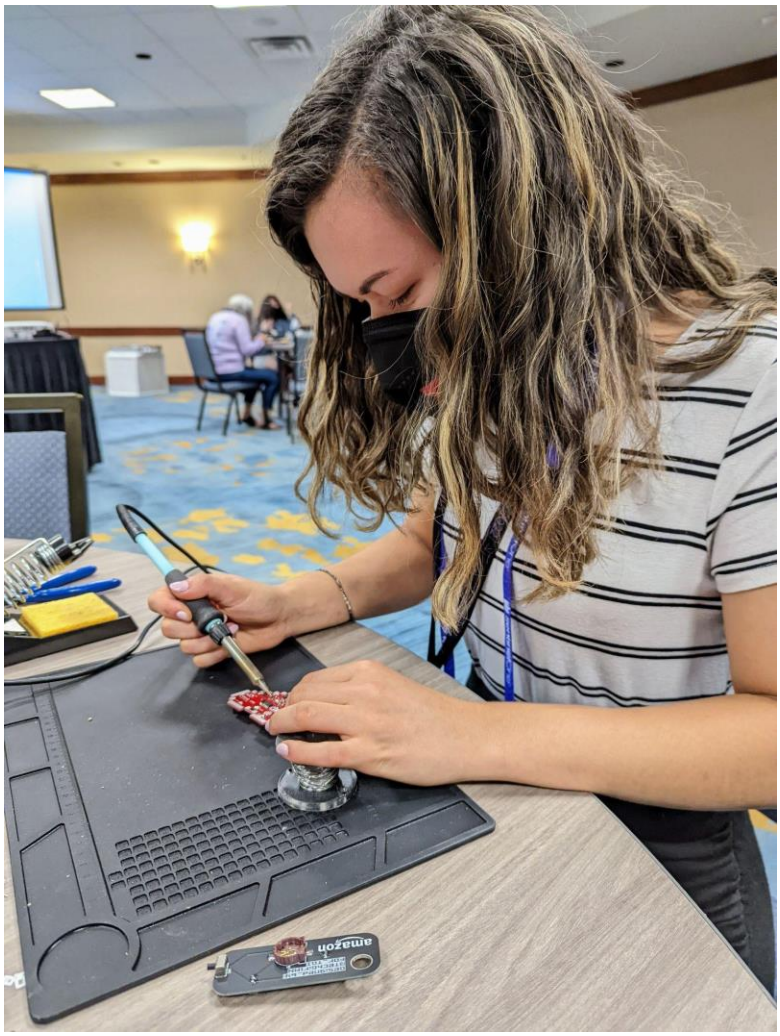
With all this in mind, I carefully looked at the schedules for the various conference activities so I could make a rough plan to try and follow. However, as I continued to join communities and network with other

professionals, I began to find more people I wanted to try and meet. I slowly began adjusting my schedule accordingly to set up meetings and lunches. I created a rough schedule that I could try and follow but knew that things might change so I kept things as flexible as they could be. As the conferences approached, I was ready to dive in and immerse myself.

Game Day(s)

The Diana Initiative - August 10-11

I started by going to The Diana Initiative where **Jen Easterly**, the Director of the **Cybersecurity and Infrastructure Security Agency** (CISA), was the keynote speaker. Additionally, I had the opportunity to listen to my dear friend **Weijia Yan**, share her journey through tech. The Diana Initiative also had a Surface Mount Device (SMD) workshop where I soldered a small heart-shaped circuit board. When turned on, the device had lights that blinked.



Overall, this was a great conference with a smaller feel that allowed for a more hands-on, discussion, and participatory approach in the presentations and workshops. It was wonderful to be surrounded by those who are working to build a more diverse and inclusive community that is welcoming to myself and others. It is inspiring to be a part of communities and initiatives like these that are trying to build a better future.

BlackHat - August 10-11

Walking into the venue for BlackHat, I immediately knew it was going to be a massive conference and completely different from the Diana Initiative. There was a giant BlackHat sign surrounded by crowds walking to and from various sessions. Every session room I saw had hundreds upon hundreds of seats. Throughout the two days, I was able to sit in on a few presentations, spend hours in the vendor hall, and check out some of the social hours hosted by companies.

For example, **Matt Edmondson** from **Argelius Labs** gave an insightful presentation titled Chasing Your Tail with a Raspberry Pi. I've always had a fascination with integrating physical security with cybersecurity, so I knew I could not pass this up. Matt demonstrated how he used off-the-shelf parts and wrote code to be able to determine if someone is physically being followed. It was interesting to learn about the various techniques and methodologies he implemented and I loved that he made it open source which you can check out for yourself here.

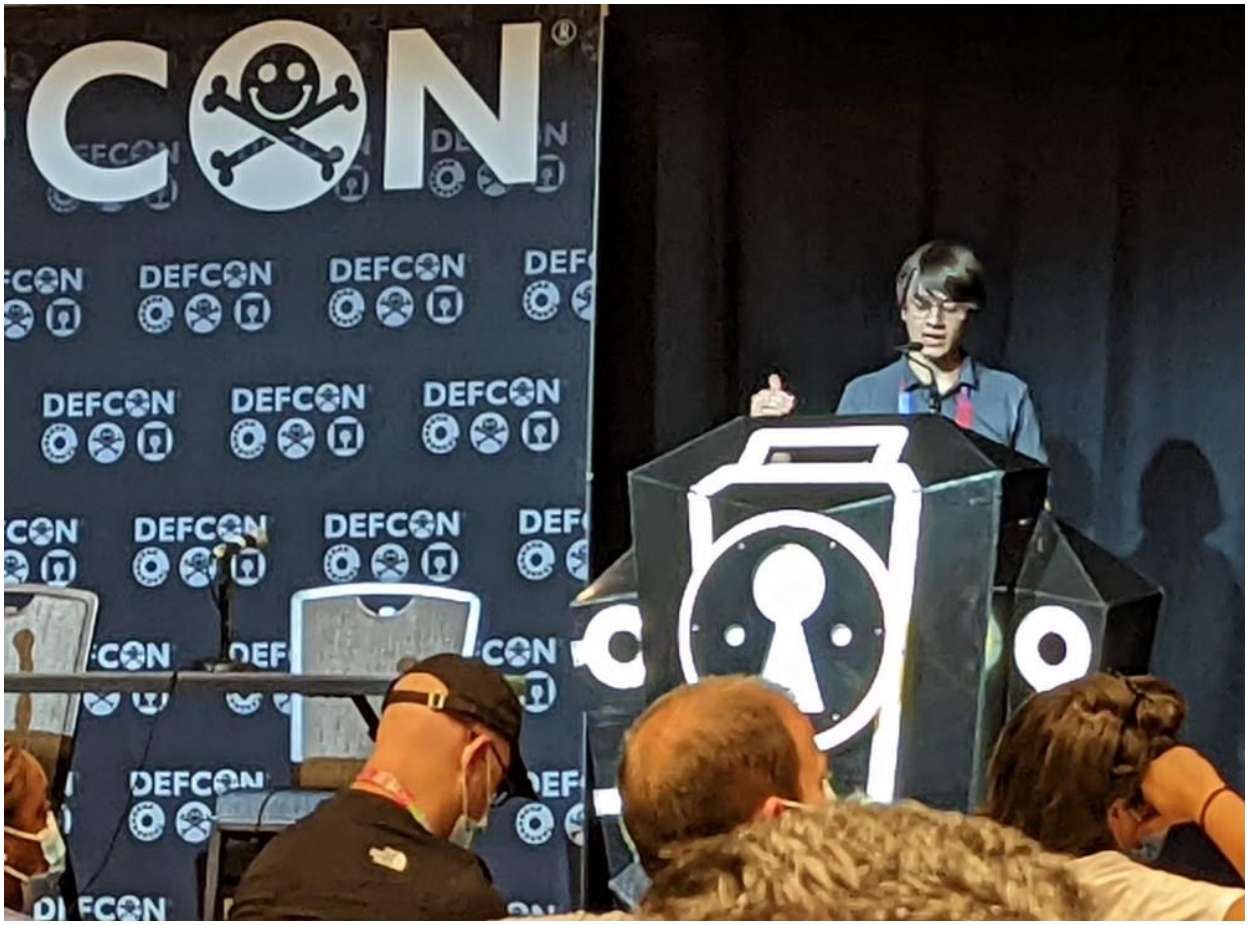
Another presentation worthy of noting is one titled Charged by an Elephant – An APT Fabricating Evidence to Throw You In Jail by **Juan Andrés** and **Tom Hege**l from **SentinelOne.** They showcased a threat actor's activities that have taken place over more than a decade. What was especially interesting was learning the various ways they planted evidence that incriminated others. It was scary to learn how they discovered multiple other threat actors were targeting the same victims.

DefCon - August 11-14

This was the big conference, what everything had led up to, and by far the most overwhelming for me. There were so many things going on that even a couple of days in, I was still finding out that there were more things to do and check out. I could go on and on about everything I did and saw at DefCon but I'm assuming you don't have hours to read so I'll save you the time and just list a few of my favorite highlights.

One of the unique things about DefCon is that they have a track of presentations called **Skytalks**. Skytalks are presentations that are completely off the record - they do not allow cameras or recording. The room had roughly 300 seats and each chair was spaced a couple of feet apart so that the volunteers could ensure that individuals were not recording or on their devices. I had the opportunity to attend two of them - Geo-Targeting Live Tweets and Eradicating Disease with BioTerrorism.

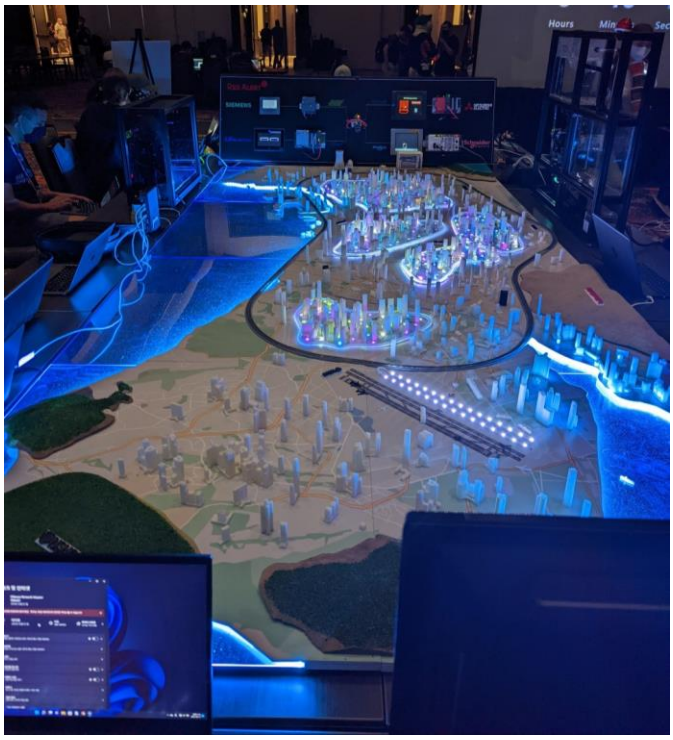
I saw why Skytalks was a huge rage at the conference. A majority of the time, one would have to get in line an hour before the talk starts to get a spot. The trick I used was to try and go to the earliest Skytalk for that day. This proved to be successful since there weren't as many people as some had stayed up late the night before (probably partying) and didn't get up as early.



Some of the other presentations I learned from was one by the Co-Founder of **Tor**, **Roger Dingledine**. He explained How Russia is Trying to Block Tor and their techniques and how the Tor group reverse engineered their attempts which caused them to change their strategies and approach. **James Pavur** gave an insightful presentation on various radio frequency attacks that go on in outer space. He demonstrated how state and non-state actors can, and have, executed physical-layer attacks on satellite communications systems that have caused disruptions.

Another component of DefCon is the vast amount of villages they have. These villages contained talks, demonstrations, and typically a hands-on component where attendees could try their hand at it. For this year's DefCon, they had 20+ villages. I was able to at least see every village but did not have time to try my hand at everything.

Of where I was able to spend time at the **Biohacking** Village, being able to see and understand the security behind some medical devices was rather interesting. They had multiple tables of various health care devices and demonstrations of how they worked. It was scary to think about how much damage an attacker could do if medical devices didn't have proper security measures in place.



Aside from this, the **Industrial Control Systems** (ICS) Village was also fascinating! The **Red Alert** CTF within the ICS Village had a 3D model of a city and participants would try and gain access to the various

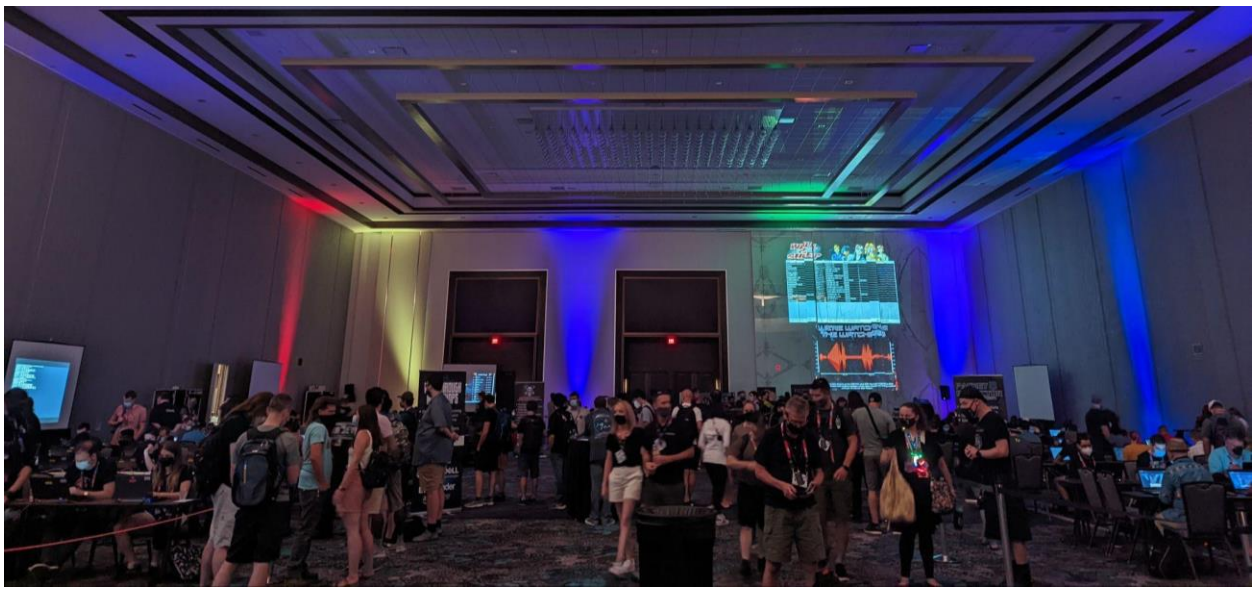
control systems to make changes. There was also a **Car Hacking** Village with a couple of cars (including a Tesla) with attendees trying their hand at breaking and circumventing the security measures.

One of my favorite villages, though, was the **Physical Security** Village. They had a variety of different physical security components, including a mock keypad for a gated community, door locks, elevator doors, etc. I tried my hand at bypassing some of the door locks and loved learning about the mechanics and design behind everything.

In the end, DefCon was by far one of my favorite cybersecurity conferences I have ever attended. There were so many things to do and I know I didn't cover even a quarter of them. I did my best to try and go to the hands-on villages over the presentations since those would be recorded. It was amazing to have a wide variety of topics, as there was something for everyone. Further, the community at DefCon was unlike any conference I had experienced. Despite the vast amount of attendees, it felt more customized, personable, and like a community than other conferences.

Networking

With thousands (easily 25k+ attendees) at these conferences, there were so many opportunities to meet industry leaders and others. Throughout the five days, I found that the Hacker Summer Camp is the time to meet most cybersecurity leaders in person. There were a few individuals and companies on my list, but there were others that I happened to run into or meet.



During the conferences, I had time to sit down and chat with **Bob Ackerman**. He founded **Allegis Cyber** - the world's original cyber-focused venture firm. Shifting from a reactive to a proactive approach and consolidating companies within the industry are some of the things he foresees happening in the future. With artificial intelligence improving every day, he noted that the offensive capabilities will also be developed and is something to watch out for.

As he was talking about the state of cybersecurity, it was very apparent that Allegis Cyber has a deep understanding of everything cyber-related and that they know the entire cyber ecosystem. Bob noted that a lot of start-ups in the industry are concerned about navigating the entrepreneurial path while trying to

have a successful company. It was insightful to hear his perspective on the industry and the problems he sees coming.

I had the opportunity to have lunch and meet **Cyrus Robinson** and **Kris Brochhausen** from **Ingalls Information Security**. They were also first-time attendees but I appreciated getting to hear about their journey and what they tried so far at the conferences. It was great to share experiences and also get some tips on what to check out at the conference.

Meeting the Founder of **GirlsWhoHack**, **Bia**, was amazing as well. She's a 15-year-old, young woman who is striving to increase the number of girls in the cybersecurity field. I was inspired to find another young woman with similar goals and aspirations. We discussed potential collaboration between my outreach program, the Cyber Community Club (Cx3), and GirlsWhoHack.

Finally, I was able to meet and chat with **Luke Potter**, the Chief Operating Officer of **CovertSwarm**. They bring together every element of cybersecurity testing to help companies locate every security vulnerability

they have. I was happy to share my thoughts and recommendations with Luke and **Jack Smith** as they're in the process of creating an intern program for their company which people should keep an eye out for.

In addition to meeting new people, I was able to see some familiar faces. Reconnecting with students from activities and competitions I participated in and colleagues from my previous cybersecurity internships, made the environment come full circle. It was a wonderful time to meet others in person and see the cybersecurity community come together.

Reflecting

As a young cybersecurity student and professional, I was overwhelmed with everything the conferences had to offer. From presentations to workshops to villages, to networking opportunities, and so much more, the conferences had endless amounts of opportunities. The five days of conferences felt like so much but I learned to slow down and stop worrying about being able to attend everything.

Ultimately, I had a great experience with the Hacker Summer Camp and can't wait to attend again. This time, I'll be more prepared and ready to learn new things! There were so many wonderful people I met, and I learned more technically, but also personally, and professionally. I highly recommend that anyone who's even slightly considering attending set aside the time and experience the conferences.

Tips + Advice

There are quite a few things I was thankful that I did that helped me make the most out of the conferences. I was glad I did research ahead of time and reached out to others for their advice. For those who plan on attending in the future, my top three tips are the following.

1. Don't try and do everything
    a. There are far too many things and you won't have enough time to do everything
2. Hydrate and have comfortable shoes
    a. It's a lengthy few days with long walks, so try and stay in the best condition you can
3. Prioritize properly
    a. Take advantage of things you can only do at the conference

While those five days were some of the busiest days I've ever had, I learned and met a ton of those in the industry. It was an invaluable experience for me that I will remember for years. I truly appreciate the time and effort that the organizers, staff, volunteers, speakers, and attendees put in to make the conferences a success. Here's to next year!

Acknowledgments: Thank you to everyone who took the time to share their knowledge with me and to the organizers and volunteers at all three conferences. I'd like to give a special note of appreciation to the Women in Security and Privacy (WISP) for sponsoring my BlackHat pass and to the Cyber Defense Media Group for sponsoring my DefCon pass.


EVENTS

CYBER DEFENSE CONFERENCES

THREE EVENTS IN ONE

Orlando, Florida, USA | October 27-28, 2022

One of the most exclusive, fun and educational CISO conferences of the year!

Limited to our selection of the top 100 CISOs in the world, amazing speakers and insider threat mitigation training by a world reknown expert - meets 100 top cyber defense companies in an intimate, high value two day summit

www.cyberdefenseconferences.com

IoT
in Oil and Gas

8th Annual CONFERENCE SEPTEMBER 12-13 2022

HILTON AMERICAS | HOUSTON, TX

3 Easy Ways to Contact Us:

Website: https://iotinoilandgas.energyconferencenetwork.com/iot2022
Telephone : +1 855-869-4260
Email address: info@energyconferencenetwork.com

Future Tech Event

UNDER THE PATRONAGE

سلطنة عُمان
وزارة النقل والاتصالات وتقنية المعلومات
Sultanate of Oman
Ministry of Transport, Communications and Information Technology

مسقط
العاصمة العربية الرقمية
Muscat Arab Digital Capital
2022

رؤية عُمان 2040
Moving Forward with Confidence

ENABLING OMAN'S VISION 2040

12 - 13 September 2022 | Oman Convention and Exhibition Centre | 9 am - 4 pm

HYBRID+ (In-Person and Online)

Future Tech is Sultanate of Oman's foremost B2B and B2G bespoke Technology Expo and Summit.

For Exhibiting Enquiries and Sponsorship Opportunities please contact:
Navneeth K, Director - Business Development
+968 9123 7892 | bdm@wpsummits.com
www.futuretechevent.com

ORGANISED BY

مسقط إكسبو
Muscat Expo

WPS
WHITE PAPER SUMMITS

FRANSEC

SECURING **FRANCE** FROM CYBER THREATS

13th - 14th September 2022

Paris, France

Join Free With Code: CDM-VIP

Join Us at the FranSec Summit on 13th - 14th September!

The 3rd annual **FranSec Summit** brings together **100+ IT security leaders** from across the **Retail, FMCG, Banking & Finance, Automotive, Utilities, Food & Beverage industries** for 2-days of insight building and expert knowledge exchange on **13th - 14th September.** Join us in **Paris, France** to hone your skills in areas including:

- *Digital transformation and cyber resilience*
- *The current cyber landscape and how to improve your security capabilities*
- *Working with third parties to improve your cyber security posture*
- *Reacting to an increasing attack surface*
- *Implementing risk-based security strategies*
- *The human factor in organisational cyber security*
- *And, more!*

CPD CERTIFIED
The CPD Certification Service

Speakers include CISOs, VPs, Heads of IT Security at: **La Banque Postale, Airbus, AXA, Interpol, Total, Suez,** and more...

Helene Bernardini
CISO
Groupe Lactalis

Xavier Boidart
Group CISO
Crédit Agricole

Maran Madiajagane
CISO
RAJA

Clara Le Gros
Deputy CISO/DPO
NATIXIS

Cristophe Civarella
Deputy CISO
Crédit Mutuel ARKEA

Stephane Boua
CISO
Groupe Les Echos Le Parisien

Michael Bonhomme
Group CISO / Head of IT Security
Baobab

Francis Bergey
Deputy CISO, Security Expert
eVoyageurs SNCF

Badi Ibrahim
Head of Hotels IT Security
Accor

Joy-Alexandra Denis
Deputy CISO
Arquus

This is a one-of-a-kind opportunity for cyber security leaders across France to come together and safeguard their assets. View the agenda & **secure your place for FREE** using the discount code: **CDM-VIP** at: **france.cyberseries.io/register/**T&Cs apply.

BLOCKCHAIN in OIL & GAS

6th Annual

CONFERENCE

SEPTEMBER 14-15

2022

HILTON AMERICAS - HOUSTON, TX

3 Easy Ways to Contact Us:

Website: https://blockchain-oilandgas.energyconferencenetwork.com/bcog2022
Telephone : +1 855-869-4260
Email address: info@energyconferencenetwork.com

A/001

SYSTEM ACTIVATED

breach

3rd MIDDLE EAST CYBERSECURITY & BIOMETRICS FORUM

CS Event Management
Your Event, Your Terms

21st September 2022

Geography of Focus: Qatar

mecybersecurityforum.csevents.ae

CYSEC SAUDI

04 OCTOBER 2022

DAMMAM, SAUDI ARABIA

JOIN US IN-PERSON

SECURING KINGDOM'S CRITICAL INFRASTRUCTURE IN THE NEWLY CONNECTED WORLD

SPONSORS

PLATINUM SPONSOR

SITE
الشركة السعودية لتقنية المعلومات
Saudi Information Technology Company

GOLD SPONSOR

iTalent

ORGANIZED BY

MAK

ENERGIA MIDDLE EAST

saudi.cysecglobal.com

NORDIC CYBER SUMMIT

4th - 5th October 2022

Copenhagen, Denmark

Join Free With Code: CDM-VIP

Join Us at the Nordic Cyber Summit Summit on 4th - 5th October!

The 4th annual **Nordic Cyber Summit** brings together **120+ IT security leaders** from across the **Retail, FMCG, Banking & Finance, Automotive, Utilities, Food & Beverage industries** for 2-days of insight building and expert knowledge exchange on **4th - 5th October.** Join us in **Copenhagen, Denmark** to hone your skills in areas including:

- *Staying Ahead of an Evolving Threat landscape*
- *Working with Third Parties*
- *Revamping Your Cyber Security Approach*
- *Migrating to the Cloud*
- *Ransomware: Reducing Risk and Incident Response*
- *The Human Factor in Cyber Security*
- *And, more!*

CPD CERTIFIED
The CPD Certification Service

Speakers include CISOs, VPs, Heads of IT Security at: **Carlsberg, Danske Bank, Velliv, Total, Nomeco, Orkla** and more...

Jarkko Rautula
CSO
TOMTOM

Duong Anders Le
CISO
JYSKE BANK

Moon Carlbring
CISO
Region Västmanland

Predrag Gaiki
Deputy CISO/DPO
QLIRO

Stale Risem-Johansen
CISO
SpareBank 1

Anne Hännikäinen
CISO
IKEA

Geir Arild Engh-Hellesvik
CISO
VY

Tobias Ander
Deputy CISO, Security Expert
ÖREBRO

Ingegerd Wirehed
Head of Hotels IT Security
LUNDS UNIVERSITET

Mikael Nyman
Head of IT Security
Länsförsäkringar

This is a one-of-a-kind opportunity for cyber security leaders across the Nordic region to come together and safeguard their assets. View the agenda & **secure your place for FREE** using the discount code: **CDM-VIP** at: **nordic.cyberseries.io/register/** T&Cs apply.

CYBER SECURITY & CLOUD CONGRESS

NORTH AMERICA

5-6 October 2022
Santa Clara
Convention Center

We're Back!
Join Us Live & In-Person

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

8 Conference Tracks

250+ Speakers

150+ Exhibitors

6 Co-Located Events

6,000+ Attendees

Speakers include:

Kavitha Venkataswamy
Senior Manager - Product Security
Capital One

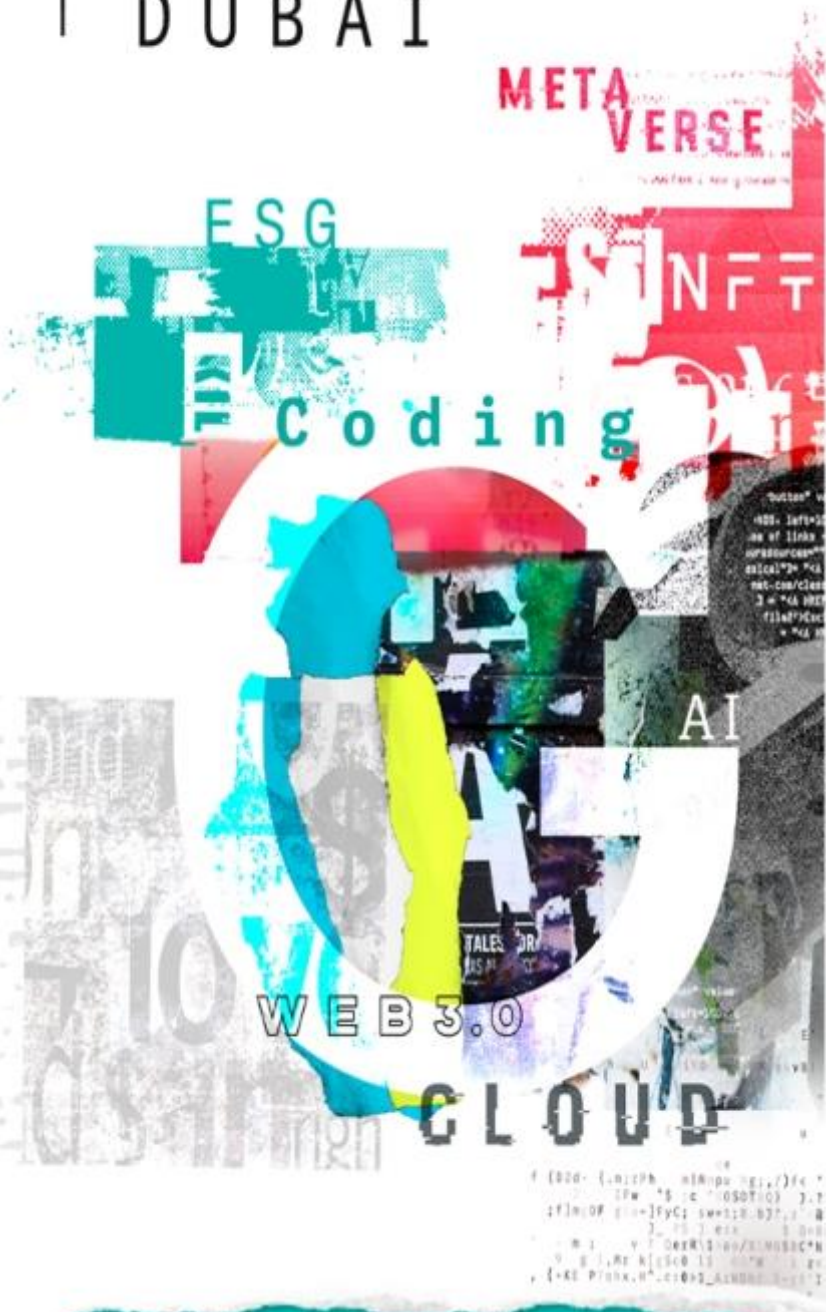
Michael Fulton
Adjunct Faculty
The Ohio State University

Elizabeth Cartier
Director - Information Security
Headspace Inc.

Register now for free tickets!

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

GITEX GLOBAL | 10-14 OCT 2022 DUBAI



BELIEVE THE HYPE, IT'S HERE.

Enter the Next Digital Universe.

GET YOUR PASS

BENELUX CYBER SUMMIT

11th - 12th October 2022

Amsterdam, Netherlands

Join Free With Code: CDM-VIP

Join Us at the Benelux Cyber Summit Summit on 11th - 12th October!

The 3rd annual **Benelux Cyber Summit** brings together **100+ IT security leaders** from across the **Retail, FMCG, Banking & Finance, Automotive, Utilities, Food & Beverage industries** for 2-days of insight building and expert knowledge exchange on **11th - 12th October**. Join us in **Amsterdam, Netherlands** to hone your skills in areas including:

- *Balancing the business's push for digitalisation with cyber security needs*
- *Devising modern supply chain security strategies*
- *Strategies to enhance the responsiveness to attacks and their mitigation*
- *Managing risk in an evolving threat environment*
- *Updating security to work cross-functionally in order to secure the supply chain*
- *How to monitor data security in the cloud and address compliance management challenges*
- *And, more!*

CPD CERTIFIED
The CPD Certification Service

Speakers include CISOs, VPs, Heads of IT Security at: **Amazon, RTL, Philips, PayPal, Volvo Financial Services** and more...

Jacques Federspiel
CISO
HÔPITAUX ROBERT SCHUMAN

Victoria van Roosmalen
CISO & DPO
COOSTO

Haissam Hariz
Deputy CISO
NIBC

Stanislav Sobolevsky
CISO
OMP.

Steffen Minkmar
Sr Head, IT Security Unit
European Investment Bank

Rick Veenstra
Sr Advisor IT Risk & Security
isala

Andre Adelsbach
VP, Group Information and Cyber Security
SES

Stella Dineva
IT Security Architect
ucb

Filip Nowak
Global Head of Cyber Defence
FERRERO

Fred Jekel
Executive Director Cyber Security
VAN LANSCHOT KEMPEN

This is a one-of-a-kind opportunity for cyber security leaders across Benelux to come together and safeguard their assets. View the agenda & **secure your place for FREE** using the discount code: **CDM-VIP** at: **benelux.cyberseries.io/register/** T&Cs apply.

Industrial Transformation ASIA-PACIFIC

Asia-Pacific's Leading Trade Event for Industry 4.0

18-20 October 2022
Singapore EXPO

www.industrial-transformation.com

We help companies in Asia-Pacific to **START, SCALE** and **SUSTAIN** their business transformation journey

CONNECT WITH US • CONNECT WITH ASIA-PACIFIC

Register now to attend in-person at **Singapore EXPO**

INDUSTRY 4.0 FOR BUSINESS SUSTAINABILITY

Themed 'Industry 4.0 for Business Sustainability', the 5th edition of the Industrial Transformation ASIA-PACIFIC - a HANNOVER MESSE event (ITAP) happening on 18-20 October 2022 will deep dive into trends and developments in three key dimensions i.e. Digitalisation, Talent & Workforce Development, and Environmental Sustainability, which influences the magnitude of sustainable business development for advanced manufacturing and its related sectors locally, regionally and globally.

An Event Of

constellar

International Partner

Deutsche Messe

a HANNOVER MESSE event

Industrial Transformation ASIA-PACIFIC

EURONAVAL

THE WORLD NAVAL DEFENCE EXHIBITION

28th edition

18 21 OCTOBER 2022

PARIS LE BOURGET

euronaval.fr

CYSEC UAE

SUPPORTED BY

هيئة أبوظبي الرقمية
ABU DHABI DIGITAL AUTHORITY

OFFICIAL GOVERNMENT SUPPORTING PARTNER

شرطة أبوظبي
ABU DHABI POLICE

1 - 2 NOVEMBER 2022

JOIN US IN-PERSON, ABU DHABI, UAE

Accelerating UAE's Digital Transformation with Next-Gen Cyber Resilience

Asma Al Yassi
Cyber Security Governance
Confidential

Dr. Lt. Col. Hamad Khalifa Al Nuaimi
Head of Telecommunications Division, Information Technology Center
Abu Dhabi Police General Head Quarter

Dr. Ebrahim Al Alkeem
Digital Transformation
Cyber Security
Artificial Intelligence
Expert Director
Government of Abu Dhabi (UAE)

Eng. Ahmed Sherif
Senior IT Support Engineer & Cloud Solutions Expert
Abu Dhabi Digital Authority – UAE

Mohammed Darwish Azad
Chief Information Security Officer
Emirates NBD

Bader Husni Zyoud
Senior Information Security Risk Management Specialist & Incidents Manager
Central Finance Department, Government Entity

Hala ElGhawi
Sr. Information & Cyber Security Risk Manager
Standard Chartered Bank

Jeevan Badigari
CISO
DAMAC Properties

Ellis Wang
Board Of The Executive & Advisory Team
The Private Office of Sheikh Saeed bin Ahmed Al Maktoum

Omar Osman
Information Security Officer
Malaffi (Abu Dhabi Health Information Exchange)

Taha Hussain
Specialist Information Security
DEWA (Dubai Electricity & Water Authority)

Shafiullah Ismail
Vice President & Head - Cyber Security and Risk
Mubadala Capital

Malak Trabelsi Loeb
Director of Corporate Global Affairs
Cyber Security Global Alliance

Munther Bin Amr
Director of ICT
Abu Dhabi Quality and Conformity Council

Khawla Al Badi
Head of Innovation and Technology
Etihad Airways

OFFICIAL MEDIA PARTNER

Industry Events

MEDIA PARTNERS

SECURITY MIDDLE EAST — THE MAGAZINE FOR SECURITY AND SAFETY PROFESSIONALS

CYBER DEFENSE MAGAZINE — WHERE INFOSEC KNOWLEDGE IS POWER

GlobalRisk Community

OXFORD BUSINESS GROUP

INTERNATIONAL BUSINESS MAGAZINE

JUMPSTART

TECH OUTLOOK CIO

ICOHOLDER

ORGANIZED BY

MAK

uae.cysecglobal.com

DIGITAL TRANSFORMATION KUWAIT

ACHIEVING 2035 VISION THROUGH DIGITAL TRANSFORMATION

02 – 03 NOVEMBER 2022

JUMEIRAH MESSILAH BEACH HOTEL & SPA - KUWAIT

IN COLLABORATION WITH:

Central Agency for Information Technology

With digital transformation as a key pillar for Kuwait Vision 2035, the country is focusing on adopting smart and digital technologies to innovate its services, drive the economy, and improve quality of life, while increasing operational efficiency and performance of key sectors. This goal has pushed for greater investment in Kuwait's ICT market which is expected to reach 10B USD by 2024 (Global Data).

EVENT IN NUMBERS

- **250+** ATTENDEES
- **150+** SENIOR DECISION MAKERS
- **25+** SPEAKERS
- **20+** MEDIA PARTNERS
- **30+** SPONSORS & EXHIBITORS

INTERESTED IN FINDING OUT MORE ABOUT HOW YOU CAN PARTICIPATE?

Email us directly at **partnerships@gmevent.ae** or call **+971 52 969 7209** and a member of the team will be happy to help.

WWW.DIGITALTRANSFORMATIONKUWAIT.COM

ORGANIZED BY:

GM EVENTS

SCAN THE QR CODE TO LEARN MORE

AVAR 25 INTERNATIONAL CONFERENCE

AVAR 2022

CYBERSECURITY COUNTER PUNCH

1ST - 2ND DECEMBER 2022 | SINGAPORE

AVAR INTRODUCES

CISO Connect

Gather insight on the challenges and opportunities faced by CISOs through Panel Discussions:

1. Challenges in Organizational & Industrial Cybersecurity
2. Cybersecurity Trends for 2023 & Beyond
3. Is the CISO the Next New Board Member?

CISO Awards

- Best CISO Startup
- Best CISO Midsize Organization
- Best CISO Enterprise

Join Us
at the only platform that brings together Security Researchers and CISOs!

https://aavar.org/cybersecurity-conference/

Gold Sponsor

ESET

Silver Sponsors

CYBER THREAT ALLIANCE

AV comparatives

AhnLab

T-Shirt Sponsor

SE Labs

Lanyard Sponsor

K7 SECURITY

Media Sponsor

AV-TEST The Independent IT-Security Institute

Supporting Sponsor

AppEsteem

Media Partner

CYBER DEFENSE MAGAZINE

/avar-asia/ /avar_asia /aavar.org

LEVELLING UP UK CYBER SECURITY

We believe there is a knowledge gap between the expertise of the cyber community and UK business leaders.

We want to close that gap.

Contribute to the programme by visiting www.ukcyberweek.co.uk/call-for-papers.

OUR PARTNERS

IASME CONSORTIUM

Chartered Institute of Information Security

CREST

UK CYBERWEEK

3 ›› 4 NOVEMBER 2022

Business Design Centre | London

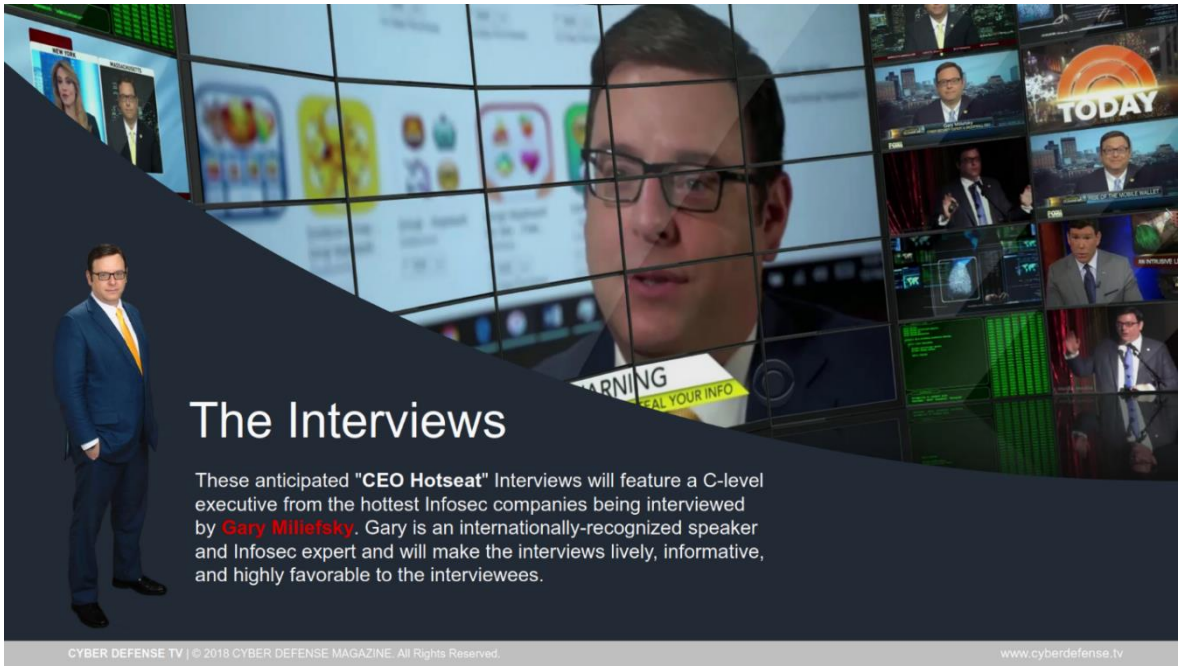
CYBER DEFENSE TV

INFOSEC KNOWLEDGE IS POWER

CyberDefense.TV now has 200 hotseat interviews and growing…

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

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



Free Monthly Cyber Defense eMagazine Via Email

Enjoy our monthly electronic editions of our Magazines for FREE.

This magazine is by and for ethical information security professionals with a twist on innovative consumer products and privacy issues on top of best practices for IT security and Regulatory Compliance. Our mission is to share cutting edge knowledge, real world stories and independent lab reviews on the best ideas, products and services in the information technology industry. Our monthly Cyber Defense e-Magazines will also keep you up to speed on what's happening in the cyber-crime and cyber warfare arena plus we'll inform you as next generation and innovative technology vendors have news worthy of sharing with you – so enjoy. You get all of this for FREE, always, for our electronic editions. Click here to sign up today and within moments, you'll receive your first email from us with an archive of our newsletters along with this month's newsletter.

By signing up, you'll always be in the loop with CDM.

Cyber Defense Magazine

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

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

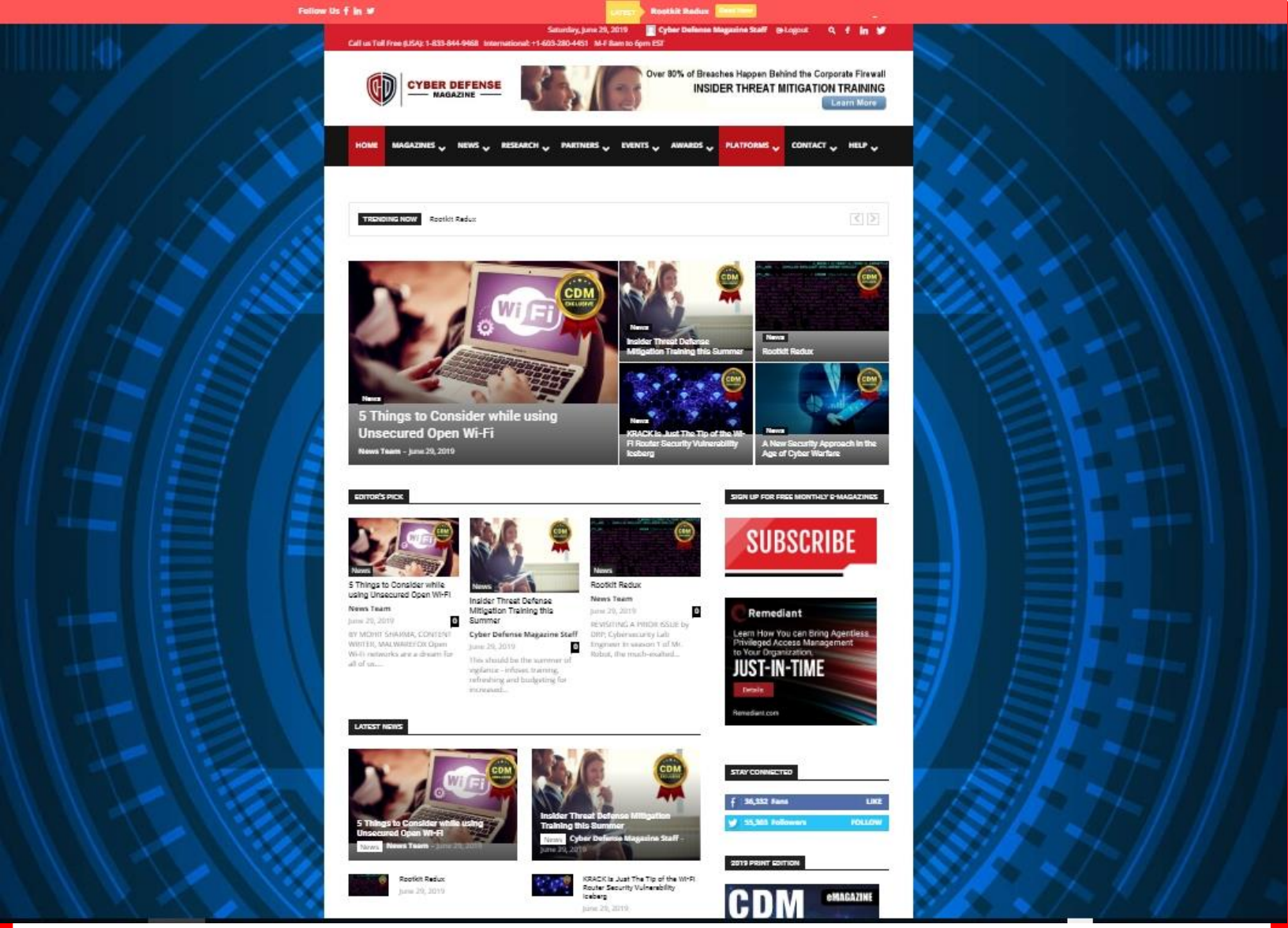
All rights reserved worldwide.

marketing@cyberdefensemagazine.com

www.cyberdefensemagazine.com

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

Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 09/01/2022



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

10 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 and our new B2C consumer magazine CyberSecurityMagazine.com. *Millions of monthly readers and new platforms coming…starting with www.cyberdefenseconferences.com this month…*

Preventing Tomorrow's Malware

Today.

www.cythereal.com

CYBER DEFENSE MAGAZINE

WHERE INFOSEC KNOWLEDGE IS POWER

www.cyberdefensetv.com
www.cyberdefenseradio.com
www.cyberdefenseawards.com
www.cyberdefenseconferences.com
www.cyberdefensemagazine.com

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