CYBER DEFENSE MAGAZINE

eMAGAZINE

AUGUST 2021

In This Edition

Understanding The Importance of Designing for Security

Evaluating Security Practices in Response to Colonial Pipeline And South Korean KAERI Attacks

Chinese Government Will Begin to Stockpile Zero-Days in September

…and much more…

MORE INSIDE!

CONTENTS

@MILIEFSKY

From the
Publisher…

TOP 10
BLACK
UNICORNS
2021
CYBER DEFENSE MAGAZINE

New CyberDefenseMagazine.com website, plus updates at CyberDefenseTV.com & CyberDefenseRadio.com

Dear Friends,

Continued uncertainty and challenges have arisen in the world of cybersecurity over the past month, and we have oriented our Cyber Defense Media Group response toward providing actionable information for meeting these trends.

In particular, as we've observed in past commentary, the emergence of a "New Normal" is problematical in this context. An illustrative example of this dynamic is the current uncertainty about whether the widespread phenomenon of Work from Home ("WFH") is going to continue or be resolved by a mass return to a centralized work environment. The cybersecurity implications are enormous.

Points of attention include ransomware and its likely connection to state actors. Whether directly or through insulation from prosecution, this will play out on the political stage. Nobody in a position of responsibility can ignore to threat this poses to the sustainability of national and global critical infrastructure.

From a cybersecurity point of view, we must prepare for all eventualities, especially those representing the "worst case scenario" of these developments.

As always, among the valuable resources we rely on to respond to cyber threats are the providers of cybersecurity solutions. Cyber Defense Media Group has now completed the nomination process for the 2021 Black Unicorns Awards **The winners will be unveiled and announced at the BlackHat USA Conference 2021 in Las Vegas, NV, USA. starting at 8:30am August 2, 2021 PST, and online, and in our Annual Black Unicorn Report for 2021.**

Wishing you all success in your own cyber endeavors.

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

InfoSec Knowledge is Power. We will always strive to provide the latest, most up to date FREE InfoSec information.

From the International Editor-in-Chief…

This month's international perspective on cybersecurity is largely driven by privacy regulations, ransomware developments, and criminals operating within jurisdictions which either deny their existence or refuse their extradition.

In an action closely related to this cybersecurity issue, the EU recently proposed a privacy initiative with strong cyber implications. We continue to see regulatory actions on privacy which also can have positive effects on cybersecurity defenses. One immediate manifestation of the continued effort to find a solution to the impasse concerning the EU-US Privacy Shield. While U.S. States are adopting their own privacy laws, it's imperative to avoid the patchwork approach in favour of umbrella regulations to facilitate trans-Atlantic data flows.

While we continue to observe that even compliance with laws, treaties and regulations may not absolve organizations from liability in the event of a data breach or ransomware attack, it's also worthwhile to recognize that at least three U. S. States have enacted "safe harbour" provisions to limit civil liability for breaches.

It appears that ransomware exploits are originating in nations which tend to harbor the perpetrators and hamper identifying and prosecuting them. We support both technical and political solutions to reach a compatible resolution of this challenge.

As always, we encourage cooperation and compatibility among nations and international organizations in responding to these cybersecurity and privacy matters.

To our faithful readers, we thank you,

Pierluigi Paganini
International Editor-in-Chief

@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.

PRESIDENT & CO-FOUNDER
Stevin Miliefsky
stevinv@cyberdefensemagazine.com

INTERNATIONAL EDITOR-IN-CHIEF & CO-FOUNDER
Pierluigi Paganini, CEH
Pierluigi.paganini@cyberdefensemagazine.com

US 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
SKYPE: cyber.defense
http://www.cyberdefensemagazine.com

PUBLISHER
Gary S. Miliefsky, CISSP®

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

9 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:

CDMG B2C MAGAZINE

B2B/B2G MAGAZINE TV RADIO AWARDS

PROFESSIONALS WEBINARS

Welcome to CDM's August 2021 Issue

From the U.S. Editor-in-Chief

The range of subjects covered by our contributing authors this month is both broad and indicative of the many facets of cybersecurity in our global economy and society. We include both immediate responses to the developing challenges of ransomware exploits and more generalized articles on preparing for the continued onslaught of cyber-attacks during a period of great uncertainty.

Our editorial policy and practice concentrate on selecting and publishing the most relevant and actionable information for cybersecurity professionals and others interested in the trends and implications of these developments.

Events of the past month have shown that the 16 elements of our critical infrastructure are fast becoming the most targeted areas for cyber criminals. In my role as editor, I would renew my call to our readers to become familiar with the 16 areas of critical infrastructure designated by the Department of Homeland Security, found at www.dhs.gov . Going forward, activities in these areas will become more and more important in the world of cybersecurity.

In that context, our articles this month cover a full spectrum of recognition of threats, appropriate preventive measures, means of assuring resilience and sustainability, and operational aspects of organizations needing to maintain the confidentiality, accessibility, and integrity of sensitive data.

We strive to make Cyber Defense Magazine most valuable to our readers by keeping current on emerging trends and solutions in the world of cybersecurity. To this end, we commend your attention to the valuable information provided by our expert contributors.

Wishing you all success in your cybersecurity endeavors,

Yan Ross

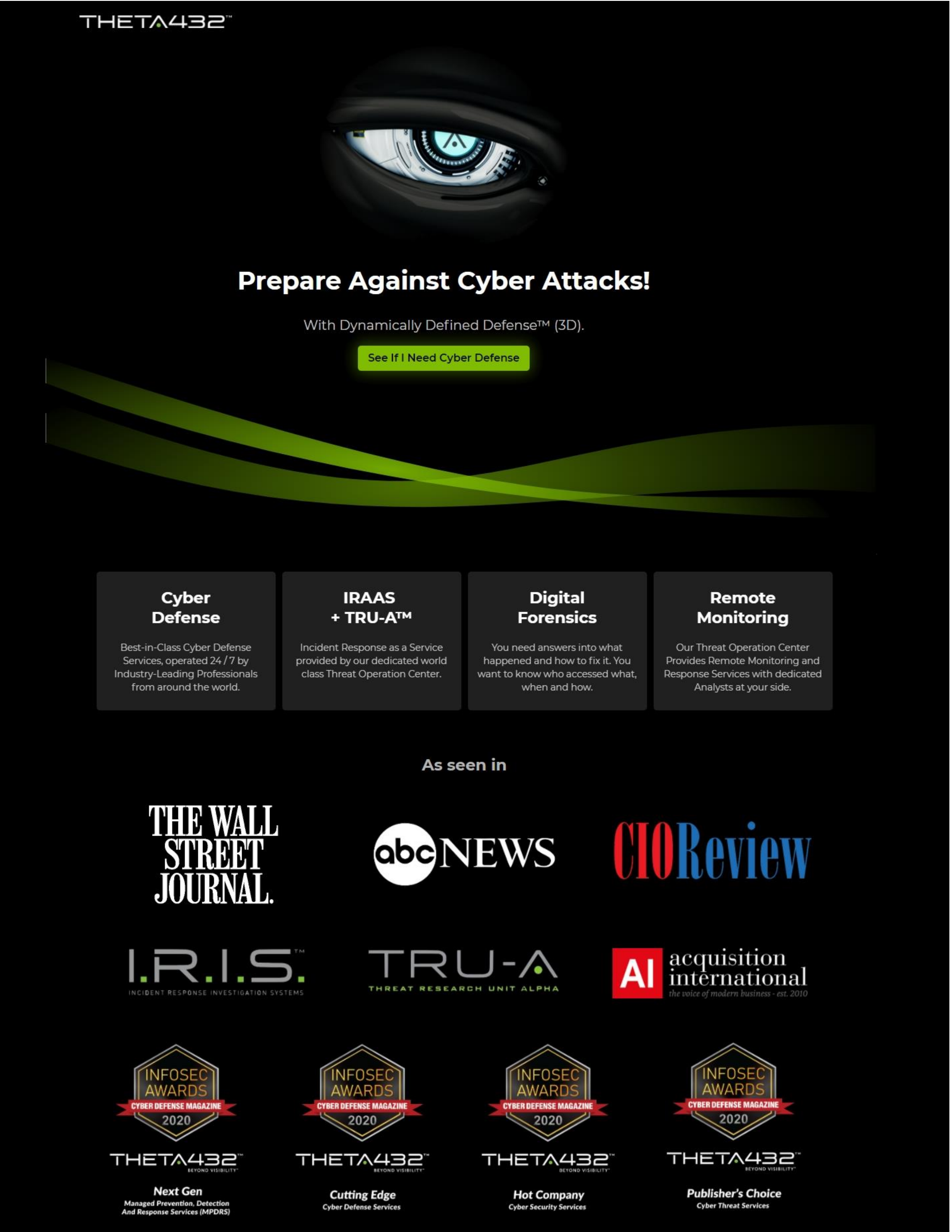
U.S. Editor-in-Chief

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



THETA432™

Prepare Against Cyber Attacks!

With Dynamically Defined Defense™ (3D).

See If I Need Cyber Defense

Cyber Defense

Best-in-Class Cyber Defense Services, operated 24 / 7 by Industry-Leading Professionals from around the world.

IRAAS + TRU-A™

Incident Response as a Service provided by our dedicated world class Threat Operation Center.

Digital Forensics

You need answers into what happened and how to fix it. You want to know who accessed what, when and how.

Remote Monitoring

Our Threat Operation Center Provides Remote Monitoring and Response Services with dedicated Analysts at your side.

As seen in

THE WALL STREET JOURNAL.

abc NEWS

CIOReview

I.R.I.S.™ INCIDENT RESPONSE INVESTIGATION SYSTEMS

TRU-A THREAT RESEARCH UNIT ALPHA

AI acquisition international the voice of modern business · est. 2010

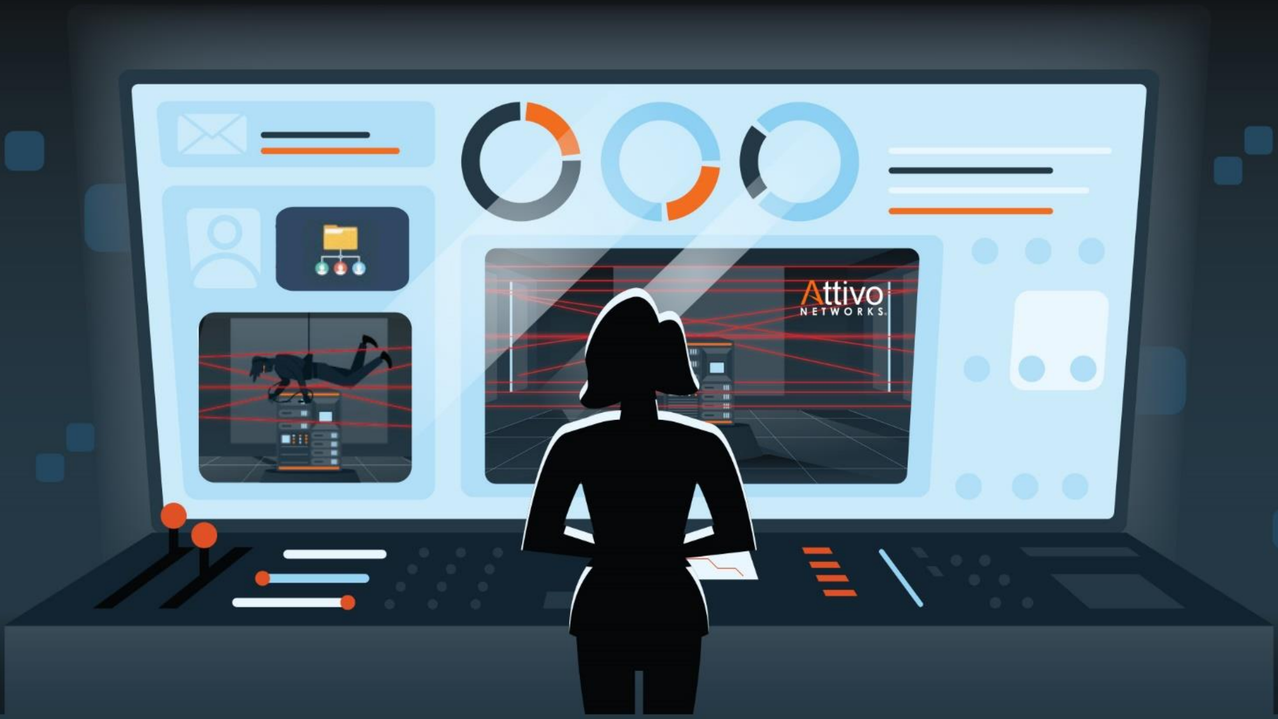
INFOSEC AWARDS CYBER DEFENSE MAGAZINE 2020
THETA432™ BEYOND VISIBILITY
Next Gen
Managed Prevention, Detection And Response Services (MPDRS)

INFOSEC AWARDS CYBER DEFENSE MAGAZINE 2020
THETA432™ BEYOND VISIBILITY
Cutting Edge
Cyber Defense Services

INFOSEC AWARDS CYBER DEFENSE MAGAZINE 2020
THETA432™ BEYOND VISIBILITY
Hot Company
Cyber Security Services

INFOSEC AWARDS CYBER DEFENSE MAGAZINE 2020
THETA432™ BEYOND VISIBILITY
Publisher's Choice
Cyber Threat Services

CONTINUOUS PEN TESTING FOR ACTIVE DIRECTORY



Is Your Active Directory Prepared for a Ransomware Attack?

Active Directory is the prime target for ransomware attackers. However, it is woefully unprotected. Attivo Networks disrupts these attacks with unprecedented visibility to exposures, vulnerabilities, and live attacks.

Over 200 Active Directory security checks show risks and detect attacks that lead to domain control for downloading malware, changing security settings, and establishing backdoors. Over 75% of assessments show multiple high-risk exposures. Are you ready? Get a free health check to see.

Attivo
NETWORKS®
attivonetworks.com

LET'S GET
STARTED!

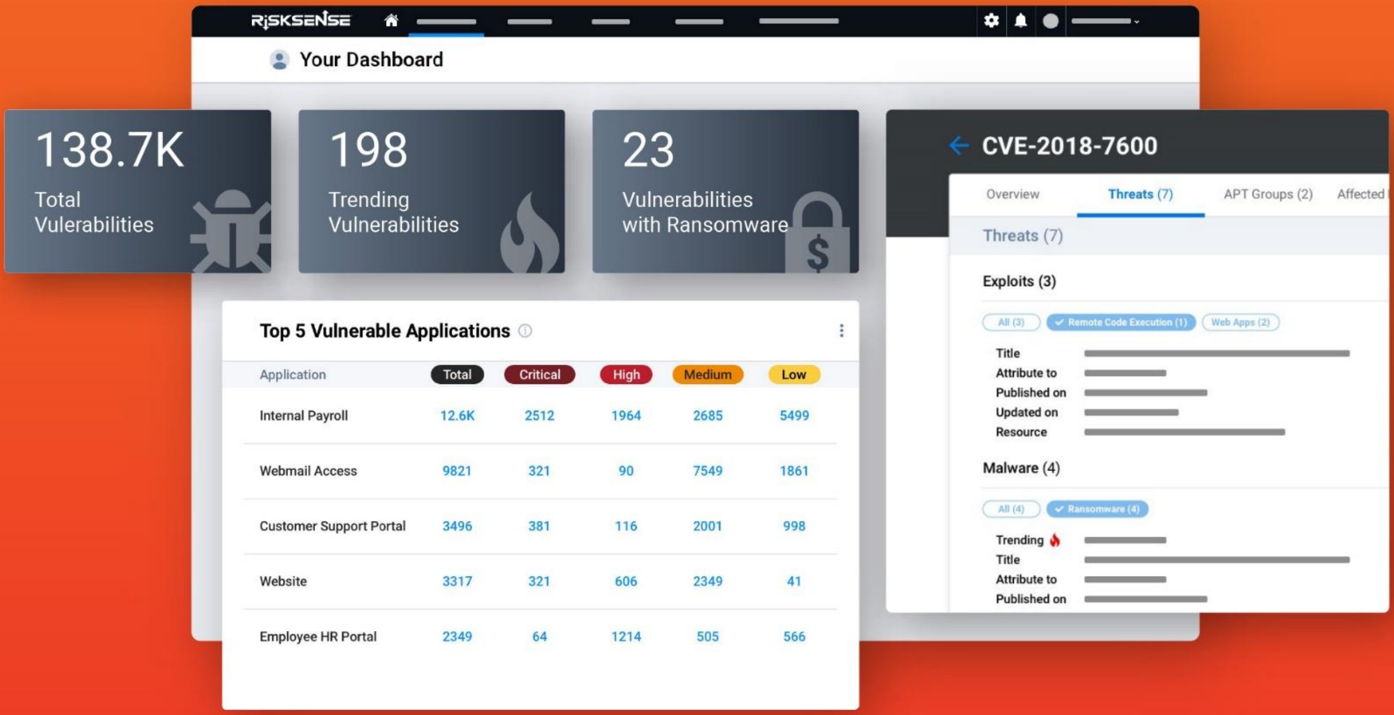
Your Fastest Response to Vulnerability Exposure

Full Spectrum Risk-Based Vulnerability Management

Vulnerability Intelligence
Active threats & ransomware

Vulnerability Prioritization
Clear directions for actions

Full-Stack Application Security
Code visiblity to risk



RISKSENSE

Your Dashboard

138.7K
Total Vulerabilities

198
Trending Vulnerabilities

23
Vulnerabilities with Ransomware

Top 5 Vulnerable Applications

Application	Total	Critical	High	Medium	Low
Internal Payroll	12.6K	2512	1964	2685	5499
Webmail Access	9821	321	90	7549	1861
Customer Support Portal	3496	381	116	2001	998
Website	3317	321	606	2349	41
Employee HR Portal	2349	64	1214	505	566

CVE-2018-7600

Threats (7)

Exploits (3)

Title
Attribute to
Published on
Updated on
Resource

Malware (4)

Trending 🔥
Title
Attribute to
Published on

Take a Proactive Stand Against Adversarial Risk

RISKSENSE®

www.risksense.com

axiad

Passwordless Anywhere with **SMARTidentity**

Secure digital interactions for users and machines to keep your business moving forward

axiad.com

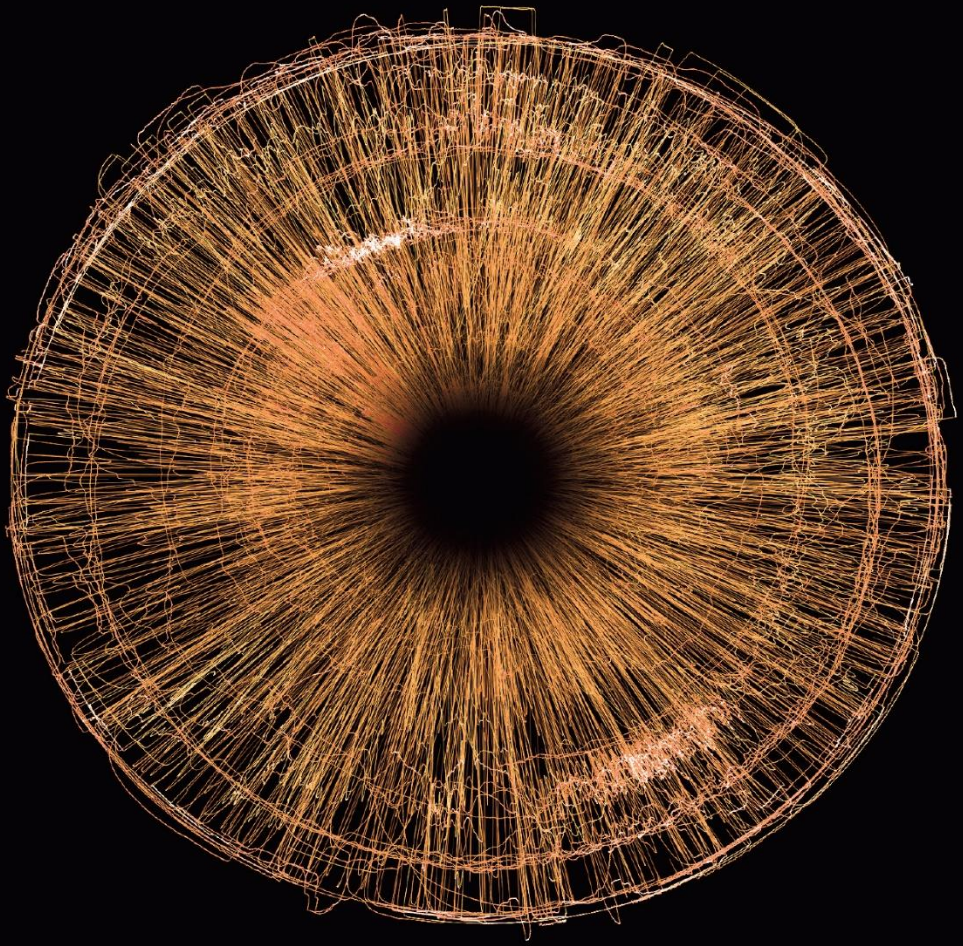
Three-key encryption, so you'll never have ransomware face ever again.
11 12
10
9
8
7 6

Things have changed. Difenda will help maximize your Microsoft security investments through technology consolidation and provide a modular approach to provide a clear view of your cybersecurity landscape through a single pane of glass.

See the difference a personalized approach to cybersecurity makes work with a partner thats focused on you.

DIFENDA

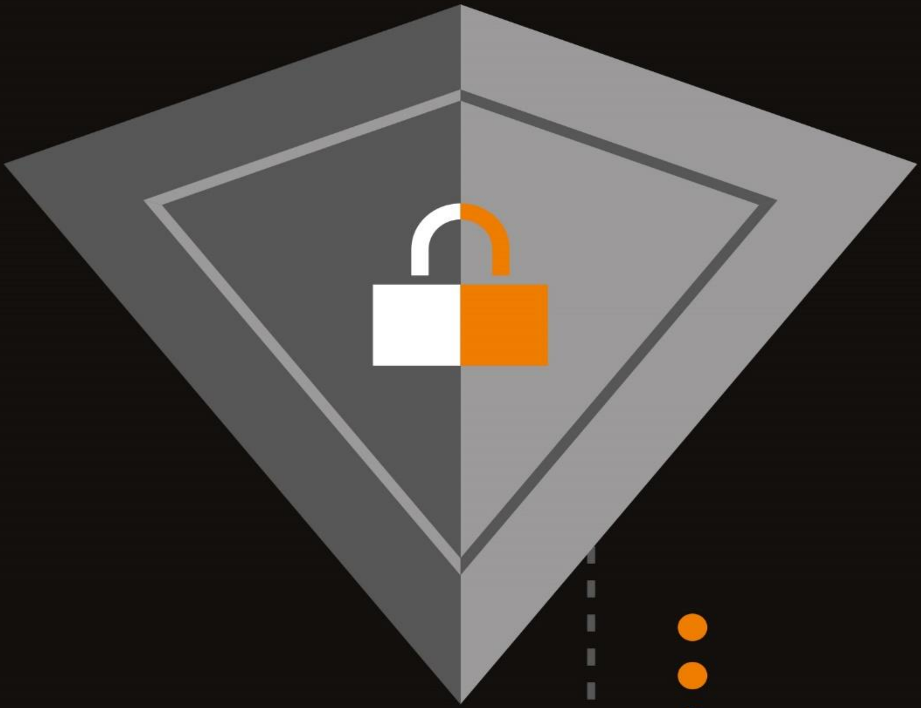
CONTACT A DIFENDA SECURITY EXPERT TODAY



A NEW WAY TO KEEP YOUR SECRETS SAFE

CONTACTLESS SECURE SHARING IN YOUR POCKET

www.freemindtronic.com



FOCUS ON YOUR BUSINESS, NOT YOUR EMPLOYEES' CYBER HABITS.

CYBERSECURITY DONE RIGHT.

FluencySecurity.com

Fluency®

Do you check the boxes with your cybersecurity?

☑ **Leadership Prioritizes Cybersecurity**

□ Assessments

□ Plans

□ Policies

□ Procedures

□ Training

□ Education

□ Testing

□ Scanning

□ Monitoring

□ Response

Antivirus

Protects devices against known infections

Firewalls

Protects networks against unauthorized access

DEFENDIFY®

Cybersecurity. *Simplified.*

Protects organizations against diverse threat landscape

What's Your Cybersecurity Strength?

A+ A A- B+ B B- [✓ C+] C C- D+ D D- F

Find out in 3 minutes

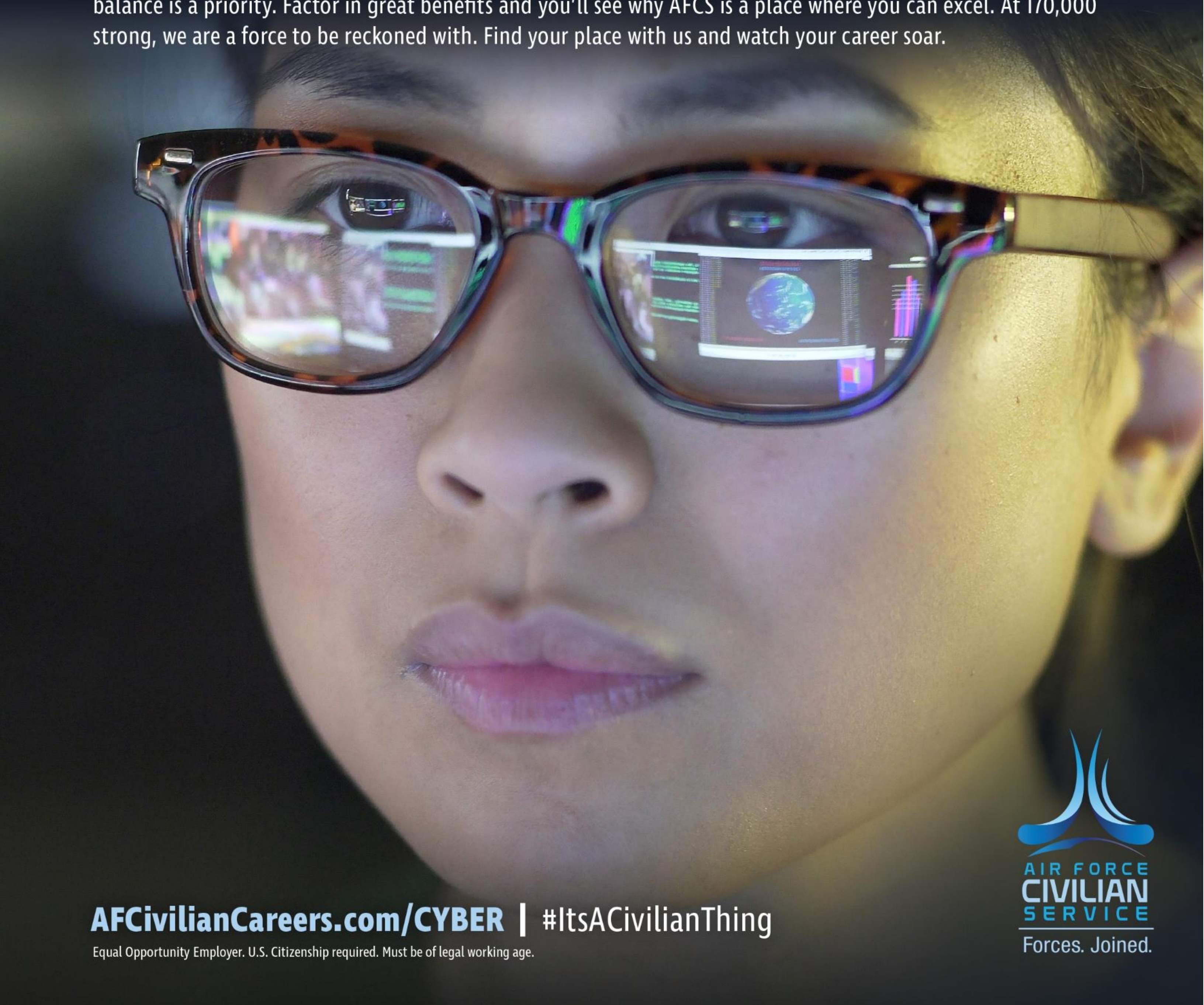
www.defendify.io/mygrade

WORK ON THE FRONT LINES PROTECTING AMERICAN INTERESTS

Air Force Civilian Service (AFCS) has hundreds of civilian cyber security and IT professionals working to safeguard Air Force facilities, vital intelligence, and digital assets. We're looking for the best and brightest to help us stay ahead of this ongoing threat.

In fact, AFCS is currently hiring cyber security specialists, information technology specialists, information security specialists, software developers, software engineers, computer scientists, and computer engineers. These are challenging and rewarding positions that put you at the heart of our mission in cyberspace. Our systems are some of the most complex in the world, and we need the best in the business to keep our infrastructure and digital information secure.

Consider AFCS. You'll nd a supportive and inclusive workplace, where excellence is rewarded, and work-life balance is a priority. Factor in great benefits and you'll see why AFCS is a place where you can excel. At 170,000 strong, we are a force to be reckoned with. Find your place with us and watch your career soar.

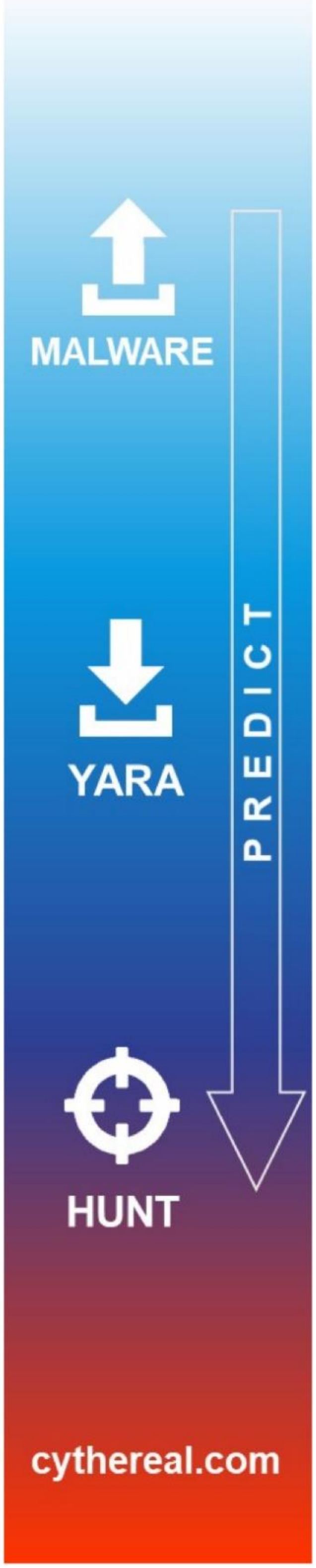


AFCivilianCareers.com/CYBER | #ItsACivilianThing

Equal Opportunity Employer. U.S. Citizenship required. Must be of legal working age.

AIR FORCE
CIVILIAN
SERVICE
Forces. Joined.

Predictive Cyber Defense



Lucio Frega, Threat Researcher
Deutsche Telekom - Cyber Threat Intelligence

DTAG-CTI (Deutsche Telekom - Cyber Threat Intelligence) protects clients against cyber-attacks worldwide.

Like us, the adversaries too have cyber-experts. They continuously enhance their malware attacks with stealth and anti-forensics capabilities. This increases our overall risk and also the cost of detection and remediation.

For example, repacked malware strains evade endpoint's protection, fluxed C2s bypass SIEM, and obfuscations fool reversing.

We can cope with this in spite of the high cost. However, it all amounts to nothing if, by the time a defense is erected, the attack has reshaped and shifted direction again, turning those defenses obsolete.

We in DTAG-CTI have erected predictive defenses using malware's code-similarity.

This predictive layer goes beyond network activity, behavior, metadata and state-of-the-art technologies. We match binaries using Cythereal's automatically generated YARA rules, unearthing previously unseen strains despite reshuffling, repacking, and other evasions. These predictive defenses nail the malware "in the bud," before it has had a chance to spread or even to report to its C2.

As an extra value, these early detections also empower early identification. We learn from the start who is against us and hunt for associations regardless of their obfuscated binaries, dissimilar metadata, IOCs, and payloads.

Together with the professionalism and commitment of our teams and partners, we have found in the expertise, dedication, and engagement of Cythereal a very powerful and astounding ally that brings threat hunting and cyber-defense to a superior level.

About the Author/Disclosure

Lucio Frega is a computer forensic examiner certified by IACIS (International Association of Computer Investigative Specialists). He has over 40 years of worldwide experience in IT/OT security in Banks, Pharma, Telcos and the energy sector. Lucio is not affiliated with Cythereal. His comments are not to be construed as the official posture of any stakeholder but himself.

Stony Lonesome Group

MISSION FOCUSED INVESTING

EST 2011

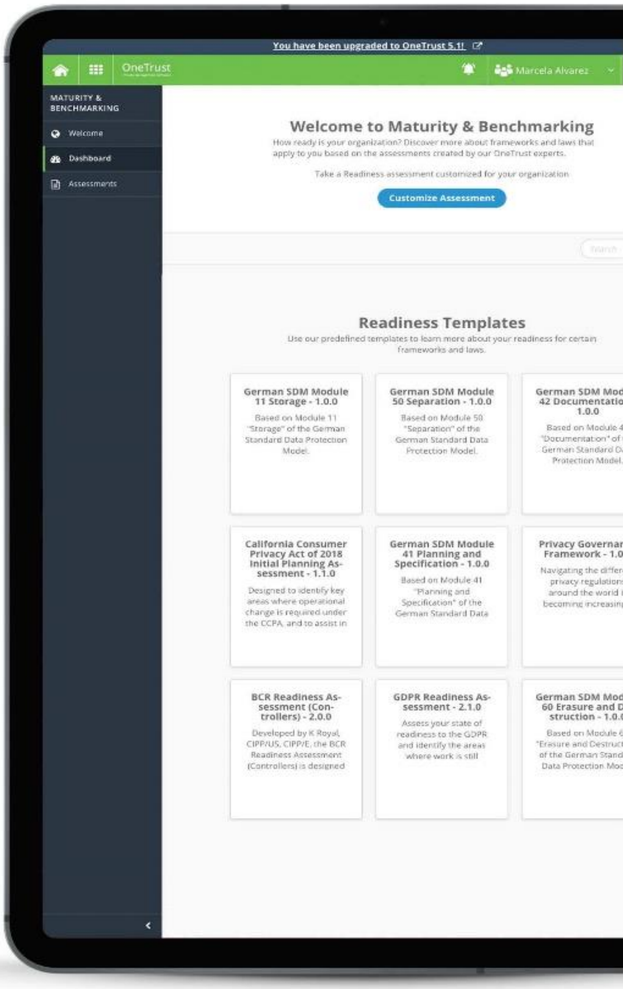
Founder & Managing Partner

SEAN DRAKE

***"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. "*

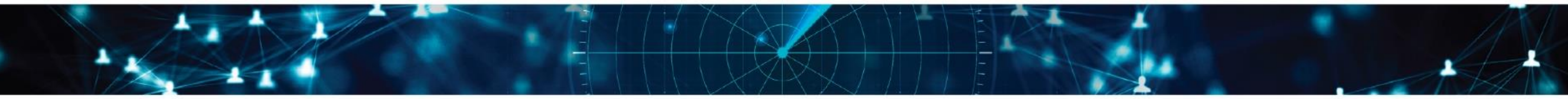
Sean Drake
Managing Partner
Stony Lonesome Group LLC
203-247-2479 ☎
www.stonylonesomegroupllc.com 🌐

cisco
Networking Academy



You have been upgraded to OneTrust 5.1!
OneTrust
Marcela Alvarez
MATURITY & BENCHMARKING
Welcome
Dashboard
Assessments
Customize Assessment
Search

STRATEGIC
COMMUNICATIONS



ARTICLES

Understanding The Importance of Designing for Security

By Camille Morhardt, Director of Security Initiatives and Communications at Intel, and Tom Garrison, VP and GM of Client Security Strategy and Initiatives at Intel

Robust security is a necessary and critical component of achieving a high-quality product. This is obvious when we consider security in a home or safety in a car or an airplane. And it's the same with computing devices. From the initial architecture formation through the device build process to ongoing product service and retirement, how companies embrace security best practices in their designs and how they follow through over the device's lifespan to keep it safe can significantly impact partners and customers.

What does it mean to "design for security" in today's digital and increasingly connected world? Let's go over six questions that can help illuminate the importance of designing for security and highlight the critical steps along the way.

1. Where should you start?

The best way to achieve good security is to design it into the system or device from the very beginning, at the concept phase, then keep security at the forefront of product architects and engineers at every stage of development.

When designing a product, you need to think beyond what you are building your product to do and consider any use cases you might not have considered. For example, consider a server platform that is embedded into an MRI machine in a hospital. A data center is a very different environment than a hospital basement. You have to think holistically about your product and think through the security implications of unintended use cases down the road. Hackers use this philosophy, using devices in completely unexpected ways to uncover potential vulnerabilities. It's hard to imagine all the potential use cases for a particular device (or how bad actors might attack it), so you need to proactively think of security in layers, and design in defense in depth so that no single exploit is likely to be successful.

2. What's the first thing that needs to happen when creating a new product?

From an architecture standpoint, you have to think about how a device might come under attack. That could include hardware, firmware, OS, application, and connectivity types of attacks. Using a 'design for security' mindset, you must think about all these security attack scenarios because the weakest link breaks the chain. For example, when thinking about making airplanes safe, designers build in redundancy, so a single failure isn't likely to cause a crash. But they also consider passenger safety and how best to exit planes quickly. They have robust communications and procedures for what to do if communications are down and many, many other aspects that comprise a safer airplane trip. This same mindset exists in technology, with many security layers built into products from the beginning. An adversary will avoid heavily protected elements of a product and look for the easiest way to break the system.

This means threat modeling needs to be one of the first things to happen when building a product. You can threat model everything from environmental factors and natural disasters to global geopolitics, or you can narrow it down to something like a network or access to a system. It's about guarding against bad outcomes. Mature organizations often have teams of researchers dedicated to creating and evaluating threat models.

3. How do you prioritize security when designing and developing a new product?

Once you get into actual design and development, you want to be able to catch known security threats. That process is part of the Secure Development Lifecycle or SDL. SDL is a series of processes that implement security principles and privacy tenets into product development to help support engineers, developers, and researchers. These processes incorporate security-minded engineering and testing at the onset of product development when it's more effective and efficient to employ. Not only does it include knowledge sharing, but also tools and services that, for example, allow someone to run checks against code. You can imagine the number of checks over time becomes massive, so you need a process that's efficient and scales to help teams to better ensure they can catch security vulnerabilities.

Automation plays a vital role here. This involves using tools that embed these checks and automate the process so designers can run a multitude of complex security checks with a click of a button. Our teams are constantly working to stay ahead of attackers by trying to find these issues and vulnerabilities before an attacker can exploit them. Beyond the SDL, other initiatives play a major role around security, including training, conferences, Product Security Incident Response Teams (or PSIRTs), bug bounty programs, offensive and defensive research, and industry collaboration.

4. Is there some sort of final security check involved before a product goes to market?

There's no single security check, but rather the completion of a gauntlet of checks, that makes a product ready for market. Even early in the Intel development process, a product generally is required to meet appropriate security milestones at that development phase in order to proceed forward. At Intel, we don't just check for security at the end. It is an integral part of the entire development process. We have a team of more than 200 security researchers internally, and they work with the product teams collaboratively to evaluate the products throughout development.

Our teams work to find and mitigate potential vulnerabilities through internal code reviews, red team activities such as Hack-A-Thons, and other events before products go to market. The data we collect is then used to develop automation and required training to help eliminate future occurrences. We also partner with the external research community, which is full of extremely smart and creative people. We want them working with us, making our platforms better. Sometimes this is known as "Crowdsourced Security" and can include bug bounty programs which provide incentives to researchers to report vulnerabilities.

5. What happens if researchers identify a major vulnerability via bug bounty programs after the product is already in the field?

At a high level (and this can differ depending on the vulnerability), products with a vulnerability initially go to PSIRTs. At Intel, this team engages with the researcher that uncovered the issue and does the preliminary evaluation to validate and replicate the issue. Then very quickly, it's triaged with Intel experts for that specific platform area who drop everything to prioritize resolution of the issue. Finding and deploying mitigations for the issue could take days, weeks, or months, depending on the complexity. In the meantime, because Intel follows the common industry practice of Coordinated Vulnerability Disclosure (CVD) for reported security vulnerabilities on launched products, we align with the researchers on a date to publicly disclose the issue to allow time to identify and deploy mitigations, in order to reduce adversary advantage.

Then once we have a mitigation, we need to help ensure that mitigation doesn't create other unintended problems. Before rolling it out into customer environments, we need to make sure we understand the full extent of its potential impact. First, internally we do what's called 'no harm testing'. Later, we do more robust testing with partners and then roll out the update to customers in a coordinated fashion. When possible, we bundle updates together so they can be validated together to save time and money for the customers. In addition to practicing inbound CVD in partnership with external security researchers, Intel also coordinates outbound vulnerability disclosure with industry partners and other external stakeholders, as appropriate, so that all affected parties are disclosing in unison for an optimal defensive position. It's all about coordinated disclosure.

6. What role does working with the larger hardware community play in designing for security?

Compute is a complex endeavor that involves hardware from multiple vendors, firmware, operating systems, and applications. And of course, if your hardware goes online, which more and more of it does with the expansion of the Internet of Things, you must strive to secure compute systems across entire ecosystems. We're really in an interesting time now. With so many connected and smart systems, we must consider security and privacy in every design decision for every product we create. These topics require broad discussion and collaboration, and they deserve our detailed attention to ethical considerations.

And where we are as an industry is far from consensus on these critical considerations: not every company designs for security or maintains a basic framework for how to update their products to stay safer from attackers. There's no real unanimity across the industry in terms of what holistic security looks like. And those are things that customers really care about. We at Intel, together with our partners in the technology market, have the opportunity to demonstrate what more comprehensive security means. We are leading by example, inviting others to follow, and educating customers that we all should demand more from technology suppliers, which raises the security bar for ourselves and the industry because so much of the world depends on technology.

Designing for security is critical for any organization producing technology products and services today. If you haven't already, consider the above questions and move to a security by design mindset to help ensure your organization can deliver safer, more reliable products that earn trust within the market.

About the Authors

Camille Morhardt – Director of Security Initiatives and Communications at Intel

Tom Garrison – VP and GM of Client Security Strategy and Initiatives at Intel

Evaluating Security Practices in Response to Colonial Pipeline And South Korean KAERI Attacks

Zero Trust and Enforcing the Principle of Least Privilege Have Become Crucially Important.

By Garret Grajek, CEO, YouAttest

In recent news, we have seen several high-profile attacks on major institutions in the United States and abroad. In early May of this year, the Colonial Pipeline in the United States was attacked and late last month it was reported that a North Korean hacking group, Kimsuky, breached the network of the Korea Atomic Energy Research Institute (KAERI) on May 14th. KAERI was established in 1959 to achieve self-reliance in nuclear core technologies and has since achieved that goal, making it a prime target for an energy-starved North Korea. In the wake of these attacks, we must reflect on the strengths and vulnerabilities of our cybersecurity mitigation attempts and look to bolster those efforts.

In the case of the South Korean attack, if the North Korean espionage group successfully exfiltrated information, it is believed this could be the largest security breach in South Korea since the attack on the defense ministry in 2016. The group could have gained access to information that would benefit the nuclear programs in North Korea, as KAERI has information on small modular reactors and other power sources. This is especially powerful information for North Korea, as only 26% of their population has access to electricity.

Kimsuky, according to United States officials, is likely tasked by North Korea with a global intelligence-gathering mission. This attack is not the first attack Kimsuky has launched at South Korean infrastructures, as they succeeded in attacking Korea Hydro & Nuclear Power Co. Ltd back in 2014. The group has also been attributed several other attacks on South Korea using a backdoor called AppleSeed for Windows and Android systems.

In response to the claims about the attack, KAERI issued a statement explaining that an unidentified outsider accessed parts of its systems, exploiting a weakness in their virtual private network (VPN). Regarding the attack, they blocked the IP address and updated their security after the attack was discovered on May 31st. The damage from this hack is not yet known.

Incidents like this highlight to the world that critical infrastructure components can be vulnerable to cyberattacks. In response, we need to ensure that the organization’s security objectives are clear and met. The focus of compliance should not be just meeting it but having real security objectives to prevent future attacks.

It is the standard procedure for companies adhering to a certain compliance level to check their networks daily for vulnerabilities. Such practices are in place because we assume that there could be a malicious actor looking to exploit any vulnerability and open our systems. For vital infrastructures such as water and energy enterprises in the United States and abroad, we need to examine our identity privilege and adherence to the Principle of Least Privilege since it is the industry’s best practice to stop the damage from hacks.

When we look at the Principle of Least Privilege, we can see the advantages of ensuring that users, systems, and processes only have access to resources they need to perform their function inside an organization. Combining PoLP with zero trust - especially around network segmenting - can help deliver the desired level of network security. Limiting the reach of any one network user by governing their access makes it more difficult for attacks such as the Colonial Pipeline and KAERI to occur. Limiting the ability of one user account to affect the whole network limits the effect a malicious actor can have on your network.

By auditing the systems in place to determine the minimum privilege necessary for any user, system, and process, organizations can implement the Principle of Least Privilege to each entity. Start by examining the organization’s protocols from the perspective of an attacker to determine points of interest most likely to be exploited. What privileges have we granted remote users? What access levels have they been granted? How much damage can a rogue user do if they have access to that account?

After answering these questions and enhancing the networks with segmentation, implementing zero trust, and then enforcing the Principle of Least Privilege, organizations can lower the risk of significant attacks. It is crucial to monitor these privileges to insure a secure network for the enterprise.

About the Author

Garret Grajek, CISSP, CEH is CEO of YouAttest. YouAttest is a cloud based IGA tool that automates both periodic and dynamically triggered access reviews for compliance and identity security. Garret can be reached online at ggrajek@youattest.com and at https://youattest.com/

Chinese Government Will Begin to Stockpile Zero-Days in September

By Randy Reiter CEO of Don’t Be Breached

July 2021 has Been A Busy Month in Cyber Security

The Associated Press published on Tuesday, July 13, 2021 that on September 1, 2021 a new law in China requires all Chinese citizens finding a Zero-Day Vulnerability to provide within **48 hours** the details to the Chinese government. A Chinese citizen must **NOT** give or sell the information to third parties outside of China (apart from the product's manufacturer).

Other Data Breach and Ransomware July 2021 News

- **Microsoft** reported that a **SolarWinds** Serv-U Zero-Day (not related to Solarwinds December 2020 Supernova attack) was exploited by a Chinese Hacking Group. The Hackers were detected targeting US defense industrial base organizations and software firms. The Zero-Day allows Hackers to remotely run code with **SYSTEM PRIVILEGES**, allowing them to perform actions like install and run malicious payloads, or view and **CHANGE** data.

- **Microsoft** released patches for three Windows operating system Zero-Day vulnerabilities that were already being exploited by Hackers. The vulnerabilities included Windows **SYSTEM PRIVILEGE** escalation issues, scripting engine memory corruption bug and drive-by attacks via web browsers.

- **Microsoft** releases a security update for Windows Print Spooler vulnerability that allows a Hacker to install programs; **VIEW**, **CHANGE**, or **DELETE** data; or create new accounts with full user rights.

- **Palo Alto Networks** addressed vulnerabilities that could allow an attacker to execute arbitrary JavaScript code in the web console or to execute programs with **SYSTEM PRIVILEGES**.

- **SQL injection** vulnerability in the **WooCommerce** plugin affected more than 5 million WordPress websites.

- Healthcare **DATA BREACHES** spiked 185% in 2021. The Healthcare sector will remain a prime target throughout 2021.

- **Morgan Stanley** disclosed a July, 2021 DATA BREACH where Hackers stole customer data such as **customer name, address, birth date, Social Security number**, and corporate company name. The data compromised did not include passwords that could be used to access financial accounts. Morgan Stanley said the compromised files were **encrypted**; however, attackers were able to obtain the **decryption key** during the data breach.

Zero-Day Vulnerabilities that allow Hackers to operate with 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 the Theft of Confidential Database Data

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

Non-intrusive network sniffing technology can perform a real-time full packet capture and **deep packet inspection** (**DPI**) of 100% the database query and SQL activity in real-time from a network tap or proxy server with no impact on the database server. This SQL activity is very predictable. Database servers servicing 1,000 to 10,000 end-users typically process daily 2,000 to 10,000 unique query or SQL commands that run millions of times a day. SQL packet sniffing 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 **protection** of **confidential** database data.

In 2020 the DHS, Department of State, U.S. Marine Corps and the Missile Defense Agency all issued requests for proposals (RFP) for **network full packet data capture** for deep packet analysis or deep packet inspection analysis (**DPI**) of network traffic. This is an important step forward protecting confidential database data and organization information.

Advanced SQL Behavioral Analysis of Database SQL Activity Prevents 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 identified. This approach is inexpensive to setup, has a low cost of operation and low disk space usage. 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 database session terminated so that confidential database data is **NOT** stolen, ransomed or sold on the Dark Web.

Advanced SQL Behavioral Analysis of the query activity can go even further and learn the maximum amount of data queried plus the IP addresses all queries were submitted from for each of the 2,000 to 10,000 unique SQL queries that run on a database server.

This type of **Data Breach Prevention** can detect never before observed Hacker database query activity, queries sent from a never observed IP address and queries sending more data to an IP address than the respective query has ever sent before. This allows real-time detection of Hackers, Rogue Insiders and Supply Chain Attacks attempting to steal **confidential database data**. Now an embarrassing and costly Data Breach may be prevented.

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 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.

Four Ways Smart Cities Can Stay Safe in An Interconnected World

Mitigating the risks of cyber threats through cyber intelligence and frontier technologies

By Ritesh Kumar, Chairman & CEO, CYFIRMA

Smart cities bring about an abundance of benefits for a nation – a more liveable space for citizens, a thriving business environment, and greater economic growth. It is therefore no surprise that world leaders and nations are focused on developing critical infrastructure and rolling out technologies to build up their own smart cities.

However, with the increased connectivity and interconnectivity of smart systems comes greater risks and opportunities for threat actors to attack and take down critical systems and services swiftly.

One example of such cyber threats is ransomware, which smart cities are particularly vulnerable to. The interconnectivity of smart systems creates more openings for cybercriminals to launch attacks, and self-propagating malware can easily take down these key systems rapidly and lead to breakdowns of critical services, affecting the lives of citizens.

Just a few months back, the ransomware attack on the Colonial Pipeline in the United States affected nearly half of the east coast’s fuel supply. We have also detected multiple ransomware attacks on government and utility organizations recently, such as a hit on renewable energies and multi-source electricity producer Voltalia which resulted in a large amount of business-critical and sensitive data being exfiltrated, as well as a potential data leak of personal identifiable information (PII) from an Indian database that is suspected to be government-related.

These incidents serve as a cautionary tale and hammers home the importance of having a clear, effective cyber defense strategy. As government leaders continue in their missions to build up smart cities, they need to proactively mitigate the risks of cyber threats through the following four considerations.

#1 Leverage cyber intelligence to stay ahead of the game

Staying one step ahead of cyberattacks requires a thorough understanding of knowing where to look, who the threat actors are, what they are after, when they are planning to launch an attack and how they intend to do so. Smart city cyber-defenders need to be proactive to gain a pre-emptive advantage. Often, this means looking into the deepest, darkest corners on the Internet. Over 94 percent of the world's information resides in the deep and dark webs, which are frequented by cyber-threat actors trading restricted information ranging from academic and research data, to financial and medical records.

To minimise the fear of data breaches and cyber threats, smart cities must adopt an intelligence-centric mindset and leverage deep technology to monitor these platforms. Predictive detection capabilities help remove the element of surprise from these cyberattacks, allowing cybersecurity agencies to take actions swiftly and prevent data exfiltration and loss.

#2 Fight AI-powered attacks with AI-powered self-defense systems

Similar to how our immune system continuously self-monitors, learns and heals when faced with anomalies, the next frontier of cybersecurity solutions should have the ability to identify abnormal foreign activities or programs through adaptive machine learning.

An automated, self-defense cybersecurity system powered by AI and predictive analytical technologies will be able to define normal and abnormal statuses, monitor the system 24/7, and respond to and recover from new threats. Having such a system will reduce the risk of attacks significantly and reduce the attractiveness of being a hacking target for threat actors.

#3 Rethink the regulatory environment for cybersecurity

While governments have enacted cyber laws, the reality is that is can be difficult to enforce. There are a few areas within the circle of influence where improvements can be made and scaled.

For a start, incident reporting can be made mandatory and this will generate a body of research data that can provide insights on threats to the nation, and inform the government on strategies it can undertake to strengthen its cyber posture. Imposing mandatory risk and vulnerability assessments also helps governments identify threats early and conduct remediations to close any cybersecurity gaps. Commencing attack vector assessments can help uncover new attack surfaces as businesses adopt new digital formats and services.

Beyond that, nations can cultivate a cyber reward culture where the discovery of bugs and vulnerabilities are rewarded, providing an incentive for the cybersecurity community to share their knowledge and promote joint solutioning. For example, Singapore conducts its Government Bug Bounty Programme where ethical hackers are rewarded with a monetary bonus for discovering online vulnerabilities.

#4 Adopt a people, technology, process and governance framework

As much as cybersecurity is a technology problem, it cannot be ignored that humans are part of the equation contributing to it. Cyber hygiene needs to be emphasised and practiced religiously. Employees and individuals need to be educated on cyber threats and risks, given the prevalence of phishing attacks and social engineering hacking campaigns.

From the technology perspective, the public and private sector should incorporate layered defenses with data and endpoint security, gateway-based security, automating scanning, monitoring and malware removal. Antivirus solutions, data loss detection and protection, and VPN solutions must not be overlooked. With processes, cybersecurity teams should conduct threat profiling, creation of threat segmentation, zoning and risk containerization. Having a habit of backing data daily would be a good policy to adopt too. Finally, when it comes to governance, a good cyber threat visibility and intelligence programme will be vital in completing a well-rounded cybersecurity strategy.

Ultimately, the increasing connectivity of our world means that the possibility of cyber threats will always be present. However, it is clear that the potential economic and social benefits that smart cities can bring to the table outweigh the risks, and nations should not be dissuaded from their smart city plans. Through gaining accurate intelligence of where external threats lie, understanding them and implementing effective cybersecurity measures, cities will become not just smarter, but safer as well.

About the Author

Kumar Ritesh is the Chairman & CEO of CYFIRMA. He has 2+ decades of global cybersecurity leadership experience across all facets of the cybersecurity industry.

Ritesh spent the first half of his career as the head of a cyber-intelligence agency, gaining first-hand cyber threats and risks insights on a global scale before transiting into the commercial arena as a senior executive for multi-national corporations such as IBM and PwC. Ritesh was also the global cybersecurity leader for one of the world’s largest mining companies, BHP Billiton.

A highly dynamic executive who successfully blends technology expertise with business acumen, Ritesh has a strong track record of developing successful cybersecurity strategies, products, policies, standards, and solutions, in addition to running complex cybersecurity programs.

He has developed prototypes for data loss prevention, social profile risk assessment, web content assessment management, intelligence-led cyber risk management, and adaptive cyberthreat intelligence tools. The co-inventor of two patented technologies for phishing fraud detection and protocol-aware PCB architectures, he is PMP, CISSP, CISM, CISSP-ISSAP, TOGAF 9.1, CIPM, and CIPT certified.

Through his blogs and public speaking engagements, Kumar educates companies on cyber security risks, solutions and trends.

Ritesh can be reached online through LinkedIn and at our company website https://www.cyfirma.com/

The Interplay Between Cyberattacks and Psychology

How do cybercriminals think? And how should that affect cybersecurity?

By Martin Banks

Cybersecurity is a complicated field. Cybercriminals are creative, and breaches can come from anywhere, from complex technical exploits to the curiosity of unwitting employees. Robust cybersecurity must account for all these different attack vectors, yet many strategies fail to account for everything.

Many would agree that cybersecurity is a matter of technical considerations, chiefly an IT issue. While this is true, it doesn't cover the full extent of cybersecurity. As with any other type of crime, psychology plays a significant role in cybercrime, yet cybersecurity protocols often overlook this area.

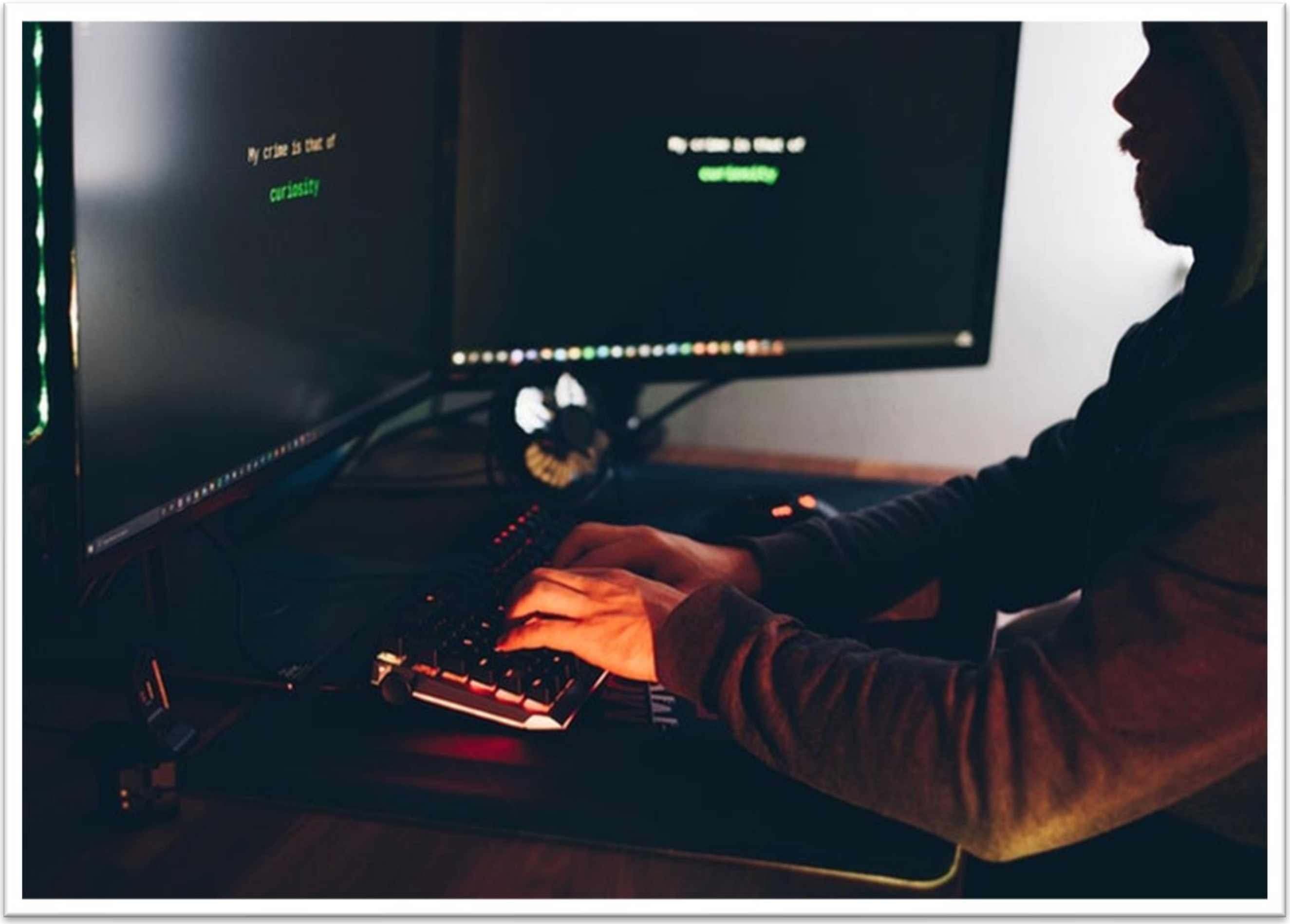
Nobody does anything without reason, and human minds are the last line of defense in any system. With that in mind, here's a closer look at the interplay between cyberattacks and psychology.

The Psychology of a Cybercriminal

Most cybersecurity professionals are already aware that they should understand their enemies to defend against them. The popularity and success of penetration testing are a testament to this line of thinking. Security teams should take it a step further, though, applying it to motives, not just methods.

According to Verizon's 2021 Data Breach Investigations Report, 93% of data breaches are financially motivated. While that accounts for most cases, it doesn't cover all motivations. It's also a broad category and doesn't provide much insight into the perpetrators behind these attacks.

Cybersecurity professionals need to look deeper into what drives the criminals they face. Understanding why someone would attempt to infiltrate a system can help guide appropriate responses. While the specifics can vary, cybercriminal motivations typically fall into one of five categories: money, frustration, hacktivism, state-sponsored attacks and fun.



Money

Similar to other types of crime, money is by far the most common motivator for cybercriminals. As data becomes more valuable to businesses, it represents an increasingly substantial payday for hackers. In 2020, the average data breach cost $3.86 million, and in some industries, that figure's as high as $7.13 million.

A cybercriminal can take multiple paths to a financially motivated attack. Typically, the most lucrative are ransomware and intellectual property theft. These often coincide, with hackers demanding a ransom for trade secrets else they sell them on the dark web. Consequently, companies with more sensitive data should focus on defending against these types of attacks.

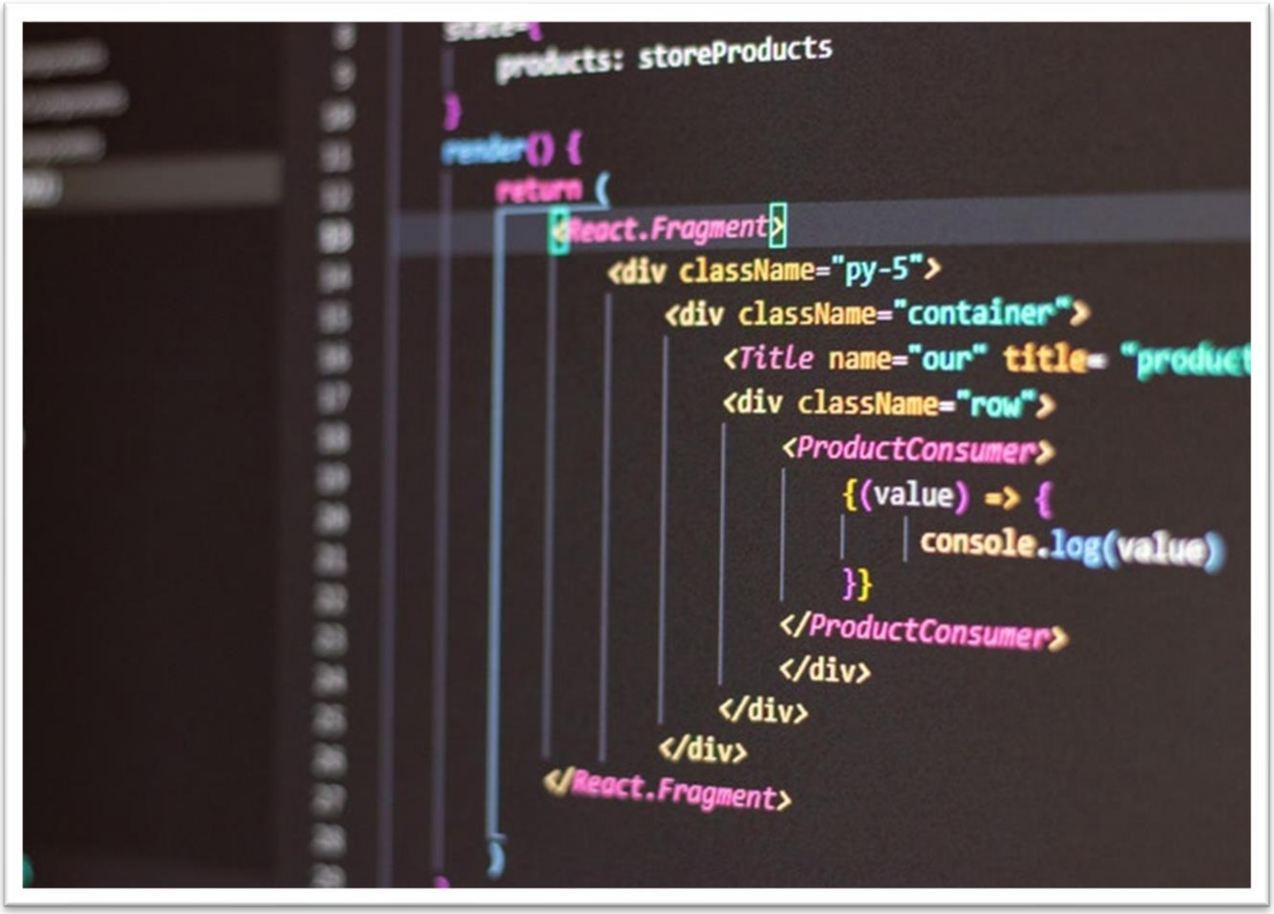
Since money is such a common motivator, businesses should take inventory of their most valuable data. Whatever has the most monetary value if lost, stolen or sold should receive the most protection. Personal identifiers, insider secrets and financial information typically fall into this category.

Frustration

While money is the most popular motivator, it's far from the only one. Some cybercriminals work out of anger and frustration against a company or industry. These criminals could be disgruntled employees or customers who feel a business treated them poorly, but they share a common goal. They want revenge.

Frustrated cybercriminals may seek to get money out of an attack, but they want to cause disruption more than anything. If they're a company insider, this is troubling since they'd have easier access to cause more damage. Regardless of where they come from, the best way to protect against these types of attacks is to prevent them in the first place.

Treating employees and customers well will go a long way. Companies should also listen to people, asking for client feedback and talking with workers. These discussions can help assuage would-be cybercriminals' anger and reveal if someone feels frustrated and may be a threat.



```
state={
  products: storeProducts
}
render() {
  return (
    <React.Fragment>
      <div className="py-5">
        <div className="container">
          <Title name="our" title= "product
          <div className="row">
            <ProductConsumer>
              {(value) => {
                console.log(value)
              }}
            </ProductConsumer>
          </div>
        </div>
      </div>
    </React.Fragment>
  )
```

Hacktivism

One often-overlooked cybercrime motivator is hacktivism, where cybercriminals launch attacks to make a social or political statement. Companies caught up in controversy or with strong ties to an unpopular political movement are common targets for hacktivists. These cybercriminals typically favor distributed denial-of-service (DDoS) attacks to disrupt operations or leak sensitive data.

Hacktivism seemed to fall off the radar in the past few years, but recent trends show it may be making a comeback. Anonymous, the most famous hacktivist collective, returned to prominence in 2020 during the Black Lives Matter protests. Around the same time, Twitter blocked a group called DDoSecrets, which had collected 270 gigabytes of internal police department records.

Like with frustrated cybercriminals, the key to defending against these attacks is prevention. As hacktivism regains popularity, companies should take care to steer clear of controversy. If they do get caught up in it, cybersecurity professionals should preemptively tighten their defenses in preparation.

State-Sponsored Actors

A similar but separate class of cybercriminals is state-sponsored actors. As governments around the globe rely more heavily on digital technologies, cyberattacks have emerged as a new type of warfare. Enemy nation-states can employ hackers to cripple critical infrastructure, spread misinformation or uncover government secrets.

State-sponsored cyberattacks may seem like something out of sci-fi, but they're already a reality and are becoming more common. In May, North Korean hackers ran a phishing campaign against South Korean government officials to steal confidential information. Many experts also suspect that the cybercriminals behind the massive SolarWinds attack were operating under the Russian intelligence service.

Government organizations and contractors, as well as critical infrastructure, are the most at-risk of these attacks. Cybercriminals typically use sophisticated techniques, so these operations should adopt high standards. Tight restrictions like zero-trust security models and vetting all business partners are ideal. Continuous monitoring is also a good idea since cyber espionage campaigns aim to be as stealthy as possible and could otherwise slip past defenses.

Fun and Notoriety

Not all cybercriminals are after something significant, be it money or making a statement. As hacking has risen in prominence, some people have started doing it simply for the fun of it. For these cybercriminals, infiltrating a system is about the challenge, about accomplishing something they can impress other hackers with.

Studies show that the brain's reward systems can react similarly to internet use as they do to drugs. This phenomenon is the driver behind internet addiction, and it likely plays into this type of cybercrime, too. For some people, a successful hack gives them a sort of high that they'll keep chasing.

As technology addictions rise, this type of cybercrime will likely grow, too. Unfortunately, given its lack of a clear goal, it's often unpredictable. While these attacks typically don't cause much damage, they're near-impossible to predict but highlight the importance of constant vigilance.

The Psychology of Cyberattack Victims

Understanding the psychological profile of cybercriminals isn't the only way psychology plays into cybersecurity. Security professionals must also understand the minds and motivations of those they're protecting. That's because the most successful cyberattacks are often those that take advantage of their victims' psychology.

A 2019 study revealed that 91% of enterprise data breach victims said that social engineering was part of the attack. To help patch these behavioral vulnerabilities, companies need to understand why employees behave the way they do.

Ignorance is a significant factor behind these attacks. Providing thorough training for all employees is crucial, but complacency is just as prevalent and dangerous. If workers don't see security as a relevant issue to them, they won't bother engaging in best practices. People tend to prefer convenience over security.

Cybersecurity training should communicate how breaches affect employees on a personal level. No amount of exercise will eliminate all complacency, though. Since people will always make lapses in judgment, cybersecurity professionals should anticipate this and prepare accordingly.

Companies should review who has the most potential for damage, which is often whoever has access to the most sensitive information. These workers should receive the most attention, be that in monitoring, extra training or tighter access controls. Keeping an eye on how employee behavior shifts is also crucial to preventing psychology-based attacks.

Thorough Cybersecurity Considers Psychology

The best cybersecurity strategies cover more than just technical considerations. Psychology, both in cybercriminals and their victims, drives cybercrime, so it should be at the center of cybersecurity too. When security teams understand how their attackers and clients think and behave, they can act more effectively.

About the Author

Martin Banks is the founder and Editor-in-Chief of Modded. You can find his writing all over the internet. He covers tech, gear, cars, and more.

Cyber Risk Protection Checklist

Managing Cyber Risks Against Your Business

By Jeff Severino, CyberLock Defense, Lockton Affinity

With the threat of cyber attacks increasing, it's more important than ever to protect your business. Many attacks result from a business being unprepared or underprepared for the threat. By taking proper action, you can significantly minimize your risk.

Manage the risk your business faces by implementing these cyber risk protection tips:

1. Antivirus and Firewall Protection

Antivirus and firewall tools protect your business the way a burglar alarm and sturdy structure protect a home. These systems work to keep cyber attacks from penetrating business systems, sounding the alarm if an attack does get through.

In today's business world, it's important to protect not only critical end-points, but central systems as well.

Use antivirus protection to protect against computer viruses and malware:

- Administrators should run regular antivirus scans on the entire system, not just your workstations.
- Whether your servers are onsite or in the cloud, they should also be subject to regular scans.

For firewalls, proper configuration is critical:

- Research suggests up to 99% of firewall breaches are caused by simple errors in configuration.
- For your firewall, an internal system modem is like a hole in the side of your house, so ensure this risk is eliminated with a systems audit.
- Configuration of both endpoint and internal firewall architecture can protect against other threats, like compromised laptops and USB drives.

- Regularly check and update your firewall configuration settings to ensure complete protection and efficient performance.

2. Network Password Protocols

Passwords are like the key to your home. Just like you wouldn’t leave your house key lying around, don’t be careless with your company’s password management. Try these tips:

- As many as 81% of business data breaches are due to poor password protocol, so it's important to effectively manage this risk.
- Strong passwords, of 8-12 characters and containing a combination of uppercase and lowercase letters, numbers and symbols, can go a long way toward minimizing the risk of a cyber attack.
- Don’t allow weak passwords, such as "12345" or "password1" and words from the dictionary or patterns of numbers or symbols.
- Always require the use of different passwords for each account and service. A trustworthy password manager can be utilized if needed.
- Enforce strong password safety measures on company mobile devices and laptops.
- Incorporate rolling updates to prompt users to change passwords either monthly or quarterly.
- Also update relevant passwords when a personnel change occurs.
- Require multi-factor authentication to provide two or more levels of security.

3. Patching and Updates Maintenance

Patching and updates maintenance is an incredibly important part of your cyber risk protection. New vulnerabilities in software files and systems may be discovered regularly. Patches published to fix the bugs can occur as often as once a day, so managing this process is key:

- Conduct a comprehensive inventory of devices, OS versions and applications. Forgotten systems and devices can lead to neglected updates and the risk of a successful attack.
- Determine how often critical services are patched and updated and look for ways to minimize risk from unpatched vulnerabilities.
- Monitor for new patches and vulnerabilities, and ensure a process is in place for testing, configuring and rolling out fixes.
- Audit your patches to ensure your administrators are aware of any failed or pending patches that may be critical.

4. Phishing Awareness Training

Many workers know they should avoid a suspicious email but spotting today's most common phishing tactics is getting more difficult.

Recent tricks include:

- Send an invoice
- Request a password reset
- Request to update payment info
- Prompt to click a download link

- Impersonating or compromising the credentials of a boss or VIP
- Faking websites or compromising real websites
- Hiding links in PDF and Office attachments

Ensure employees are trained to spot these threats and your business enforces safe authentication procedures prior to all fund transfers.

5. Porting and Internal Network Traffic Controls

Keeping unwanted traffic out of your network is ideal, but what happens when that fails? This is where porting and internal network traffic controls comes into play.

Should any unauthorized visitor get into your home, you want to ensure they don't find the bedroom safe unlocked and open. The same goes for your business systems. Ensure the following:

- Network segmentation is designed so only those who need it have access to critical systems.
- Other computers that connect to the network are segregated from these critical systems and sensitive information centers.
- Common ports are "closed" or protected by default.
- Follow procedures to ensure access changes maintain network security.
- Review logs daily for unusual or suspicious behavior.

6. Back-Up System Protections

Even if a cyber attack doesn't result in the theft of your business's trade secrets, client data or financial credentials, a great deal of damage can be done if such data is damaged or lost. Having adequate back-up system protections in place is crucial. Consider these tips:

- The best systems include multiple, redundant backups. These backups should be segregated from the network and stored in geographically isolated locations to avoid contamination in the event of a network intrusion.
- Recommended back-up frequency can range from every day to monthly, depending on the needs of your business.
- If your business incorporates more sensitive systems and larger numbers of records, you should back up more frequently.

7. Cyber Liability Coverage

Given the potentially devastating impact of a cyber attack against your business, the right cyber liability policy coverage can mean the difference between your business surviving the attack or closing shop.

Cyber liability coverage can help cover costs related to a cyber attack or data breach, including:

- Privacy breach notification expenses
- Litigation
- Loss of income

- Regulatory fines and penalties
- Other related expenses

For the best protection, purchase standalone coverage with broad, comprehensive coverage and no sublimits.

About the Author

CyberLock Defense from Lockton Affinity provides industry-leading cyber liability insurance that offers full limits of cybercrime (cyber theft), social engineering, fraudulent funds transfer and more. With more than 35 industry groups eligible, including professional services, health care, retail, financial services and more, this comprehensive coverage helps protect your business against the costs associated with a cyber attack at affordable rates.

Those interested in coverage can visit CyberLockDefense.com or contact CyberLock Defense practice leader Jeff Severino at 913-652-7520 or JSeverino@locktonaffinity.com.

4 Steps to Prepare for a Ransomware Attack: A C-Suite Guide

By Rob T. Lee, Chief Curriculum Director and Faculty Lead at SANS Institute

The increased threat posed by increasing ransomware attacks, including the latest Kaseya attack that impacted nearly 1,500 organizations, has forced the C-Suite to think differently about the possibility of compromised systems. In the aftermath of Colonial and JBS, this attack highlights the critical need for businesses to plan for these events. Just as business leaders have an emergency preparedness plan in a natural disaster, it is critical to implement one for ransomware.

While these attacks had a substantial impact, quick action helped mitigate the scope of the damage. Had Colonial not quickly sprung into action, the effects would have exponentially increased if leadership had stalled on response. Flights out of the southeast were already making stops due to limited fuel at their originating airports. Had the situation remained uncontained for much longer, our transportation infrastructure, which was critical to helping distribute COVID-19 vaccines and other essential services, would have been even more crippled.

But how can leaders prepare for a ransomware attack that could take an entire organization's system offline? While CISA's ransomware checklist is a great place to start, organizations should ready a comprehensive ransomware preparedness strategy ahead of time that be adapted depending upon the severity of an attack. Here are four steps leadership should follow in developing a ransomware response strategy.

1. Evaluate the Levels of Risk Ransomware Could Pose to Operations Ahead of Time and Conduct Tabletop Exercises

Organizations need to understand where they are most vulnerable, from their most critical operations to other seemingly innocuous areas like HR or business records.

In the case of Colonial, although the ransomware attack took down its payment system, company leadership also decided to shut down the pipeline's oil production to mitigate damage. While some business operations may not be top of mind when thinking about potential ransomware impact, any business operation relying upon internet access is vulnerable. Organizations need to secure their most critical networks and think through how other business operations could be hampered by ransomware. If one segment of the business is compromised, it can have ripple effects across the entire enterprise.

2. Develop a Business Continuity Plan

It is critical to create a business continuity plan (BCP) and a disaster response plan (DPR) before any cyber incident, particularly a ransomware attack. These plans are critical to ensuring an organization can move quickly to get business up and running in the aftermath of an attack and mitigate damage. What systems could be held up by ransomware? Is valuable organization data backed up and encrypted regularly?

In high-stakes situations like ransomware attacks, company decision-makers must be involved from the get-go. Which leaders should be interested in these early-stage conversations? How will customers, key stakeholders, and the public be notified of the attack? Which entities should be engaged to help mitigate any additional risk?

Having plans in place is imperative but practicing them is also equally as important. Tabletop exercises are critical to helping business leaders and managers get acquainted with the protocol beforehand. Knowing exactly who is responsible for what and what strategies should be deployed when is vital. Plans should be easily accessible, saved in a secure location, and even physically printed if an attack results in a total system compromise.

3. Lay Out Your Payment Plan

If paying the ransom becomes the only path forward, it is crucial to have a payment plan in place. C-Suite leaders need to determine ahead of time where the company funds will come from and who will be responsible for the conversion to cryptocurrency and subsequent payments.

Having these plans in place before an attack will make the response process more efficient and prevent further costly mistakes.

4. Focus on Prevention

Ensuring that suitable security protocols are implemented companywide serves as the first line of defense from ransomware attacks. Train employees on security best practices early and often, as basic cyber hygiene can prevent costly mistakes. Applying a solid zero-trust architecture is also a smart, common-sense way to reduce the impact of any cyberattack.

Ransomware is something no organization wants to experience; however, preparing for that possibility is vital. Planning for a ransomware attack can help limit fiscal damage and human risk resulting from inaction or a poorly executed response. Analyzing the potential scope and impact of a ransomware attack should be on the top of the C-Suite priority list.

About the Author

Rob Lee is the Chief Curriculum Director and Faculty Lead at SANS Institute and runs his own consulting business specializing in information security, incident response, threat hunting, and digital forensics. With over 20 years of experience in digital forensics, vulnerability and exploit discovery, intrusion detection/prevention, and incident response, he is known as “The Godfather of DFIR”. Rob co-authored the book Know Your Enemy, 2nd Edition, and is course co-author of FOR500: Windows Forensic Analysis and FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics.

Black Market as Sustainable Ecosystem

By Milica D. Djekic

According to definition, the ecosystem is any complex network or interconnected system being observed in a much more general sense. The interconnections between the parts of such a system should get analyzed in details as their interactions could be well-studied and understood by the participants being interested in. The need for a comprehensive research comes from the essence of the things that can offer us the chance to cope with so complicated concepts in so simple terms suggesting those complex grids are well-explained to everyone. Right here, the sustainability is applied as the phrase that something if appropriately managed can be used again and again and from some perspective – the sustainability could get correlated with the maintainability as the way to keep things as they are and make them somewhat renewable and repairable if needed. The sustainable ecosystem is any complex grid or interconnected unit that has some sense of the self-management and it's significant to mention that any system if not innovatively maintained can shrink into itself as the rules of its functioning could become well-known to its opponents. In this case, we would talk about the black market as sustainable ecosystem that can also collapse once it gets discovered, investigated and resolved by the authorities. The more the investigation knows about the black market the better chances are for the case management to smash such a parasitic organism within the community.

The reasons why some systems can shrink are they would cope with the same and same patterns of their operations, so it could become predictable to anyone monitoring them from outside and finding the methods to deal with them from inside. The black market as sustainable ecosystem could get analyzed as a set of criminal offenses, malicious actors and value flows that should be investigated carefully and in a time consuming manner as no one from the suspects would remain unresolved to the criminal justice case. The interconnections and interactions between the actors in such an ecosystem could be so complex and sometimes it takes time to figure out how such a complicated system works. Being the part of the black market is the criminal offense as the actors distributing such a good through the communities could take advantage over stolen objects that would never get taxed by any government. In other words, the black marketers are so risk taking persons and in the societies with less developed system the black market can make the huge disadvantage to the state's budget and the overall safety of its members. On the other hand, no advanced country would want to deal with the black market on its territory as that sort of the crime can affect the quality of life to many public members as well as cause some disadvantages to the entire economy. To be honest, it's beyond the scope of this effort to discuss those socio-economical impacts too deeply as the primary goal of our article is to appoint some criminologist effects of such a criminality to the entire community and security of the people. In some ways, someone could deal with the information about the crime or the entire black market, but that person could hesitate to report such a finding to the local authorities.

As anything today the black market can get the transnational connotations and the practice would show there would be so many such oases on the web and in so many cases, the best approach to tackle such a concern is to shut down that internet location even if all the actors being involved would not get brought to the justice and they simply try to transfer to a much safer environment to them and continue doing with they used to do. It's hard to believe that the criminals would change their habits that easily and even if they want to quit with the crime they would always cope with the spirits from their past who would try to pull them back into that surrounding.

Any sustainable ecosystem is capable to manage itself through its interactions, actors and resources. Sometimes the rules would change, but the concepts would remain same. For instance, the actors could be different or they can interact in the completely new manner, but the basic principles would stay as they are. In case of the black market, we can say that social entity is more like the huge organism within the community that would engage so many actors committing the crime and offering the objects being obtained through the offenses to the community members for the quite attractive pricings. The reason why those pricings are suitable is the good is gotten through the illegal activity and nothing only the risk is invested to get the possession over so. So, if the expanses to obtain something being quite expensive are low and they include only the communications and logistics management it's obvious the competitive pricing can be the motive more to earn the big profit. Let us explain this a bit closer! For example, if the black marketers are doing the selling of portable IT devices they would use the service of the professional thieves who would steal such a good somewhere and provide so to the marketers for some financial compensation. So, those are the costs to the black marketers who can sell so for the popular pricing and still count on the good profit. The good can get sold as new or used and that can be done through the specialized markets, shops and stores. The thieves can steal something being so branding new or they can get in possession of the used objects. Anyhow, the good would always find its customer.

The new good could get found through the shipping of the valuable objects such as cloths, technology, tools and much more. Depending on the geographical location the shipping can go through the air, water or land and maybe it would be stolen in some area and offered on the fully new location. The metropolitan areas are the convenient spots to camouflage the track as there is the huge concentration of the people either being local or international. On the other hand, if the street crime occurs the criminals would provide the used good to the black marketers for some income and those guys could distribute that through the second-hand delivery systems of trading. Sometimes the members of the community could get involved into that chain as they would so naively buy something inexpensive from the black marketers simply believing they are their neighbors or friends. For instance, it can happen that some vehicles such as the bicycles could get stolen in some town, transferred to another, fixed there and then sold to the local community members as the used ones with the explanation they are imported from the overseas as the second-hand offering. The community member would see the bike is in the good condition; the price is good as well and that's how such an ecosystem would maintain itself. In other words, what we need hare the most is the awareness about who is who and who does what in that interconnected system, so far.

The black market ecosystem could be mentioned as sustainable for some reasons. The point is the street criminals, burglary offenders and thieves would get the money, valuable objects and the other useful things through the crime and maybe they would keep the money, but also sell anything they can to the black marketers. It would appear that those criminals are also the part of the black market network as they would feed it with the goods. Once the local gangsters get the values through the criminality they would be in position to deal with the money and spend some amounts on the stuffs being available in the shopping centers, trade malls and the other stores. So, the money being collected through the crime would be injected into the legal streams and someone would get the salary at the end of the month working as a staff in such a shop. That person would further make some spending through earned income on, say, new watch, gym or hairdressings. In other words, it's obvious how any single link in such a chain would impact each other and how the entire ecosystem would get correlated with each other. So, if anyone has bought the used vehicle which originates from the vehicle theft that person would feed the community simply giving the money for the fuel. If the criminals steal such a vehicle again and make some changes on it selling it to someone else, the new money would get available to many and they would get in position to spend so on their behalf. Probably someone would pay for the gym instructor to get the training in the fitness club and the next day that guy would stay without his wallet in the street offense. Maybe he would buy the new piece of the furniture for his home feeding the employees from that shop and the burglary would just happen there, so what he has bought would end up on the black market being offered to someone else.

From such a perspective, it's clear that the legal and black market would have the strong correlation and they would work together as the sustainable ecosystem. The link that would keep them together is the money that would circulate amongst the communities. The fact is the actors leading the legal businesses would pay the tax for their incomes, but they would never ask for the origin of the money being offered to any product or service. On the other hand, the black market would get fed through the crime and no one there would pay any cent to the state, so it would appear that such a spending being make for some good or favor could get the connotation of the laundered money. Basically, it would seem that the entire black market case needs a lot of deep understanding as the criminal groups could be such collaborative about each other as they got the good interest to rely on one another. In addition, the entire criminal environment could get assumed as so complex and dynamic network and as we analyze through this effort the black market as the sustainable ecosystem it's so obvious that some criminologist practice and doctrine could deal with the similar points of view. On the other hand, it's important to understand the mechanisms how the black market works mainly because that's the suitable way to conduct the result-driven investigation. Any case that can be resolved effectively and accurately is normally well-documented and shared with the public giving the awareness to anyone that the crime is so punishable. In other words, effectively resolving the investigation is the best way of the offense prevention and so many best practices would use such a doctrine to manage the risk in their communities, so far.

About The Author

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

Eight Top Use Cases for PKI in the Modern Enterprise

How PKI Is Still the Gold Standard for Identity in the Ever-Changing IT Security Landscape

By Alan Grau, VP of IoT, Embedded Solutions Sectigo (750 words for Cyber Defense Magazine)

Organizations are under increasing pressure to establish affective layers of cybersecurity defenses and practices. Confidence in traditional authentication measures for resources and applications is low, regardless of the environment, as big, news-shaking security breaches seemingly happen every day.

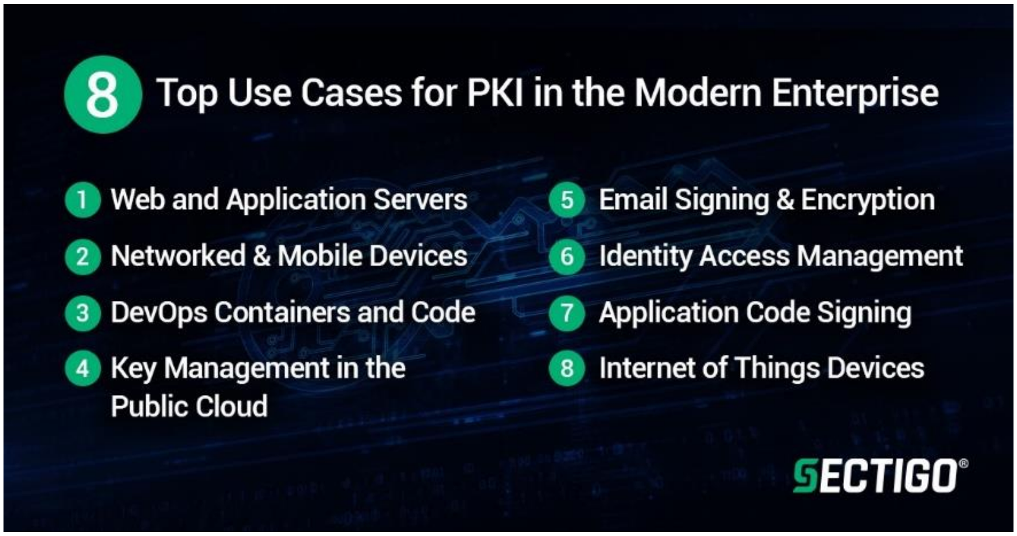
At the same time, sophisticated computing architectures, innovative connected devices, and emerging threats intersect in ways that demand an advanced level of security; one that can identify and verify all identities, whether human users, connected machines, or applications. Authentication failures make top news stories, such as the recent SolarWinds and Microsoft Exchange compromises. The IT security landscape has changed, the network security peremitor no longer exists and digital identity is the new perimeter.

It is mission-critical to authenticate the identities of people, devices, and processes and stop everyone and everything that doesn't have a bonafide and validated identity from gaining access.

PKI Rises to the Challenge

Using X.509 digital certificates based on asymmetric encryption using public/private key pairs can strengthen the verification of digital identities and secure connection between entities. Further, this process must be dynamic and continually verify devices, processes, and users.

PKI answers the demand for authentication and encryption and is considered the gold standard in digital privacy, identity, and security. It's already an integral part of our lives, often without our notice, including use in credit cards, passports, and e-commerce website authentication. PKI has, for decades, offered interoperability, high uptime, and governance. More recently, PKI has been utilized to cover an ever-growing set of use cases. Today's PKI management system can automate tasks, minimize manual processes, manage a broad range of portfolio tasks, scale up to manage millions of certificates, enable crypto-agility, and increase visibility into certificates with a "single pane of glass" view.



8 Top Use Cases for PKI in the Modern Enterprise

1 Web and Application Servers
2 Networked & Mobile Devices
3 DevOps Containers and Code
4 Key Management in the Public Cloud
5 Email Signing & Encryption
6 Identity Access Management
7 Application Code Signing
8 Internet of Things Devices

Eight Top Use Cases for PKI in the Modern Enterprise

As already complex environments expand further to include mobile devices, cloud infrastructure, DevOps, and Internet of Things (IoT), modern enterprises rely on PKI for robust digital identity in a variety of use cases. Here are the top eight ways to use PKI and fully automate digital identity:

1. **Web and Application Servers**
   SSL/TLS certificates encrypt communication over the internet and ensure a trusted client-server connection. Enterprises should implement this level of authentication and encryption across websites and applications in the cloud and behind the firewall.

CAPTION: An organization's in-house and cloud data network and servers need to be protected against cyber-attack.

2. **Networked & Mobile Devices**
   Employees require secure remote access via Wi-Fi and VPN to applications and networks using laptops, smartphones, and employee-owned devices. PKI certificates replace easily hacked passwords and increase trust by offering the strongest, simplest, and most cost-effective form of client authentication.
3. **DevOps Containers and Code**
   Engineering teams can increase security of their DevOps workflows with code signing certificates and high-volume, short-lifespan SSL certificates to ensure the integrity of containers, the code they run, and the production applications that use them.
4. **Key Management in the Public Cloud**
   Certificates protect your applications hosted in the cloud. Using one centralized certificate management solution that automatically discovers, issues, and renews all your certificates in both your cloud and entire enterprise environment ensures your applications are always running smoothly and eliminates downtime due to expired certificates.
5. **Email Signing & Encryption**
   S/MIME email certificates avoid the increasing number of sophisticated attacks on email users and infrastructure, including phishing attacks. By encrypting/decrypting email messages and attachments and validating identity, S/MIME email certificates assure users that emails are authentic and unmodified.
6. **Identity Access Management**
   To support a Zero Trust security strategy, PKI certificates and key pairs strengthen digital identity verification and secure the connections between entities beyond and within the firewalled network architecture.

7. **Application Code Signing**
   Code signing adds a layer of assurance for both internal and external-facing applications, informing users they can trust the software they are using.

Caption: Authentication is essential for protecting connected devices of all types - for home, business, and industry.

8. **IoT Devices**
   With the vast number and wide distribution of IoT devices, strong device identity authentication and remote security deployment to all connected devices are necessary to securely build-out, scale, and manage IoT ecosystems. Digital certificates provide strong device identity, and enable secure firmware updates, secure boot and secure device to cloud communication.

Summary

Protect the identities of your people, devices, and data, both within the corporate network and beyond your firewall. The risks of not adapting to the new IT security landscape can be staggering. After all, enterprises that fail to secure digital identities are not only vulnerable to criminal activity and fraud; they are also risking operational performance, customer experience, and compliance. Poor authentication practices have already led to numerous high-profile breaches and outages, resulting in compromised information, federal investigations and lawsuits, and billions of dollars in lost revenue and fines. The risks are apparent, and solutions are ready. It is time for a digital identity makeover.

About the Author

Alan Grau is VP of IoT, Embedded Solutions at Sectigo, the world's largest commercial Certificate Authority and provider of purpose-built, automated PKI solutions. Alan has 25 years of experience in telecommunications and the embedded software marketplace and joined Sectigo in May 2019 as part of the company's acquisition of Icon Labs, a leading provider of security software for IoT and embedded devices, where he was co-founder and CTO. He is a frequent industry speaker and blogger and holds multiple patents related to telecommunication and security.

Prior to founding Icon Labs, Alan worked for AT&T Bell Labs and Motorola. He has an MS in computer science from Northwestern University.
Alan can be reached online at <alan.grau@sectigo.com> and at our company website https://sectigo.com/

Greater IT Freedom with Tighter IT Security Underscores New Enterprise Security Paradox Report

How twelve months and new corporate security threats have changed IT and security leaders’ thinking on ensuring workers’ secure remote access to corporate assets

By Marc Gaffan, Hysolate CEO

More than a year into the worldwide forced experiment in remote-first IT strategies, how have IT and security leaders’ views changed with regard to keeping workers productive and enterprises protected? That was the essential question we set out to answer in our most recent IT security survey.

Moreover, we were looking for an evolution in thinking from the sentiments expressed back in the spring of 2020, when we published our first survey report, *The CISO’s Dilemma*. In this early 2020 study, IT and security leaders viewed IT freedom and corporate security as competing priorities, in which only one or the other could prevail, and only by sacrificing the priority deemed the lesser of the two.

Mixed opinions on remote IT from early in the pandemic response

For our 2020 study, we surveyed IT and security leaders at the height of companies' mad scramble to go remote-first at any cost. COVID-19 was surging around the world with no vaccines in sight, and companies were making up business continuity plans on the fly. Helping workers remain productive from home while trying to preserve a corporate security perimeter that had expanded geometrically overnight was pushing companies to radically rethink their remote access policies.

The result? Thirty-five percent of companies relaxed their security stance to encourage worker productivity. Taking a different tack, 26 percent introduced more stringent endpoint security to better protect corporate assets. And, perhaps the greatest signal of uncertainty, 39 percent left their security policies untouched.

With no prevailing attitude regarding how best to keep operations moving while enabling everyone who could work remotely to do so, the only clear signal coming from the field was the idea that encouraging IT freedom and boosting corporate security were opposite sides of a single coin, a pair of "either/or" outcomes.

How far we've come in the course of a year

So what are IT and security leaders thinking today? We conducted our 2021 survey about a year after the study that yielded The CISO's Dilemma. Twelve months of remote-first lessons and a bunch of high-profile ransomware attacks later, disparate worlds of thought regarding worker productivity and corporate security have converged, but not in any way that we had expected.

Ninety-six percent of security personnel and 84 percent of IT respondents said their companies need to increase employee IT freedom, regardless of where they are working. Further, 87 percent also said that providing greater IT freedom has a positive impact on overall employee productivity. OK, good: companies recognize that worker productivity is tied to IT freedom, and nearly all respondents are calling for more IT freedom.

At the same time, however, 79 percent said their companies need to enact greater IT restrictions on employees. When nine in ten call for greater IT freedom and eight in ten call for more stringent IT, it doesn't take a data scientist to realize that most respondents are calling for their companies to move in diametrically opposed directions at the very same time. We've called this phenomenon (and our 2021 survey report) *The Enterprise Security Paradox*.

Understanding the duality of The Enterprise Security Paradox

On the bright side, it's clear that respondents no longer see IT freedom and corporate security as mutually exclusive. But on the murky side… How can any given IT or security leader be demanding both at the same time? The answer comes to light by examining the other significant findings of the study.

Ninety percent of respondents say employees at their company have jobs that require them to engage in IT activities that they describe as “risky,” including installing unsanctioned applications and provisioning sandbox environments for developers, among others. Also, 17 percent of respondents say the employees at their companies rely on their corporate-owned endpoints for conducting personal business, exposing the company to further risk. Given this context, survey respondents say that only seven percent of employees are satisfied with their current corporate security policies, and the vast majority (93%) are actively working around IT restrictions.

Today’s workers browse questionable websites, download email attachments, install third-party applications, and more, and our study reveals an acknowledgment on the part of IT and security personnel that companies need technology solutions and policies that support workers' quest for IT freedom without compromising enterprise security.

Work today is, of course, highly collaborative. SaaS applications and remote access solutions make it increasingly easy to outsource more and more business processes to vendors. Survey respondents see this growing reliance on external entities as a source of risk that they need to manage carefully. More than 85 percent of respondents say that the access their companies provide to contractors and other third parties is a concern. When we examined the data by industry, the story is even more interesting: A full 100 percent of respondents in the financial services and retail sectors say third-party access is a potential problem.

But it’s not just external parties that today’s IT and security leaders are worried about. Ninety-one percent of security personnel and 75 percent of IT leaders say their companies need to enact more IT restrictions on their own employees. They’re looking for new solutions that can enhance security while expanding IT freedom.

Investing in new isolation solutions

The good news for these survey respondents is that the vast majority (93 percent) of the companies they represent have managing remote IT as a budget item for 2021. The top budget items reported are isolating untrusted incoming content and allowing the use of non-IT-sanctioned applications & websites that are required for their jobs, split almost evenly at 42 percent and 40 percent respectively.

In terms of specific technologies in use or targeted by respondents, endpoint privilege management (EPM) technology is the most common, reported to be either currently in use or soon to be implemented by 95 percent of respondents. Application and browser isolation solutions also are among the most popular approaches either soon to be or currently in use at 88 and 90 percent respectively. Desktop-as-a-service (DaaS) is showing comparable popularity (88 percent), while virtual desktop infrastructure (VDI) lags behind at 70 percent.

Rounding out the key findings

The Enterprise Security Paradox report demonstrates that IT and Security leaders recognize the need for a multifaceted approach to orchestrating secure access at scale. Enterprises need solutions that can simultaneously free workers to engage in the full breadth of their job responsibilities while making sure that the most risk-laden tasks (downloading email attachments, installing 3rd-party applications, browsing questionable websites, etc.) can be accomplished without compromising enterprise security.

Our report shows that respondents are keen to identify technologies that will help them both expand IT freedom and tighten IT security concurrently. IT and security leaders are primed for new technology solutions that can increase worker productivity while enhancing corporate security, thereby solving the Enterprise Security Paradox.

To read the full 2021 survey report, The Enterprise Security Paradox, click here. To read the full 2020 survey report, The CISO's DIlemma, click here.

About the Author

Marc is CEO of Hysolate, a startup that is changing how we manage and secure our endpoints. Prior to joining Hysolate, Marc was the Chief Business Officer at Nexar, where he led sales, marketing, biz-dev, customer success and field operations. He is a thought leader on application security and distributed denial of service (DDoS) and has appeared before the US Congress, FDIC and Federal Trade Commission on cyber security and identity theft topics.

Marc can be reached online at marc@hysolate.com and at our company website https://www.hysolate.com/

A PETs-Enabled Path to Secure & Private Data Monetization

By Ellison Anne Williams, CEO & Founder of Enveil

Large enterprise organizations are always looking for ways to create new revenue streams and that's never more true than today. One approach to finding such opportunities is to assess internal data holdings and explore how those existing assets might be further leveraged. In today's environment, almost any piece of data can be monetized and organizations are increasingly pursuing avenues to turn their data into revenue-generating products and services. And such efforts may benefit more than just the near-term bottom line: research suggests that businesses that work to monetize data assets outperform those who do not.

But while data is both a competitive asset and potentially lucrative revenue generator, it can also be a risk trigger. According to Accenture's Technology Vision survey, 81 percent of executives agree that as the business value of data grows, the risks companies face from the improper handling of data grow exponentially. Leveraging data assets for monetization purposes can introduce privacy challenges and security vulnerabilities that traditional risk-mitigation strategies are often not designed to address. In order to overcome such barriers, organizations are increasingly asking, "How can we create revenue while respecting the security and the privacy of existing data assets, and protecting the interests of those who wish to leverage our data?" There is good news for these exploratory organizations: technology is now ready to provide a practical, scalable answer.

Advances in a category of solutions known as Privacy Enhancing Technologies (PETs) are changing the game for unlocking data value by facilitating the secure and private usage of data. These technologies

— which include homomorphic encryption, secure multiparty computation, and trusted execution environments, among others — allow businesses to responsibly monetize existing data assets by respecting the privacy of both the customers using the monetization service and the data itself. It is critical that data owners consider both of these components, the data and participants, or the risks associated with monetization may outweigh the benefits.

At the core of any effective monetization strategy is the holistic security and governance of the data itself. Some organizations are working to address this issue by adopting a data-centric approach to security, focusing on the security of the data rather than just the networks, servers, and applications it resides on. The goal of this holistic approach is to protect data wherever it is within an organization, whether at rest on the file system, moving through the network, or while it's actually being used or processed, as represented in the Data Security Triad. If there is data of value at stake, it must be protected at all times.

While Data at Rest and Data in Transit are commonly protected using standard data and transport encryption, the Data in Use segment is frequently overlooked by many organizations. Protecting data while it's being used is especially of critical importance when it comes to leveraging data for monetization purposes. PETs solutions are uniquely positioned to address these Data in Use vulnerabilities because they can allow sensitive or regulated data to be securely processed and in a privacy-preserving manner without the risk of exposure. With PETs, organizations can analyze, use, and provide access to data assets in ways that may have previously been determined to be too risky, especially if that data is to be shared with a third party.

PETs can also serve to protect the users of data monetization platforms by protecting their interests and intents. For competitive reasons, organizations generally want to avoid revealing their specific interests in a third-party dataset, even to the data owner. PETs allow these users to perform encrypted queries and analysis, ensuring the content of their interaction with the data is never exposed beyond their walls. For data owners, this expands the range of potential targets and ensures that users never introduce sensitive or regulated content, such as those they may be included in the query itself, into their environment.

Another significant barrier to monetizing existing data assets has been the need to combine or move data assets to a central or even third-party location. There are a number of issues with such an approach, only some of which involve data privacy. But homomorphic encryption, a pillar of the PETs category, can overcome this challenge by enabling a decentralized framework for secure data sharing and monetization. When designed to work as a proxy layer, the technology can also allow organizations to integrate with existing data governance mechanisms such as access control measures and audit systems. This ability to control and audit data usage and access is key to any monetization initiative.

There is no question that there are new revenue opportunities waiting to be unlocked by securely and privately leveraging existing data assets in a privacy-preserving manner. However, while pursuing technical answers to the question of "Can we?" organizations must also consider the foundational question of "Should we?" before they embark. Data monetization is a cross-functional undertaking and it is important that all internal stakeholders, including privacy, security, and legal teams, are involved to help identify and mitigate potential risks, and ensure that monetization activities are pursued in a way that fully respects the privacy and security of the data as well as those leveraging it. Privacy Enhancing Technologies can deliver on that commitment, providing organizations with a path to responsibly leveraging data assets.

About the Author

Dr. Ellison Anne Williams is the Founder and CEO of Enveil. Building on more than a decade of experience leading avant-garde efforts in the areas of large scale analytics, information security and privacy, computer network exploitation, and network modeling, she founded the startup in 2016 to protect sensitive data while it's being used or processed – the 'holy grail' of data encryption. Ellison Anne leverages her deep technical background and a passion for evangelizing the impact of disruptive technologies to cultivate category-defining solutions that enable secure data search, analytics, sharing, and collaboration. She holds a Ph.D. in mathematics (algebraic combinatorics), an M.S. in mathematics (set theoretic topology), and an M.S. in computer science (machine learning).

Align Business Logic with Vulnerability Management to Mature Your Security Program

By Florindo Gallicchio, Managing Director at NetSPI

There's no doubt about it: attack surfaces grow and evolve around the clock. With network configurations, new tools and applications, and third-party integrations coming online constantly, an atmosphere is being created that opens the possibility of unidentified security gaps. The fact is that cyberattacks can affect your business and are, unfortunately, more prevalent than natural disasters and extreme weather events. And we know from our own NetSPI research that nearly 70 percent of security leaders are concerned about network vulnerabilities after implementing new security tools.

Prevention is key to a mature cyber security program. In fact, according to a recent Ponemon Institute study, when cyber security attacks are prevented, organizations can save resources, costs, damages, time and reputation. Yet, companies still may think they are protected by buying the latest cyber security technologies or just by working to change team behaviors that pose the most risk (i.e., using stronger passwords, avoiding phishing scams, etc.). While there is a place in a security program for these and other security measures, time and budget constraints create major barriers. Therefore, it is critical that an organization's vulnerability management program is strongly built on a strategy that is risk-based and business aligned.

Automated scanning is not enough

Many organizations consider vulnerability management to be running a scanner with all the checks turned on, and then addressing the high-risk findings. The truth is, in my experience, this bottom-up approach presents two major problems:

- Scanner policy configurations are not one-size-fits-all. When set to scan for all possible technology vulnerabilities, the scanner can produce an enormous amount of noise in which meaningful vulnerabilities may be missed or ignored. This "spray and pray" method creates more confusion and eventually apathy toward purposeful vulnerability analysis.
- Similar vulnerabilities can pose drastically different risks. For example, a discovered open share on a file server containing HR data may be categorized by a scanner as medium risk, but the actual risk to the business is high or even critical. A discovered open share on a print controller containing fonts or no files at all may also be categorized as medium risk but in fact is a low risk to the business. Without the proper context an organization may treat these two findings as equal and expend the same time and effort (cost) in addressing both when they do not merit equal treatment.

Develop a business aligned vulnerability management program

Strategy is a concept that can mean different things to different people, in part because there is not a standard approach to cyber security program development. Each business has different security needs. As security leaders, we address the threats that pose imminent and perceived harm to the environment, and those that get noticed most, get attention first. And understandably so, given the ever-advancing threats companies face. Often is the case, however, that what is considered harmful to the environment is not always rooted in what is most important, or what poses the most risk to a business. That is where a business-aligned vulnerability management program comes into play.

A business-aligned vulnerability management program takes into consideration the vulnerabilities that would have the most significant, negative impact on the business, the most relevant threats that could exploit those vulnerabilities, remediation strategies, as well as the controls needed to counter those threats. Such a strategy is built on a framework that enables, implements, and maintains the program and informs all security initiatives, controls, and processes.

While developing a business-aligned vulnerability management program, it is important to ask, "What are the ramifications?" when considering a potential risk, a discovered vulnerability, a detected event, a proposed initiative, or virtually any other consideration affecting security posture. Below are a few hypothetical situations to demonstrate how asking about ramifications can help strengthen a business-aligned vulnerability management program.

Vulnerability Finding	Ramifications?	Remediation Recommendations
Poor Administrator Account Password	Attacker can gain access to and steal data. Poses enterprise risks to information, business operations, regulatory compliance, and business reputation. Regulatory non-compliance leading to financial sanctions. Legal action by affected customers leading to financial reparations.	Change the admin password. Strengthen the admin password. Use multifactor authentication. Use "zero trust" access model. Purchase technology to enhance identity and access controls. Conduct vulnerability testing more often.
Vulnerable Version – PHP	Successful exploitation of available vulnerabilities may allow a remote unauthenticated attacker to execute arbitrary commands directly or indirectly on the affected systems. As a result, the confidentiality, integrity, and availability of the affected systems and associated data may be compromised.	Disable or uninstall PHP if it is not required for a defined business purpose. If PHP is required, upgrade to the latest stable version of the software or apply vendor supplied patches. If no fix is available, contact the vendor for solutions and consider isolating the affected service via host based and network firewalls.
SQL Injection	SQL injection may allow an attacker to extract, modify, add, or delete information from database servers, causing the confidentiality and integrity of the information stored in the database to be compromised. Depending on the SQL implementation, the attacker may also be able to execute system commands on the affected host. In some circumstances, this provides the means to take control of the server hosting the database, leading to the complete compromise of the confidentiality, integrity, and availability of the affected host.	Employ a layered approach to security that includes using parameterized queries when accepting user input. Strictly define the data type that the application will accept. Also, disable detailed error messages that could give an attacker information about the database. Additionally, following the principle of least privilege when assigning permissions for the service account and database user helps limit the impact of a successful SQL injection attack.

The key is to understand the risks most likely to disrupt the business from meeting its objectives, identify the threats that would cause and amplify those risks, and select the controls most appropriate for managing those threats. The controls should then be regularly measured and audited to ensure they are implemented correctly and are effective in protecting the organization. Measured improvements in security maturity are an expensive undertaking. The costs in terms of money, time, and effort can skyrocket if guardrails aren't applied to focus the process on specific objectives, otherwise it is a continuous game of catching up each time a vulnerability scan is run. That’s why a vulnerability strategy is critical.

Do not rely on tools to find business logic vulnerabilities

Most vulnerability data come from scanners, but the most important vulnerability data often comes from humans, specifically penetration testers.

It’s a fact that good pentesters use automated scanning tools (ideally from many different sources) and run frequent vulnerability discovery and assessment scans in the overall pentesting process. Scanning is generally considered an addition to manual, deep dive pentests conducted by an ethical hacker. When correctly understood, manual penetration testing leverages the findings from automated vulnerability and risk assessment scanning tools to pick critical targets for experienced human pentesters to: 1) verify as high-fidelity rather than chasing false-positives, and then 2) to consider exploiting as possible incremental steps in a serious effort to eventually gain privileged access somewhere important on the network.

Purely automated tools or highly automated testing activities cannot adequately perform testing of the business logic baked into the application under the test. While some tools claim to perform complete testing, no automated technology solution on the market today can perform true business logic testing. The process requires the human element that goes well beyond the capabilities of even the most sophisticated automated tools.

Vulnerability data tracking helps ensure remediation

Vulnerability data must be tracked to ensure remediation – otherwise vulnerabilities may fall through the cracks and leave your organization exposed to a data breach or other cyber security attacks. Further, developing vulnerability tracking requires a system for managing remediation workflows that can handle these seven tasks:

- Ingestion of various data formats with flexible normalization
- Reviewing of normalized data for changes and modifications as needed
- Distribution of normalized data to various external systems
- Tracking the data distributed externally to keep a central listing up to date
- Ensuring policy is adhered to across the various systems where the data vulnerability remediation is tracked
- Sending notifications and keeping humans involved in the process, especially when vulnerability remediation is overdue
- Reporting on the outcome of vulnerabilities by group, business unit, or globally across the organization

This all ties back to risk-based security. The security industry should understand why risk-based security strategies are more effective than compliance-based strategies but are often challenged as to how to make the shift. To mature your security program and achieve a risk-based strategy, it is essential to align business logic with vulnerability management and track and prioritize the vulnerabilities that pose the highest risk specific to your business.

About the Author

About Florindo Gallicchio: Florindo Gallicchio is a Managing Director at NetSPI and serves as a strategic advisor to executives, boards of directors, and technology staff. He is a senior risk management and information security practitioner with extensive experience in building and running cyber security programs to securely manage the business while also achieving and maintaining compliance to regulatory and industry requirements. Prior to joining NetSPI, Florindo was the CISO at a global advisory investment firm in New York City. He began his career with the National Security Agency while serving in the U.S. Navy, where in ten years of service he worked in signals and communications intelligence collection and systems exploitation.

Florindo can be reached online at (Florindo.Gallicchio@netspi.com, @SecureFlorindo, etc..) and at our company website https://www.netspi.com

Top Tips Every SMB Must Know to Safeguard from Phishing Scams

People, processes, and intelligent threat response safeguard SMBs

By Nadav Arbel, co-founder and CEO, CYREBRO

Phishing, coming in the form of emails, scam phone calls, and phony web sites remains the most grave cybersecurity threat that SMBs are facing, and in 2020 businesses accrued approximately $12 billion in losses alone. These attacks are widespread due to the persuasive social engineering tactics that target staff (and executives) with tailored campaigns to lure employees into opening malicious files and links while masquerading as a trusted entity to suspend disbelief.

The ‘parade of horribles’ begins once attackers gain inside access. They’ll exploit your accounts, such as email, to learn more about the company’s activities to maximize their haul. The big score comes when the attackers start communicating with the finance department, requesting sensitive banking info, changing account information, or rerouting payments to their own accounts. They’ll also attempt to defraud others in the company by impersonating the compromised user, taking full advantage of the inherent trust of workplace relationships.

They’ll then ultimately steal sensitive information or hold SMBs hostage with ransomware.

Phishing attacks are avoidable when we take common sense steps; it doesn’t take a security sleuth to identify when something is ‘off’. Spelling mistakes, unusual requests, peculiar timing, pressure tactics, threats, unexpected attachments, and abnormal looking email addresses or web links are all red flags. We all can become ‘human firewalls’ by exercising caution and contacting our IT teams or any known sender through a different medium when in doubt. A telephone call may be an anachronism when colleagues would prefer to receive a text, but investing some extra time to identify threats can forestall severe consequences.

Know Your ‘Red Flags’

Security awareness training is your first step to defend against these attacks. It boils down to not clicking on or opening anything that looks suspicious. Educate your employees about potential dangers and help them to identify common attacks and inconsistencies within emails. A good practice is never to send sensitive data through email. Mistakes do happen and attack victims should immediately delete all emails that contain sensitive data such as text credentials or unencrypted sensitive company data, both from the inbox and from the trash folder. This is something that should be done regularly, regardless of whether an attack has occurred.

The best offense is a good defense and it’s preferable not to become a victim in the first place. Here are some of the most important red flags to look out for to protect the confidentiality and integrity of your business systems.

1) Attackers Often Impersonate the Biggest Brands

Our team recently encountered a scenario where a phishing email leveraged Microsoft’s brand awareness and status as a trusted company to entice a user to click on an email link. The link exploited flaws in a nonprofit's website to redirect the would-be victim to the phishing page, disguised as a familiar Microsoft log-in page, which would then capture his/her credentials. Security platforms are capable of recognizing indicators of an attack going forward.

However, the onus is often still on employees to react responsibly, following security awareness training. The phony Microsoft site was convincing, but the employee’s eagle eye spotted some irregularities. Microsoft never sends users emails that claim messages are ‘being held up by our server’ and reputable companies never ask users to verify their credentials in this manner.

2) Phishing Emails Frequently Display Design and Grammar Mistakes

The phishing email contained a Microsoft logo that didn’t match the company’s design scheme (also pay attention to other elements such as size and colors), nor did the font fit the branding. These messages also often contain spelling mistakes and poor grammar that wouldn’t be representative of an established brand. Always note that some emails may not contain these errors but use pressure tactics instead. For instance, an email purporting to be from your CEO may demand sensitive information; don’t be afraid to inquire whether it’s really him/her.

Other red flags are less overt but can still be uncovered with minimal effort.

3) Malformed Links and Emails:

Hovering your cursor over the link in the email will reveal a suspicious-looking URL (never click it!). Addresses that appear to be legitimate at first glance but are irregular are the product of typosquatting, where hackers will either change a single letter in the URL or add an incorrect top-level domain. For example, Microsoft is always Microsoft.com and would never be written as Microsoft.co or MIcrosoft (written with a lower case ‘I’ instead of the correct ‘i’.

4) Asking for Credentials and Unusual Messages:

One of the most common scams involves an email that tells a user their account was compromised and that they need to log in to reset their passwords. As a rule, reputable companies never ask users to enter their credentials via email. As in the example above, Microsoft never sends users emails that tell them urgent messages are waiting. Hackers use this type of message to tempt users and play into their fears that they are missing essential information. Even executives are lured by threats of lawsuits or government penalties.

Being Proactive, Not Reactive

Having the capacity to easily recognize red flags throughout your organization is vitally important, but businesses can also be proactive by working with their IT team to establish secure configurations. The threat environment is more acute than it used to be, and IT teams should consider disabling legacy MS Office features such as running macros that originate from email, blocking OLE Excel update links, and disabling some outdated SMB network protocols (first verifying that those changes don’t interfere with their workflows). Administrators can enable features that bolster traditional passwords, such as multi-factor authentication, and disable admin rights from end users. This helps prevent a workstation from being compromised and halting any lateral spread over a network. Admin rights allow malware to do whatever it wants to on a PC. Contact your advisor to learn more about what actions to take to safeguard your specific systems and have a conversation about whether the appropriate security systems would help change your company’s posture from passive and reactive to proactive and responsive.

Good IT hygiene practices work together with ‘human firewalls’, as well as security platforms that scrutinize incoming emails and/or threat intelligence systems to monitor and inform IT managers about when attacks occur and how to best respond to those incidents. It’s important for IT managers to understand how to use their security systems well, or signals could be missed. It’s not the number of systems that determines security: it’s how they’re used and the quality of the response. The best rule of thumb is always: if it looks suspicious, say something. Send it to a security specialist who knows how to deal with it safely. Better yet, employ a threat intelligence system throughout your network to avoid the situation in the first place.

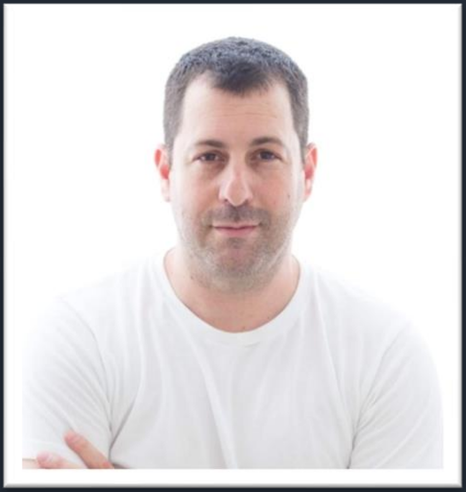
Visibility and Threat Response Help to Stay a Step Ahead

Threat intelligence systems monitor the entirety of your IT assets, including email services, to uncover unusual behaviors and occurrences that match known attacks. Most email providers offer tiers of service that include rudimentary reporting which can be used in isolation or fed into platforms that utilize expert threat hunters and machine intelligence to analyze the full context around security incidents. Threat intelligence platforms will surface attacks from all sources but like traditional PC security systems, they cannot always foresee what the next threat will be or identify a false positive that impacts your business operations with unnecessary system downtime. SOC Platforms (Security Operations Center) combine human insight with machine intelligence for better results. Traditional SOCs are substantial and costly undertakings.

The sheer variety of disciplines IT professionals must master to be security experts and dedicate themselves to threat hunting and response exceeds the resources of SMBs. Systems such as SOC platforms are designed to overcome that limitation by making incident response more accessible and practical. These platforms can utilize the same defenses as large enterprises, which have the capacity to build out their own SOC with dedicated experts and technologies.

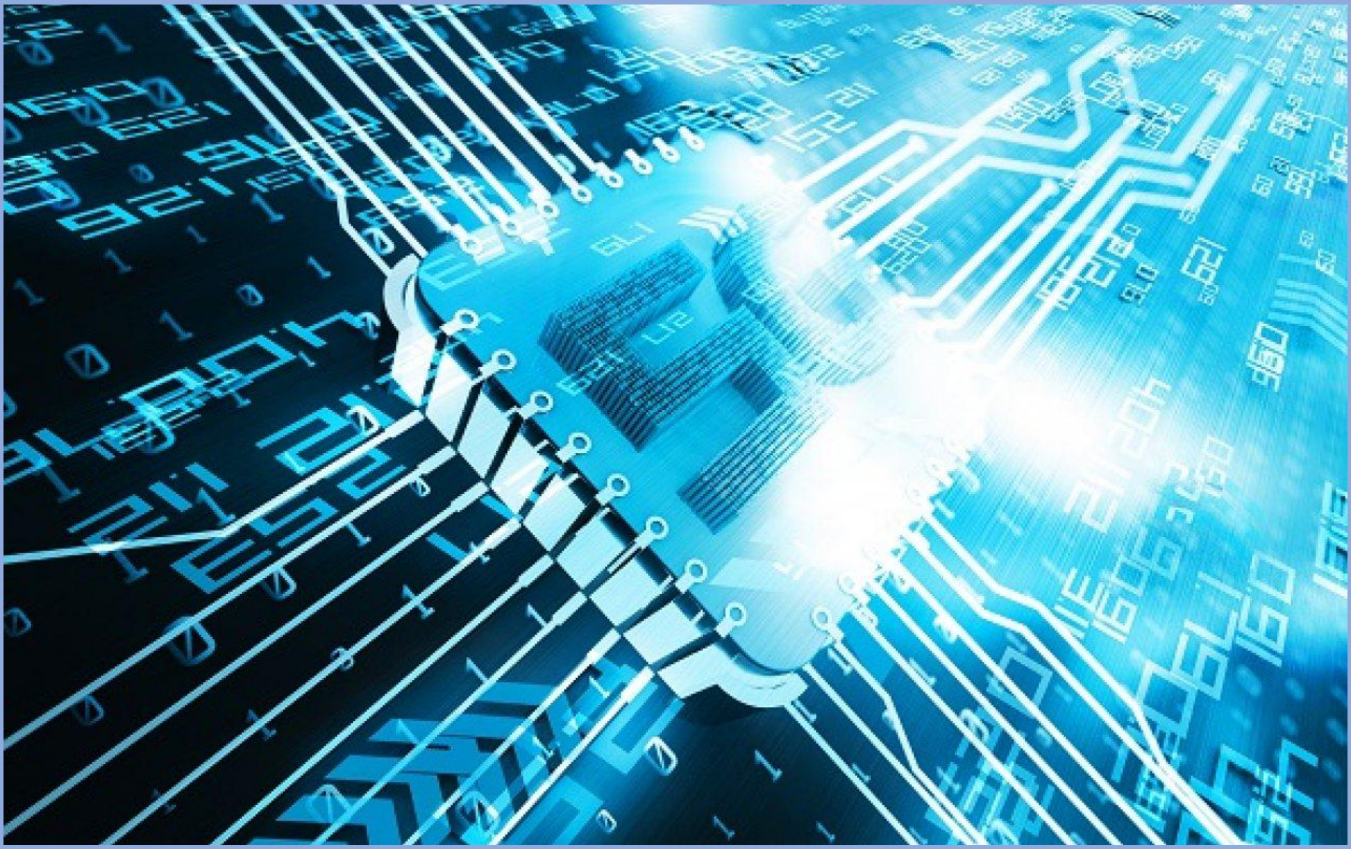
Bad actors are clever and always uncover new ways in. The financial incentive is immense and following the steps outlined above will protect your business from becoming the next victim. Steps like educating your workforce, hardening systems, or making investments that leverage the information that’s being gathered from all sources to equip your IT team with insights and guidance into what’s happening in real-time, versus being hit by costly incidents. Cybersecurity is a process that can begin with small steps and benefits from expert guidance.

About the Author



Nadav Arbel is the co-founder and CEO of CYREBRO. He has spent 20+ years revolutionizing how companies operate their cybersecurity with groundbreaking Cyber-Tech, Cyber-Operations & AI in Cyber Security, Cyber Defense, and Forensics. Nadav also previously headed the Cyber Security Division for the Israeli Police Force where he established and commanded the Israeli Cyber & SIGINT technology unit.

Nadav Arbel can be reached online at (https://il.linkedin.com/in/nadav-arbel-05a06230) and at our company website https://www.cyrebro.io/



From Security-Enhanced 5G Networks to Security-by-Design 6G Systems

Towards Trustworthy and Resilient Information and Communication Systems

By Dr. David Soldani, Adj. Professor, UNSW, Australia

While commercial activity is wholly focused on fully realising the vast potential of 5G, technical research attention is now turning to 6G. Many 6G initiatives are underway globally and, although details remain uncertain, the investments provide a fascinating prospect for our future.

However, one certainty is that, more than ever, close global collaboration will be necessary among all stakeholders to realise the 6G vision. The integration, or direct involvement, of vertical associations, such as 5GAA and 5GACIA, with 3GPP standardisation development organisations is essential. The current working model will not be sustainable due to the wide spread of revolutionary technologies forming the fabric of our lives and work environments.

It also requires an ecosystem of public and private players, combined with a multi-disciplinary approach to ensure that all assets forming 6G systems are interoperable, comply with standardised security evaluation criteria (such as the GSMA/3GPP NESAS) and even the smallest asset in the end-to-end supply chain supports the minimal set of approved security requirements.

6G gaining momentum

Although 6G is likely to go live around 2030, the number of 6G initiatives underway globally and corresponding investments offer an intriguing prospect for the future. The requirements likely demanded by 6G include yet unfulfilled 5G use cases and more advanced scenarios emerging for next generation/6G networks. Examples of such emerging scenarios include Terahertz frequencies, holoportation, tactile/haptic communications, ubiquitous services (land, air, space, and sea), imaging and sensing.

In Europe, within the EU Horizon 2020 Research and Innovation (R&I) framework programme, three projects focused on 6G development have been announced: Hexa-X, RISE-6G, and NEW-6G. The European Commission (EC), within the Smart Network and Service framework programme, has proposed a €900 million budget to invest in 6G research, with particular attention to standardisation leadership. Beyond that, several countries have allocated budget to conduct their own research., Australia, Japan, USA, UK, Finland, South Korea and China have announced, and there is pressure on other nations to join.

6G network architecture

6G wireless aims at bridging the “physical” and “cyber” worlds, shifting *from connected people and things to connected intelligence*. In short, 6G wireless is the technology to deliver artificial intelligence to everyone, anywhere and at any time.

The 6G wireless architecture will be shaped by five key constituents: virtual-X, tactile, inferencing, sensing, and learning. The primary spectrum will be millimetre and terahertz waves (above 110 GHz), which will allow us to apply real-time (RT) wireless sensing capabilities, the fabric to link the physical and cyber worlds.

The primary service will be virtual reality (VR) for everything. The virtual-X channel will allow access to digital content in the cyber world. The augmented tactile channel will carry haptic feedback, as the augmented neural system for the physical world. The inference channel will exchange services between the AI engine and the end user.

The Edge Node will be mostly used for local Machine Learning (ML), so the classical Point of Presence (PoP) at the edge will become the Neural Edge and the 6G Base Station (BS) the Deep Neural Node. Neural Centres (Cloud with Global AI capabilities) provide AI services to external customers (AIaaS). Examples of such services could include AI-enabled high precision localisation and end user mobility trends. Quantum (Q) key distribution technology can be deployed for the fibre-optic link between the Neural Centre and the Neural Edge.

6G technology enablers

We anticipate five essential technology enablers that will be necessary to fulfil the needs of the next generation system to realise the fundamental shift in paradigm from the internet of things to the internet of intelligence, the latter being defined as functions with the ability to represent knowledge, process knowledge and make decisions.

Combined Sensing and Communication

The first paradigm shift is about going from an information-centric approach of bits and bytes to uplink and downlink sensing, with sensing capabilities imbued in devices and access points (radio heads, denoted as Neural Edges) operating at very high frequencies and using very large detached and contiguous bandwidths.

The capability of 6G wireless link transmission is expected to be improved by at least 10–100 times that of 5G to achieve a Tbps target. 6G wireless is also anticipated to widen supported frequency bandwidths, operate at a variety of carrier frequencies, and transmit at minimal transmission power. Going to the upper mmW band (100–300 GHz), and, in the future, the THz band (>300 GHz), network throughput and resource sharing among users could be pushed far beyond that of 5G, especially in densely populated areas.

The upper mmW or THz band also has the potential for sensing networks. Sensing is an important part of future 6G networks and devices. We will be able to sense the environment and context (like radar or lidar systems today) and integrate this information with anything that can be captured by devices, thus making it possible to offer Sensing as a Service.

Artificial Intelligence at the Network Edge

The second paradigm shift involves moving from an artificial intelligence-enhanced network (5G) to an AI-native communication platform, as discussed above. In addition to supporting the concept of the ML pipeline by design, 6G Wireless is expected to incorporate outer semantic channels. Mimicking how our brain works, an AI native 6G wireless system could support semantic communication capabilities by design.

Space, Air and Extreme Ground Connectivity

The next generation of communication systems is expected to provide ubiquitous services in remote areas not previously served (e.g., outer space and across oceans). Such services will create a seamless integrated connectivity framework consisting of terrestrial (land-based and marine), airborne (pseudo satellites, aircraft, balloons, drones, etc.) and space-based (LEO, MEO, GEO satellite constellations) infrastructures.

The uniqueness of NTNs is in their capability to offer wide area coverage (for instance, the LEO beam footprint size ranges from 100 to 1000 km) over locations (e.g., rural areas, vessels, airplanes) that are expensive or difficult to reach with terrestrial networks. Therefore, the NTN represents a coverage extension for the terrestrial network in a global market seeing steady demand growth.

Privacy Preservation, Security Controls and Assurance

The fourth paradigm shift concerns cyber security and privacy protection. In general, 6G wireless is projected to be secure by design.

To shift from a security-enhanced network to a security-by-design system, 6G needs to integrate security at the heart of the infrastructure and instil the whole network end-to-end with a defence-in-depth strategy. Also, the standardization process for 6G must provide new mechanisms for security control, security assurance and privacy preservation.

6G wireless is expected to support, but not be limited to, the following mechanisms:

- **Zero-Trust architectures (ZTA)**: no asset is trusted implicitly, and continuous access control, authentication and identification are used.
- **Distributed Ledger Technologies (DLT)**: immutable, transparent, and autonomous ledgers using distributed consensus and cryptography provide an authoritative record of secure transactions.
- **Post Quantum Cryptography (PQC)**: creating quantum-resistant ciphers that future quantum computers cannot crack.
- **Adversarial ML**: better evaluate ML algorithm's robustness and the development of defenses against attacks.
- **Cyber-Resiliency**: continuous detection and appropriate response to adverse events, ability to with-stand attacks, autonomously evolve, and adapt to threats.

Industry players, governments, security agencies and regulators are recommended to adopt the GSMA NESAS for testing and evaluating telecoms equipment. The NESAS is an authoritative, unified, and constantly evolving security assurance scheme for the mobile industry and could be a part of certification and accreditation processes for current 5G and future 6G network security authorization in any country.

Prosumer Centric Systems

The final critical paradigm shift is that we are moving from an operator-centric system to something truly centred on the end user. The end user is expected to become a true prosumer, meaning that they will be able to create as well as consume content and information, making it available to communities of people and cyber entities.

About the Author

David Soldani received a Master of Science (M.Sc.) degree in Engineering with full marks and *magna cum laude approbatur* from the University of Florence, Italy, in 1994; and a Doctor of Science (D.Sc.) degree in Technology with *distinction* from Helsinki University of Technology, Finland, in 2006. In 2014, 2016 and 2018 he was appointed Visiting Professor, Industry Professor, and Adjunct Professor at University of Surrey, UK, University of Technology Sydney (UTS), Australia, and University of New South Wales (UNSW), respectively. Since 2018, Dr. Soldani has been contributing at Huawei Technologies as Chief Technology Officer (CTO) and Cyber Security Officer (CSO) within the ASIA Pacific Region, and, since 2020, he has been serving IMDA, in Singapore, as Chairman of the IMDA 5G task force. Prior to that he was Head of 5G Technology, e2e, Global, at Nokia; and Head of Central Research Institute (CRI) and VP Strategic Research and Innovation in Europe, at Huawei European Research Centre (ERC).

David can be reached online at https://www.linkedin.com/in/dr-david-soldani/

To Stay Safe, Companies Must Integrate the Human Element in Cybersecurity

Combatting the Unpredictability of Cybercrime with Personality Awareness

By John Hackston, Head of Thought Leadership, The Myers-Briggs Company

Not too long ago my company (The Myers-Briggs Company) partnered with ESET on a study that showed how companies are tightening up on cybersecurity in key ways, such as through compliance training and use of more complex passwords. However, many breaches have as much to do with *human error* as they do with purely technological factors, and many breaches could be avoided if organizations integrated the 'human factor' with technology-focused strategies.

For most companies, focusing on the human factor takes the form of making people aware of the various dangers that can exist and how to avoid them. But companies need to go beyond this kind of external awareness and teach employees to also look inward and develop their 'self-awareness'. This means understanding not just where vulnerabilities exist, but where employees, as individuals, are uniquely vulnerable to cybercrime.

The unpredictability component in cyber defense

Cybercrime is difficult to define because it can take almost any form, and the range of strategies that its practitioners may pursue can be as wide as the range of approaches toward building systems or software.

Cybercriminals don’t have to deal with oversight, process and policies like legitimate software developers. They can iterate with impunity and may fully embrace the latest development in fields such as Artificial Intelligence. For example, cybercriminals have started using AI to navigate security systems. Even more concerning, however, is the potential for AI to assist in exploiting human blind spots and weaknesses. To that point, we’ve seen AI used to more effectively execute social engineering attacks by using methods very similar to those used for legitimate purposes, such as recommendation engines. It has always been easier to destroy than to build, and computer systems are no exception.

An integrated strategy

One of the best ways to understand the ‘human vulnerabilities’ is to use business tools already in place to understand other aspects of human thought and behavior, such as psychometric assessments, which can help tailor training to the needs of the team. For example, The Myers-Briggs Type Indicator model looks at four dimensions of personality that identify:

- Where you focus your attention--the outside world of people and activity (Extraversion) or the inner world of thoughts and feelings (Introversion)?
- Your preferred method of information intake--gathered through the five senses (Sensing), or more abstract patterns and possibilities (Intuition)?
- How you prefer to make decisions, based on objective logic (Thinking), or your values and how people are affected (Feeling)?
- How structured you like your life to be--do you prefer to remain decisive and in control (Judging) or do you like to keep your options open (Perceiving)?

Our research shows that where we fall along these four preference pairs may influence our strengths and blind spots when it comes to cybersecurity. For instance:

- Those who prefer Extraversion (vs. Introversion) may be quick to discern external attacks. On the other hand, they may also be more vulnerable to the kind of 'social engineering' attacks that leverage manipulation of human emotions, which are becoming more deceptive and dangerous as AI progresses.
- Those with a preference for Feeling, who are guided by personal values, also tend to be more vulnerable to social engineering attacks than those who prefer Thinking (who tend to be more analytical in their approach). On the other hand, those who prefer Thinking may be prone to overestimating their own abilities when it comes to cybersecurity, which also makes them vulnerable to dangerous errors.
- Those who prefer Sensing (vs. Intuition) tend to pick up on details, and thus are more likely to recognize the minutiae of phishing attacks than those with preferences for Intuition (who tend to be more oriented toward looking at the big-picture). But they may also be more prone to taking security risks, particularly if their preference for Sensing is combined with a preference for Perceiving (which comes with a tendency to be relatively flexible, and often a little impulsive).

Cyber-criminals understand our psychology--we need to as well

In the famous (or perhaps infamous) horror film/novel "Silence of the Lambs", Hannibal Lecter was a particularly deadly foe because, in addition to being thoroughly psychotic, he was also a credentialed psychologist. As such, he knew how to exploit his victims. Likewise, cybercriminals can be very good at anticipating the blind spots of their victims. The more people are aware of their own blind spots, the better equipped they are to avoid such attacks.

Better insight into the different cyber security-related strengths and blind spots associated with various personality types can help organizations develop tighter policies and protocols. For example, employees with a preference for Intuition (vs. Sensing) may benefit from emphasizing the need to look for specific detailed cues, such as an awkwardly placed link. Alternatively, those who prefer Sensing might benefit from being trained on identifying a clue that is less obvious, such as an undue sense of urgency.

Furthermore, understanding personality type can help guide the leadership strategy used to implement cybersecurity policies. For instance, our research shows that the traditional ‘top down’ approach may not be the most effective, as at most companies any employee at any level of seniority is capable of putting the business at risk.

Integrating the best and latest technologies with a firm grasp of the human element of cybersecurity can inoculate your organization from the ever-growing list of cyber-security threats.

About the Author

John Hackston is head of thought leadership at The Myers-Briggs Company. He is a chartered psychologist with more than 30 years’ experience in helping clients to use psychometric tests and questionnaires in a wide range of contexts including selection, leadership development, performance management and team building. John can be reached online at (https://www.linkedin.com/in/johnhackston/and at our company website https://www.themyersbriggs.com/

How Cyber Insurance Can Protect Your Business from Breach of Privacy Claims

By Irena Ducic, Growth Marketer, Embroker

Every company that stores and handles sensitive customer, partner, or vendor information has the responsibility to protect that data from a variety of potential attackers. If this data is stolen or its privacy compromised in any way, the company can be held liable for such incidents.

These types of claims can potentially cost your company a lot of money, not just in settlements or damages, but also in legal fees and the recovery process. According to a report by IBM, the average cost of a data breach in 2020 was a frightening $3.86 million.

Given that 2020 brought with it an increase in remote working and online business communication as a response to the global pandemic, companies had to leverage the benefits of technology and the Internet to conduct their operations successfully. Almost 50% of businesses now use the cloud as a preferred storage option for storing classified information, and even though many do properly invest resources towards cybersecurity, there is no such thing as absolute protection from potential hackers.

Cybercrime is constantly on the rise, with predictions estimating that a business will fall victim to a ransomware attack every 11 seconds over the course of 2021. Since most data breaches are linked to human error, it's important to make sure your employees receive the necessary training to recognize and report a cyberattack.

But beyond investing in cybersecurity experts and staff education, transferring some of this risk to a third party via insurance is another very important step in your company's efforts towards managing cybersecurity risks and the many unfortunate outcomes that can arise from them; a common one being privacy liability claims.

The Dangers of Privacy Liability Claims

A data breach incident seldom affects just the breached company. Depending on the extent of the attack, it can end up affecting a significant number of other victims. The process of discovering a data breach and recovering from it is often long and daunting and it can cause severe financial losses to the breached party and everyone else affected by the incident.

Let's suppose that your company suffers a data breach that extends to your clients' records. The affected clients can decide to sue your business for breaching their privacy, which will lead to a host of expensive legal fees, potential compensation, or settlement money, as well as having to pay experts to investigate the scope of the incident and contain the damage.

Breach of privacy claims get a lot of public attention, especially long-lasting and expensive lawsuits. Even if you are a small business, the data breach could become public knowledge quickly and potentially cause severe damage to your company's reputation. All things considered, data breaches often come at a staggering price.

This is why, once again, you should strongly consider transferring some risk to an insurance carrier by purchasing an adequate cyber insurance policy to protect your assets.

What Is Cyber Insurance?

Cyber liability insurance protects businesses from the consequences of cybercrime, including cyberattacks, phishing attempts, and data breaches. It not only covers the costs of potential legal fees in the case of third-party claims against your company but also pays for additional expenses related to the cyberattack or data breach. A comprehensive cyber insurance policy could extend to provide you with the resources needed to investigate the extent of the incident and design a robust cybersecurity policy that would help prevent future attacks.

A cyber insurance policy can be split into two types of coverage: first-party and third-party. First-party coverage is designed to protect your company by covering all your losses stemming from a data breach, whereas the third-party policy covers the costs of the other affected parties, such as your clients, partners, or vendors.

Let’s have a look at what costs a comprehensive cyber insurance policy should cover:

- **Notification costs:** When a company becomes a victim of a data breach, it has the responsibility to notify everyone affected. Depending on the company’s size and the extent of the breach, this could mean a substantial amount of money.

- **Computer forensics costs:** Your chosen cyber insurance policy should not only cover all the expenses related to the attack but also help you hire experts that would look into its origin and cause and help companies minimize future exposure by implementing better security protocols.

- **Credit monitoring costs:** Simply put, your insurance policy pays for all the victims’ insurance policies. State regulators require this, and they usually ask for extensive protection.

- **Legal costs and civil damages:** A single data breach can affect hundreds or even thousands of victims, which can result in a huge number of class action claims. These payouts are often costly and it helps to have your insurance cover legal expenses, potential settlements, or awarded damages.

Specific Privacy Coverages

Your customers entrust you with their personal information and expect you to protect it from any unauthorized exposure. If attackers access this data, they breach your clients’ privacy. That usually results in class action claims against your company, which, as mentioned, could cost you a fortune. Most insurance experts recommend that businesses add specific data breach coverage to their cyber insurance policy to cover the following:

- **Data loss and recovery:** Discovering a breach and recovering from it is a lengthy process that also requires significant funds, so it’s good to have your insurance kick in and take care of it for you.

- **Business interruption and related loss of revenue:** It takes months to recover from a serious data breach and that could bankrupt your business if you aren’t making any money in the meantime. Your insurance policy would cover for lost business income while your business gets back on its feet.

- **Extortion attempts:** The attackers could ask for ransom money in order to return your data or not leak it to the public. It would be best to let your insurer handle this situation for you and decide if the payment should be made.

- **Public relations costs:** Privacy breaches could cause substantial reputational damage to your company. Your insurer would help you hire a team of experts to control the crisis and create a plan for containing the negative impact.

How Much Will You Have to Pay to Be Protected?

The price of your cyber insurance would depend on several key factors:

- **The size of your business:** The more employees you have, the greater the risk that your company falls victim to a phishing attack.
- **Industry:** Based on the industry you are in and the type of data you store, the insurer estimates your risk level. For example, someone in the healthcare industry faces a more severe threat of a data breach than someone in the business of manufacturing clothing.
- **The amount and sensitivity of data you store:** If you store sensitive personal information, health records, or payment information, you will be classified as a high-risk business.
- **Strength of your security measures:** The insurer appreciates and rewards businesses that implement strong security measures and have sound cybersecurity policies in place.
- **Annual revenue:** It is more likely that criminals would target a business that has more clients and makes more money.

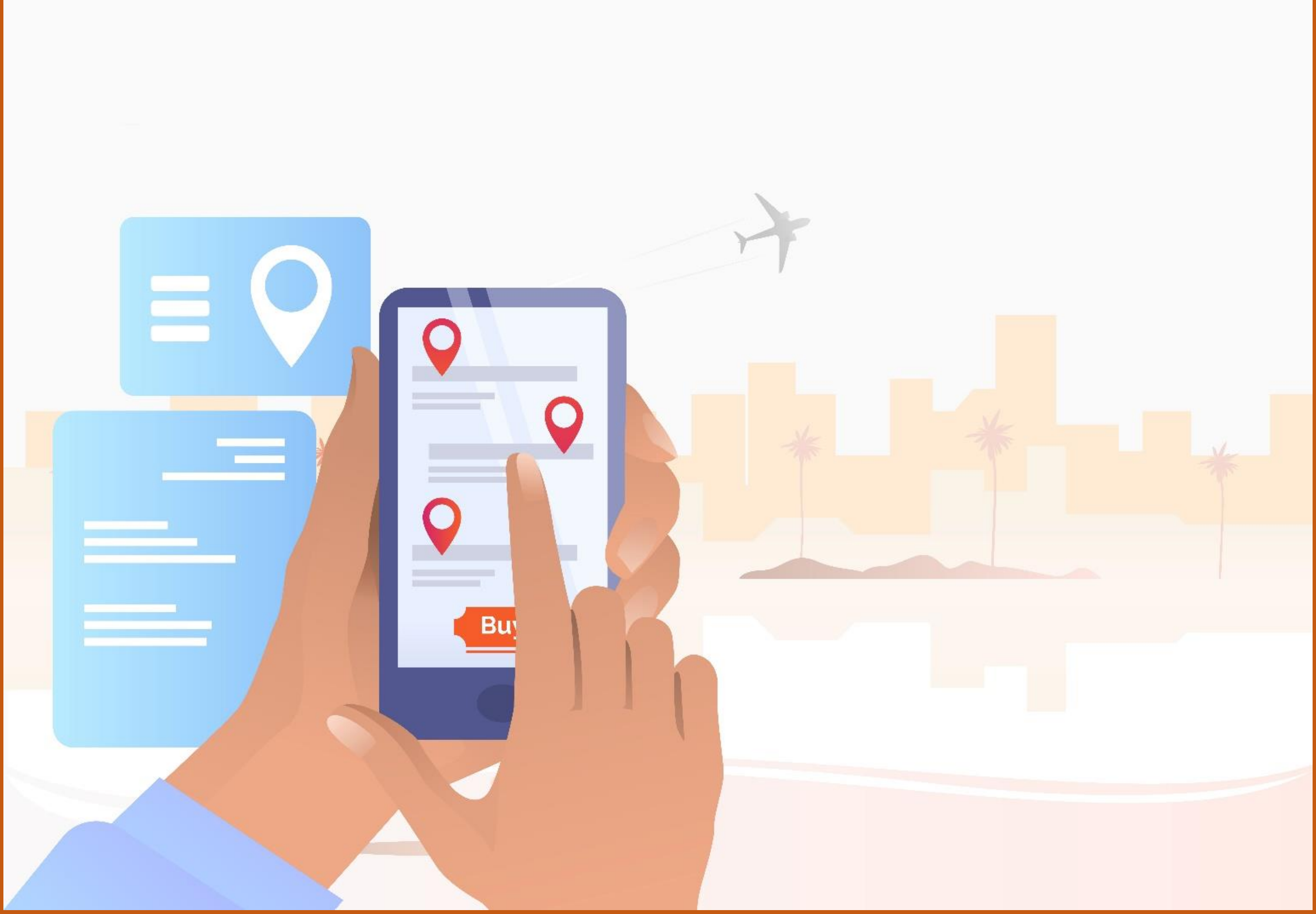
On average, a cyber liability policy in the US costs medium-sized businesses about $1,500 per year. Of course, the aforementioned characteristics of your business and others, such as the state in which you operate and the terms and limits of your policy, could drastically alter the cost of a cyber policy.

Even though a cyber insurance policy does not protect you from cybercrime, it does provide financial support that could help your company survive a potentially devastating data breach. The consequences of such incidents can sink even the strongest companies should they be left unprotected and without the financial safety net that robust insurance coverage can provide.

About the Author

Irena Ducic is a Growth Marketer at Embroker, a digital insurance company reinventing how businesses ensure they can take the risks they need to grow. Irena is a philologist by education and a great admirer of language and its value to all things marketing.

Irena can be reached online at irena@embroker.com and at our company website https://www.embroker.com/



Is Mobile App Accessibility Putting Consumers and Companies at Risk of a Hack?

By Andrew Hoog, CEO of NowSecure

Over the last few years, billions of mobile apps entered the market and more are being added every week. From banking and video conferencing, to gaming and social media, these apps have become part of everyday use, providing convenience and quick accessibility to the internet at users' fingertips. In fact, it's estimated that 69% of all digital time spent is in mobile apps, above web apps and PC apps. However, despite this "always in your pocket" convenience, security and privacy have often been an afterthought in the race for mobile app innovation.

According to a recent Gartner report, mobile app security failures are expected to be the biggest mobile threat for enterprises through 2022. Currently, about 85% of mobile apps available in app stores have security issues – some of which can be easily addressed while others more serious – and around 70% of apps leak personal information, potentially violating the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA). This puts large technology companies at the forefront to lead the charge to mitigate problems that could appear, including hardware and software issues and various security flaws. It's imperative that industry leaders develop standards and automation to address these issues and create a more secure environment, which starts with identifying the challenges.

A breakdown of risks

While the underlying architecture and design of mobile apps versus web are significantly different, both suffer from critical risks that can be broken down into four categories:

1. **Privacy:** Privacy should always be important and respected. More often than not, mobile users willingly share personal information in exchange for a free mobile app or free services without realizing the risks in their data sharing. This has led to initiatives such as GDPR and CCPA to protect mobile consumers since users typically don't understand those underlying risks.
2. **Fraud:** Fraud is another big risk to users. In fact, there have been multiple fraud-driven software SDKs found embedded in thousands of mobile apps, impacting billions of mobile users. Fraud can also be detrimental to not only consumers but enterprises. For example, when mobile apps are used for business banking, if a hacker gains access to a business user's credentials, they now have access to money and other sensitive data which could cost the entire company billions of dollars.
3. **IP theft:** IP theft is one of the biggest risks to enterprises and has a significantly growing impact in the U.S. If hackers gain access to this information, they can drain the value of the company over a long period of time, creating the most overall risk. For example, DroidCleaner, an app that claimed to clean devices of useless files and performance issues, instead collected device data, stealing contact information, login credentials and more that can then be used to attack backend systems.
4. **Espionage:** Espionage is more rare and more sophisticated, using a very targeted approach of creating a mobile app that is designed to attract millions of users and harvest person information. Due to this potential threat, a number of mobile apps, such as TikTok, have been blocked from government agency employee and military use by western governments.

It's important to understand these risks in order to create a secure mobile ecosystem, and industry, business and technology leaders should begin generating awareness about security and start building educational programs around the issue.

The importance of security standards

Security isn't a single point in time and can't be a one-and-done approach. It needs to be an ongoing process to maintain a safe environment for all mobile users and it's essential that developers build in security from mobile app inception.

Developers may not be security experts, but by creating universal industry security standards, they now have a predictable and understandable framework to incorporate security into their mobile apps from the onset of coding. Independent industry standard certification helps test to ensure those standards are met for the mobile apps the build. By combining developer standards and industry standard certifications, users are protected with a secure mobile app experience while developers and manufacturers will be held accountable for their products.

With the help of industry standards organizations, developers can learn what and how implement security into their mobile apps and then tap these certification programs. These industry-standard security certifications will also help show the value of security to the marketplace and provide transparency to users - and if a mobile app doesn't have the certification, developers will likely look to fix any issues to obtain it in order to stay competitive in the market.

While industry standard certifications aren't perfect, they do evolve over time and set a threshold that's been agreed upon by industry leaders, giving companies simple, minimum requirements to follow that from a security perspective might include end-to-end data encryption, proven cryptography, maintained and updated software SDKs, granting only necessary permissions, and implementing expiration dates or end-of-life policies.

Even a basic introduction to mobile app security will have a tremendous impact and drive change towards a more secure market. If the industry takes the time to understand the problems that are seen repetitively, they can effectively be avoided, which is why it's important that organizations that are backed by prevalent technology companies and working with industry leaders across markets are leading the charge to create and adopt standards.

For example, the ioXt Alliance is an industry-led organization that creates replicable, testable principles that address common security issues and successfully improve security for all end-users through its certification program for IoT devices and mobile applications. Being certified though the ioXt Alliance provides a continuous process where the certification status is reevaluated as new mobile app versions and updates are released into the market, ensuring accountability and transparency across all parties, and a safer environment for all mobile apps that user can trust.

With the mobile app market booming, consumers and businesses are building them quickly and using them all the time-- often without consideration of security. Because app developers are more focused on innovative features and may lack a security background, more often than not, the mobile apps that are being put in the app stores contain vulnerabilities leaving users exposed to privacy violations, fraud, IP theft and espionage. Universal standards for mobile apps are emerging to play a big role in protecting all users and creating a safer environment. Industry-backed standards organizations like the ioXt Alliance are leading the way to ensure security is built in from the onset of development and testing is done continuously, creating a critical turning point for the global marketplace and billions of users around the world.

About the Author

Andrew Hoog is a computer scientist, mobile security and forensics researcher, and CEO of NowSecure – the mobile app security testing technology company. For the past eight years, Hoog has focused solely on mobile security and regularly briefs senior government officials and top banking institutions on the topic. He's a testifying expert witness, author of two books on mobile forensics for Android and iOS, and holder of two patents in the areas of forensics and data recovery. As a former CIO, Hoog has unique insight into solving enterprise mobile security problems and is responsible for the vision, strategy and growth of NowSecure. When not breaking (or fixing) things, he enjoys great wine, science fiction, running and tinkering with geeky gadgets.

It’s Time to Issue Company Passwords Again

By Rob Cheng, Founder and CEO, **PC Matic**

The recent PC Matic Password Hygiene & Habits Report found that only 16% of employers issue passwords to employees. This is an alarming statistic given that 80% of businesses allow employees to choose their own passwords. This is risky behavior since it’s also been reported that many employees use the same password for both work and home and 50% of people have never changed their personal passwords at all.

There’s no question that poor password behaviors are putting business data at risk. The Verizon Data Breach Investigations Report has found that as many as 81% of company data breaches are due to poor passwords. If companies are allowing employees to use the same passwords across personal and business apps, they are simply asking for a breach.

This underscores the fact that employees simply can’t be trusted to create safe passwords or save them securely. The Workplace Password Malpractice Report, 2021 from Keeper found 31% of employees have used their child’s name or birthday for their password. And 49% of employees admit to storing passwords in a document saved in the cloud, while 55% save them on their phone. Thus, if a cybercriminal breaches these environments – access to both work and personal data is at the ready.

How Did We Get Here?

Prior to the internet, businesses and government institutions regularly issued passwords to employees. But with the dotcom gold rush, new personal passwords were required as we began to build our own accounts. We set up personal passwords for everything from pets.com to Facebook. Then, somewhere, somehow, someone decided that if we can choose our personal passwords, we should choose our work passwords as well. What a devastating move.

It's worth noting that the targets of cyberbreaches have also evolved. Hackers aren't as motivated to infect the individual as they are now to breach large companies and critical infrastructure. And they know they can breach these companies by accessing an individual's passwords. By hacking individual accounts via consumer-facing companies such as Equifax (consumer credit) and Twitter, they gain access to the servers of business and government. Remember, most Americans are using the same passwords at home and work.

Go Back to Go Forward

To protect corporate data, and prevent employee-enabled exposure, it's time to put password control back into the hands of IT. One of the most simple, inexpensive alternatives to password protection is for employers to go back to issuing passwords again. Company-issued passwords will substantially reduce any company's attack surface and this approach is a simple, easy practice to implement. It puts IT back in control, where stringent password practices can be implemented and monitored.

Where should we start? Email. Email access is an essential element in the hacker's playbook that allows the criminals to read emails, reset passwords, and send fake emails. Next, we should disable password-reset features for critical applications such as VPN and remote access tools such as TeamViewer and Citrix's GoToMeeting.

There are numerous sites that generate and distribute passwords via email. While the goal should be that the employee memorizes passwords, it's critical to know it is not a secure practice to store passwords in the cloud without password controls in place.

We are in a digital arms race, and currently cybercriminals are building ever more sophisticated, offensive capabilities. By taking steps to issue passwords for employee use, we can disable several tools from the cyber-attacker's playbook and place control back on IT where it belongs.

About the Author

Rob Cheng is the founder and CEO of South Carolina-based cybersecurity firm PC Matic. Rob is a world-renowned cybersecurity expert and speaker who has been featured in national outlets and publications such as Fox News Channel, The Associated Press and USA Today. Best known for his role as the spokesperson for PC Matic on a host of national television campaigns, Rob's expertise has led to PC Matic becoming a leader in the global cybersecurity market.

Non-enterprise grade communication platforms cause instability in the workplace

Non-Enterprise Grade Communication Platforms Causing Instability in The Workplace

By Nicole Allen, Marketing Executive, Salt Communications.

Enterprises require stringent administrative controls for platforms that drive mission-critical business processes now more than ever. In the age of the mobile workforce, control measures are particularly important for communication and collaboration channels, which are key drivers of operational performance.

According to a new study from Maintel, companies must learn to listen to user concerns about corporate-approved communications platforms or risk their workers using unsanctioned tools. A large percentage of workers shift towards consumer systems such as WhatsApp or Facebook Messenger for work purposes rather than business-grade resources. The way employees want to interact and the channels that are currently sanctioned by businesses are substantially disconnected.

As the workforce becomes more mobile, collaboration is more important than ever for business success. The COVID-19 pandemic has hastened the transition to remote working, which shows no signs of abating. Upwork predicted that 73% of businesses would have remote employees by 2028 in its "Future Workforce Report," while IBM predicted that the global mobile workforce would reach 1.87 billion workers by 2022. Enterprises would need purpose-built real-time communication systems that securely link workers in remote locations while allowing administrators to track and audit utilisation as the mobile workforce grows. The ability to control the lines of communications within that organisation would also be an immediate requirement.

Non-Enterprise Grade Apps can be the most common

Consumer-oriented platforms are far more common than many enterprise-grade platforms, according to respondents to Maintel's survey. This stems from the ease of use, reaction speed and collaboration. Also on the rise is the use of modern, often consumer-oriented apps. These platforms are currently, however, largely used for non-work purposes, unless it is to talk to peers.

Security threats and the impossibility of organisational monitoring mean that many of these outlets in the workplace are frequently blocked. For example, according to the study, Instagram is not approved by 41% of organisations, Facebook Messenger by 34% and Snapchat by 38%.

Many workplaces have implemented a BYOD approach which is why the above apps pose a risk. Bring your own device (BYOD) refers to a system in which employees communicate and access work-related systems via personal networks. These systems may store sensitive or confidential information from within their corporate networks. Smartphones, desktop computers, laptop and USB drives are all considered personal devices. When you utilise BYOD, your users' personal devices have less power and visibility than you would like. Employees aren't always cautious, and if they have too much data access, they might cause havoc. Even if you spend a lot of time training your employees on best defence practises, there's no guarantee that when they're stressed or busy that they'll follow the advice. Organisations sometimes need to communicate in a manner that blocks certain external apps which often isn’t possible with BYOD.

There are many reasons as to why organisations may wish to prohibit certain systems to protect their organisation, with the desire to maximise activity within the workplace, reduce expenditure and optimise their security. When workers struggle to use these resources, it's typically because their experience is inferior to that of consumer platforms; which is why we see so much use of WhatsApp and Facetime for business purposes. Employees should be consulted closely to determine what frustrations they have with current resources, and then pick and build strategies to make these platforms more appealing.

All platforms will need a policy

Businesses must also let go of the notion that just because they have a "corporate-appropriate" communications system, it can't be misused, either intentionally or accidentally. What is permissible and reasonable at work, and what is not, must be clearly stated in policies.

In addition, the reasons for these policies are to promote adherence and build greater understanding of safety among the workforce are worth explaining. Businesses can also ensure that anybody who uses their services, such as a business partner or a client, is represented with the same specific guidelines.

How to Communicate with your employees safely

Listening and reacting to your employees' feedback on existing, business-based resources is the best way to avoid pushing them into the arms of vulnerable, unmonitored consumer-focused communications networks.

Dialogue between management and employees is the most effective way to inspire staff members to use the right resources, and it can also lead to changes in practises and business-approved platforms that can enhance the user experience and make it more efficient. Regardless of which platform is used, best practises must be clearly communicated.

Enterprise communications is subject to stringent regulatory criteria in some industries. The privacy and regulatory pressures on today's businesses necessitate a strategic and measured approach to compliance. The organisation's ability to fulfil its regulatory requirements is jeopardised by lax administrative controls. Decision makers need to know that IT managers have control systems in place for effective enforcement at all times to reduce the risk of fines, penalties and most importantly when it comes to private communications; leaks.

IT teams need an enterprise communication platform with comprehensive administrative controls for controlling users, tracking operations, and implementing corporate policies in order to achieve information security, regulatory enforcement, and bottom-line business improvement.

Salt Communications works with clients all over the world who recognise the value of maintaining complete control of their confidential communications. Public leaks damage their organisation's credibility and, in some instances, jeopardise the protection of their employees and the general public. With a secure communication platform such as Salt Communications in place, you will be able to control your communications and feel safe in any situation you may encounter during your daily operations.

If you require further assistance feel free to reach out to our team for more information on this article. To sign up for a free trial of Salt Communications or to talk to a member of the Salt team, please contact us on info@saltcommunications.com.

About Salt Communications

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

About the Author

Nicole Allen, Marketing Executive at Salt Communications. Nicole has been working within the Salt Communications Marketing team for several years and has played a crucial role in building Salt Communications reputation. Nicole implements many of Salt Communications digital efforts as well as managing Salt Communications presence at events, both virtual and in person events for the company.

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

Security Issues of Working Remotely

By Pat McNamara | Security Administrator/Educator | DIYsecurityTips site owner

Beginning last near working remotely has become a big adjustment for many people. Jobs that were once confined to the office have now shifted to 100% or partially remote schedules.

The biggest concern for working remote are the privacy and security issues surround it. While a lot of people will work from home, some go out to public areas with free Wi-Fi zones. It is important to note that free Wi-Fi is quite often, insecure and unencrypted.

This poses huge risks especially when sending & receiving sensitive company data across the network. In order to maintain good network security one must be aware of the surrounding network landscape. If for example, you go to a local coffee shop to work on some projects for work and there’s free Wi-Fi, how do you know it’s safe to use? The short answer is, don’t. Free Wi-Fi is generally NOT safe and you should absolutely use a VPN to do any network related activities on your devices.

The reason for this the lack of security is that most free Wi-Fi networks are unencrypted and easy targets for attackers. It is easy for an attacker to make a fake access point using special tools. This means when you connect to the Wi-Fi you think belongs to the coffee shop it is actually is the attacker's machine. That attacker can now capture your data going through the Wi-Fi and do all sorts of bad things with it!

You can use a virtual private network (VPN) to ensure your internet traffic in encrypted, making it very hard for attackers to see what you are sending/receiving across the network. A VPN:

- Makes your devices harder to access from a remote attacker
- Allows for safe network connections in public places
- Encrypts your internet traffic so you can perform banking, financial, email tasks.

Another security concern is outdated browsers. A lot of our work is done using browser based applications and other website. There are a huge variety of web based attacks and risks. One of the most important things to remember is that you should always keep your browser updated.

You can find the update icon in the upper right-hand side of your browser window. There will be an arrow pointing up or an exclamation mark (depends on the browser) to indicate that an update is ready for download. This is usually next to the ellipses for your browser settings.

You will also want to steer clear of suspicious sites. Most sites will have a padlock next to the URL indicating that your connection is encrypted but that website can still host malware and ads. This encrypted connection doesn't mean you are free from other threats.

There are things you can do to minimize the risk of browser, network, and device threats. You can help to avoid these risks when using safe and secure practices!

- **Man-in-the-middle (MITM) attacks**

This is a very common attack most often found in free Wi-Fi zones. An attacker will position themselves on the same free Wi-Fi network and create a fake access point that looks identical to users. They might think they are connecting to "Free_starbuckswifi_2.4g" but in fact they are connecting to the attacker's machine.

From here, the attacker can capture all traffic going to and from the victim's devices. Credit card numbers, account credentials, and other sensitive data are just some of things that can be stolen.

- **DoS/DDoS attacks**

Denial and distributed denial of service attacks are designed to deny the access or function of a service, network, website, or device. Using a VPN not only encrypts your network in a tunnel but it also makes these attacks more difficult to execute.

With a VPN, your IP address is changed to another one each time it hits a VPN endpoint. This happens several times until it reaches its destination (like a web address); the attacker won't be able to attack your original device IP address, keeping your internet connection secure.

- **Data leak or data theft**

Data leak/theft occurs when an unauthorized party gains access to sensitive data or accounts. This unauthorized access can happen when someone "sniffs" your internet traffic whether through insecure Wi-Fi or other means.

Another way a leak or theft can happen is by social engineering. This is the art of human hacking; as they are the weakest links in security. A person who is too trusting working for the most secure company can be the weak link. If an attacker is a good social engineer, they can get their victim to disclose proprietary company information, names, email addresses, and more.

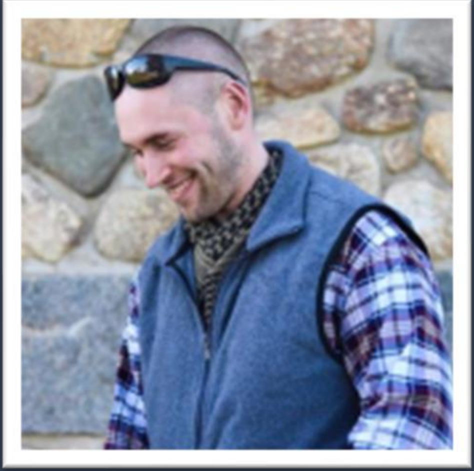
- **Browsing risks**

To lower the risk of compromising accounts, receiving unwanted downloads, or malware keep browsers updated and know the sites you are visiting. It is recommended that you copy/paste the URL of the website in question and run it through urlvoid or safeweb.norton. These websites will scan that URL for malicious activity, blacklist status, and report other metrics about the site.

Yes, this will take a few minutes by the time it's said and done, but do you really want to risk an account compromise or worse? Whoever said security was convenient? We do a lot of important things through a browser, and we should all do our best to keep them protected.

With this knowledge, you can work remotely while remaining secure. These measures can be implemented to protect your companies' data along with your own. Attacks aren't going away so it up to us to continuously practice good cyber hygiene. With a combined effort from security technologies, educators, and people willing to learn, the risk can be lowered.

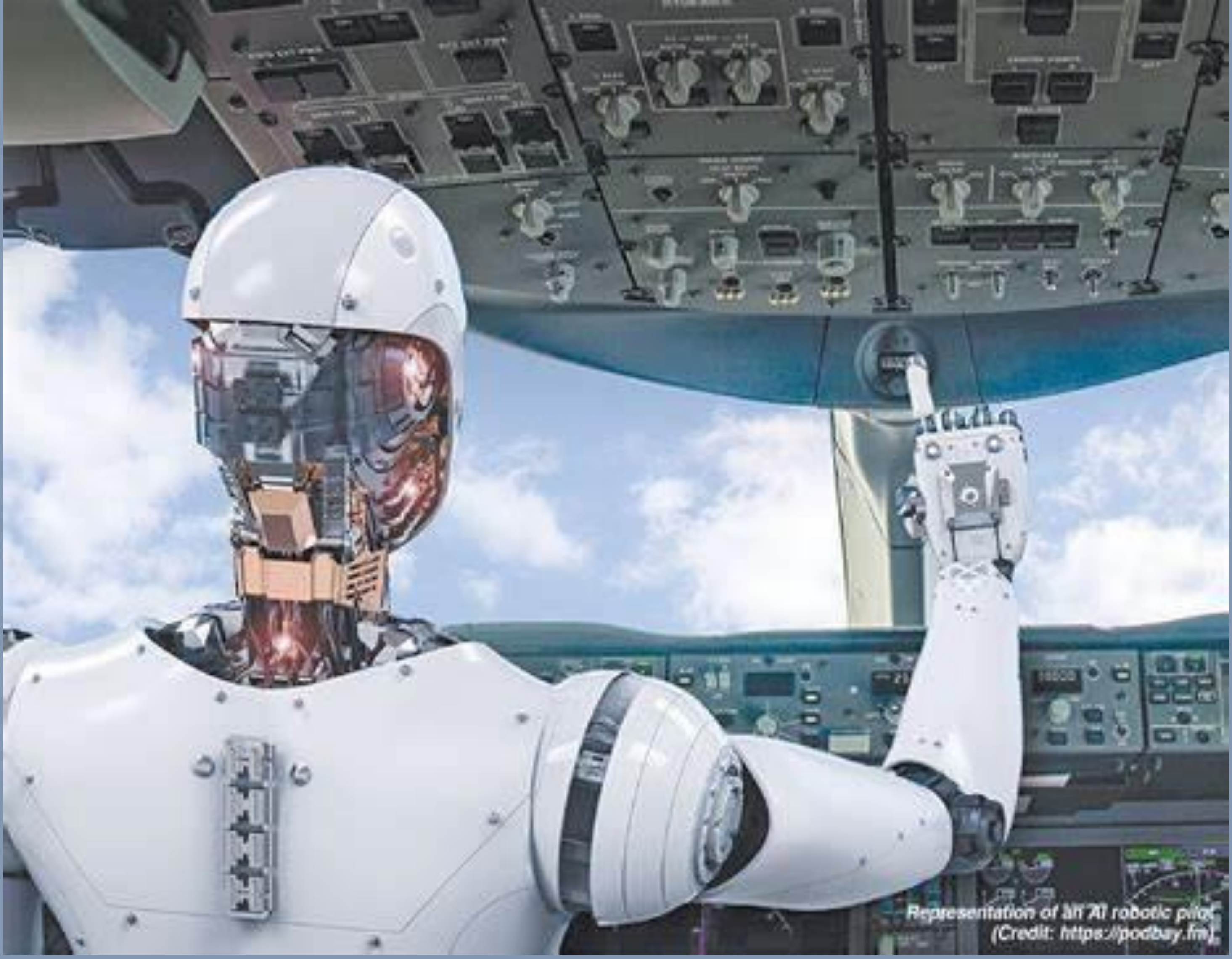
About the Author



My Name is Pat M. I am the lead writer and owner for DIYsecurityTips.com. This is a website dedicated to the security awareness education of tech users. I hold a bachelor's degree in cyber security and networks from University of Maryland Global Campus, Security+ce and GSEC certifications, and work as the Security Administrator for a Tribal Government.

Currently I am studying for advanced certifications focused on offensive cyber operations through SANS Technology Institute. When I'm not writing or working, I enjoy learning about cyber attacker methods, tools, and processes, spending time with my wife, and gaming. I also like to brush up on the basics of computing, learning new cyber tools, and completing CTF labs with TryHackMe.com. I am also extremely passionate about security and wants everyone to learn how to protect their data, maintain their privacy, and use safe security methods. This is a subject I love and I hope you can learn something!

I can be reached online at business@diysecuritytips.com, on LinkedIn, and at our company website https://diysecuritytips.com www.linkedin.com/in/👥💻🗁patrick-mcnamara-939667161



Representation of an AI robotic pilot
(Credit: https://podbay.fm)

Taking AI from Pilot to Proficiency

By Al Ford, Federal AI Alliances Manager, Dell Technologies

The Federal government is prioritizing artificial intelligence investments, and new research highlights steps to continue to move AI initiatives forward.

In March 2021, the National Security Commission on Artificial Intelligence (NSCAI) published a report recommending Federal leaders double research and development spending for AI each year, targeting $32 billion by fiscal year 2026.

Additionally, in June, the White House announced the creation of the National Artificial Intelligence Research Resource Task Force, which will write the road map for expanding access to resources and educational tools. The goal is to spur AI innovation and economic prosperity nationwide.

AI capabilities offer new opportunities to enhance operations, derive value from data, and more. One significant opportunity is the potential to use AI to mitigate cyber threats – to understand anomalies and respond quickly enough to contain a threat.

However, new research finds almost three-quarters of Federal agencies are struggling to grow localized AI projects beyond the pilot stage. A lack of AI-ready infrastructure presents a formidable hurdle, according to the study.

In a study underwritten by Dell Technologies and NVIDIA, MeriTalk surveyed Federal IT decision makers on AI plans and progress. Despite challenges, Federal IT pros are bullish on AI – 87 percent say operationalizing AI is a cornerstone to achieving a digital-first government.

Overcoming the AI Challenge

While there is momentum, 85 percent of Federal IT leaders agree government can do more to embrace AI technologies, specifically at the network's edge, where so much data is collected.

Many agencies have not taken the key steps needed to establish a foundation for widespread AI integration; citing challenges with data center-level security, power consumption, and lack of systems management expertise. The majority – 81 percent – say their agency needs help understanding what an AI-ready compute infrastructure looks like.

To move forward, agencies can evaluate their "AI maturity" and consider steps needed, which may include modernizing networks, upgrading storage capabilities, investing in high-performance computing, and expanding scalable cloud solutions, the report shared.

Additionally, agencies are evaluating the skill sets needed – integrating more data scientists, engineers, and others with AI-related expertise. Many are hosting or considering AI training courses to upskill the workforce, and working with industry partners who offer needed AI implementation and analysis skills.

AI at the Network's Edge

Federal leaders see a wide variety of applications for AI at the network's edge, including Internet of Things (IoT) deployments, intelligent video analysis, and sensor technology applications. All bring new opportunities to transform systems and Federal missions.

To continue to evolve capabilities at the edge, agencies can focus on the essentials – a comprehensive data strategy and supporting infrastructure and skillsets. This includes upgrading and rethinking storage, committing to high-performance computing, and leveraging cloud across the agency.

Unlocking AI's Potential

Federal IT leaders say their agencies are striving to achieve enterprise-wide AI proficiency in the next three to four years, citing the opportunity to improve cyber threat protection, enhance operational efficiency, and improve analytics.

Agencies can learn from Federal AI leaders whose agency's AI proficiency is "ahead of the AI curve." Their organizations report advanced data maturity – implementing agency-wide data management and governance and using data as a high-value asset (42 percent versus 28 percent of their peers).

The leaders are also significantly more likely to say that federated learning, a machine learning approach that computes at the device itself using local data, is one of their agency's top AI priorities (90 percent versus 64 percent).

The report recommends several steps:

1. Take a holistic approach to AI-ready compute infrastructure
    - Get a leg up on enterprise-wide AI proficiency. Consider storage, high-performance computing, security, networking.
2. Prioritize data management
    - Address data challenges, including data complexities and silos, and a lack of clean, usable data. Fewer than one in five say their agency's data management is completely prepared to operationalize AI.
    - Integrate agency-wide data management and governance, and use data as a high-value asset.
3. Embrace the edge
    - Address data center security concerns, power consumption/availability, and systems management.

These steps are helping Federal leaders build the foundation to expand successful AI pilots across their organizations and missions – fueling new efficiency and new possibilities.

About the Author

Al Ford is the Federal AI Alliances Manager at Dell Technologies. Ford has over two decades of sales management, business development, marketing and alliances experience in the IT solutions industry – half of which targeted Federal Government employees, including the men and women of the U.S. Military. Ford has also spear-headed new and successful approaches to reach and meet the special needs of the Federal customer and warfighter. Al can be reached online at Twitter, LinkedIn, and at our company website https://www.delltechnologies.com/en-us/industry/federal/federal-government-it.htm

To Reduce Risk, Feds Need To Reevaluate Their Cyber Toolset

By Matt Marsden, Vice President, Technical Account Management, Federal at Tanium

From SolarWinds, to JBS Meatpacking, to Colonial Pipeline and more – successful cyber breaches in 2021 have left the federal government more wary of their cybersecurity tools and practices than ever before.

In addition to the executive order aimed at strengthening the nation's cybersecurity, Kathleen Hicks, Deputy Defense Secretary, recently ordered and completed a review of the Pentagon's Cybersecurity Maturity Model Certification (CMMC) program. This effort signals a growing effort to reduce the exposure of federal and critical infrastructure systems to hacks.

To "reduce risk against a specific set of cyber threats," per CMMC, federal agencies and contractors need real-time data to make sound decisions. But, agencies often have more security tools than they actually need, and only 31% of federal cybersecurity managers are confident with their tools' ability to provide data in real-time, according to new research.

To better protect federal networks, agency IT teams should reevaluate their basic security posture and how they safeguard endpoints across the enterprise. Some of the top drivers for reducing risk, respondents noted, include compliance governance and policy, tools rationalization/consolidation, end user training, visibility across the enterprise, supply chain management, and real-time data.

The Dangers of a Distributed Workforce

In today's majority distributed workforce, where many endpoints are now used beyond the traditional local access network (LAN) perimeter, adversaries have extra opportunities to infiltrate an endpoint device that has traveled outside the safety of the office environment.

To add to this increased vulnerability, bad actors only have to infiltrate a single endpoint once. From there, they can tag along through the perimeter on that same endpoint via a VPN and move across the entire network. Due to the increase in hybrid and remote work, distributed endpoints have made it much easier for adversaries to accomplish their goals – work that was once far more labor intensive, time consuming, and risky.

The traditional approach to cybersecurity, that primarily focuses on protecting the LAN perimeter, no longer fits the bill. We need a new approach, one that is utilized effectively, keeps up with workforce changes, and protects agency data.

A majority of Federal cybersecurity managers agree – 99% said they are working to rationalize and merge their agency's security tools.

Where to Start

To begin the tool rationalization process, federal IT teams can first record and evaluate those currently employed across the enterprise. This helps the team better take stock and see which tools are being used (and for what tasks), and which are not used as much, if at all. After that assessment is completed, IT teams can decide which tools to keep, replace, retire, or merge – activities which often require financial resources, technical expertise, strategic investment, and time.

However, there is not just one way to conduct a tools rationalization process. Each agency will have to develop its own strategy based on mission, business, and security needs, but the costs – often the biggest hurdle to change – do not have to be prohibitive.

With funding from the Modernizing Government Technology Act, Technology Modernization Fund, and American Rescue Plan to help aid agencies as they complete this needed transformation, they can expect a cascade of positive side effects. A majority of federal cybersecurity managers agreed that rationalizing and consolidating their agency tools creates a positive domino effect, delivering improved utilization, increased interoperability, reduced cost, and improved functionality/user convenience.

This approach also helps Department of Defense agencies and contractors, in particular, improve their cyber maturity level – and their CMMC level status.

Big picture: we can only effectively reduce risk if we stop carrying legacy problems forward. Agencies need a new approach to grow resilient to cyber security disruptions, maintain compliance with regulations, and ensure they are receiving the best return-on-investment.

Of course, every agency will have unique needs and must understand that there is no cyber silver bullet to strengthen systems. But agency IT teams should adopt a security tool customized for a borderless environment, designed to address workforce challenges, and flexes in response to the changes agencies have, and will continue to experience.

At the end of the day, data and the endpoint devices that move, store, and utilize it are at the heart of technology, and are ultimately where federal IT teams are prioritizing their security. To achieve success, teams need a modern approach that can provide comprehensive, real-time visibility and control at scale across every endpoint on the network – regardless of where that endpoint is physically located.

Control depends on visibility, and true visibility can only come from complete – and completely accurate – data. This means leveraging a single, ubiquitous, real-time platform that integrates endpoint management and security, unifies teams, breaks down data silos, and closes the accountability, visibility, and resilience gaps that often exist between IT operations and security.

About the Author

Matt Marsden is the Vice President, Technical Account Management, Federal at Tanium. He is a career cyber professional with more than 24 years of experience working with the Federal government. Matt began his federal service in the United States Navy supporting submarine operations afloat and transitioned to Civil Service where he supported the DoD and Intelligence Communities prior to joining Tanium. Matt can be reached online at LinkedIn and at our company website https://www.tanium.com/solutions/federal-government/

What is the Main Goal of Penetration Testing?

By Glenn Mabry, Senior Instructor / Tech Researcher for Legends of Tech

Digital security is one of the top priorities for today's business world. The internet has enabled businesses to work with customers and clients all over the world – and now that remote work is becoming more common, even a company's workforce relies on their online network to share and store sensitive information.

Businesses invest heavily in their digital presence, from website design to cyber security. But when it comes to security, how can they be certain that their network is as strong as they think? For cyber security professionals, the best way to test a network's strength is with a process known as penetration testing.

What is Penetration Testing?

Simply put, a penetration test (also known as "white hat hacking") is a simulated cyberattack performed on an organization's network. A penetration tester will typically scan the network for potential vulnerabilities before trying to exploit them and "penetrate" the system.

A penetration test has two typical outcomes: either the “hacker” is successful, or the network successfully responds to stop the cyberattack. Both outcomes are beneficial for the organization, as they can inform decisions the company makes to improve their security measures.

Why Should a Company Do Penetration Testing?

Corporations can yield significant benefits from conducting penetration tests on their networks. This is mainly because penetration tests help strengthen their security network. A more robust digital security helps companies protect internal information and customer data. It can also save a business lots of money; according to IBM, U.S. companies lose an estimated $7.35 million per data breach on average!

Here are some of the other benefits of penetration testing.

Identify a System's Vulnerabilities

If a penetration test is successful – in other words, if the cybersecurity team bypasses security measures and accesses the network – a company might feel discouraged with their current system. However, this incident is a great opportunity to make positive changes. After all, in this case the “hacker” was on their side!

A penetration test allows your company to spot vulnerabilities in your system in a safe, consequence-free environment. If you take the information from this test and work with your cybersecurity team to design new measures to address these vulnerabilities, you can get a better system for the future.

Reduce Network Downtime

The fallout from a cyberattack can be varied. Sometimes, the hackers steal customer data. Other times, they install malware that harms your network on a greater scale. But whatever damage you experience, the result is the same: you’re going to have to take down the network while you assess and repair things.

However, if you regularly conduct penetration tests (at least once or twice a year), your network will likely require less repair or maintenance. This means you’ll be able to fix your network quickly after an incident – or better yet, your network will prevent the attack from being successful!

Help with Regulatory Compliance

There are many standards and regulations in place to protect data across different industries. If you work in commerce, you’re likely beholden to the PCI DSS (Payment Card Industry Data Security) standard. If you work in healthcare, you’re legally required to comply with HIPAA regulations.

Whatever standard your industry uses to protect customers or clients, you can use penetration tests to guarantee that your business complies with these requirements. Industry compliance is very important, as it helps you avoid regulatory fines, possible lawsuits, and many other issues that can harm your business.

Protect Company Reputation

Regular penetration tests don't just protect you from fines or legal action. They can also improve your reputation with the public! Customers expect businesses to protect their personal data, especially when it comes to things like credit card purchases or medical records. If your business is transparent about penetration testing and network improvements, customers will know that you take their data privacy seriously.

Mitigate Damage from Cyberattacks

Finally, let's discuss the most important benefit your business will get from penetration testing: a way to mitigate damage when a cyberattack inevitably hits your network! Experts estimate that there are 2,200 cyberattacks that occur each day – and that means one will eventually reach your business.

However, if you've been doing regular penetration testing on your network, bad actors will be less likely to do real damage when they try their attack. Your cybersecurity team will have created a strong, robust network that can stand up to all manner of cyberattack, and that means your business and its data will be safe.

Types of Penetration Testing

Clearly, penetration testing is an important part of cybersecurity – but what type of test is best for your business? Here are the primary types of penetration test that your business can use to assess your security measures.

White Box

In most cases, the individual doing your penetration test will be an employee of your company, which means they'll have full knowledge of how your system works and access to it. This is called a "white box" or "glass box" test, because the hacker already has the knowledge he or she need to understand the system.

In white box testing, the cybersecurity professional isn't exactly trying to breach the company's network. Instead, he or she is doing an in-depth audit on the network, looking for any potential vulnerabilities that a hacker could exploit. This type test is ideal for companies that want a very thorough assessment of their digital security.

Black Box

In the event of a real cyberattack, your hacker likely won’t know have much information about your specific system. So, if you want to test your security against real-world circumstances, you’ll want to conduct a black box test.

These tests require a high degree of technical skill, and they often yield especially useful insights about flaws and vulnerabilities you might have overlooked in your system. However, they are also a “trial and error” style of test, which means they don’t always find every possible flaw in your system.

Grey Box

If you want the best of both worlds for your penetration test, you’ll want to consider a “grey test.” In this instance, the hacker will have partial knowledge of the network, which allows him or her to conduct a thorough test while still mimicking real-world circumstances. This will allow you to fill in any gaps in your security system.

About the Author

Glenn Mabry is a senior Instructor / Tech Researcher for Legends of Tech. With over twenty years in the industry, Glenn is a tech expert with experience in cyber security, data science, cloud, networking, coding and more. Legends of Tech is a technology training network that gives the industry's top Subject Matter Experts the ability to showcase their skills and learners the advantage of staying ahead of the extremely fast-paced industry.

Who’s Responsible for social media Public Safety?

By Darren Millar, senior vice president, operations, PiiQ Media

Social media is firmly embedded in our society at this point – and there’s likely no going back. It’s here to stay, and it’s increasingly part of our daily lives. The use of social media is generally an innocuous activity; you share photos and memes with friends and family or to easily spread the news to your network when you get engaged or start a new job. Unfortunately, for all of the benefits that social media brings (connection, communication, information), it also comes with dangers that can’t be ignored.

We’ve all heard and seen stories about children being lured by predators online, scams and fraud being perpetrated, of course, but social media can also have a far wider-reaching impact on not just individual safety but the safety of the greater population.

One word: Misinformation

Social media tends to create siloes at best and echo chambers at worst. People rely increasingly on social media as their primary source of information – but they also have a tendency to stay focused on the groups and sources that are similar to them or that are most likely to reinforce what they already think or believe. And this enables misinformation or just plain falsities to run rampant.

A 2019 study published in Science by MIT Sloan professors found that falsehoods are “70% more likely to be retweeted on Twitter than the truth and reach their first 1,500 people six times faster.” It’s not just people spreading this misinformation but bots, too. Researchers found that in polarized Twitter networks, which represent the highly polarized nature of America at large, a few bots "are able to shift a disproportionate number of people over a threshold" to take on a new opinion or take actions like joining a protest. "When it comes to bots in a polarized network, a little bit goes a long way," one researcher observed.

Desperately seeking fame

Andy Warhol's famous declaration that "in the future, everybody will be famous for 15 minutes" may have been more prescient than anyone could have imagined. The rise of social media has also led to the rise of social media stars and "influencers," which in turn has galvanized the desire for fame in many more people. And there are some who would do almost anything to get those coveted 15 minutes. That includes making outlandish or provocative claims or intentionally spreading disinformation just to increase the number of social interactions.

The impact on public safety

One of the most recent, relevant examples of how misinformation has directly impacted public safety is the spread of false information related to COVID-19. Multiple studies have found that misinformation on social media played a huge role – and continues to do so – in eroding the public's trust in officials, seeding doubt, disseminating conspiracy theories and much more.

There's also the potential for the online equivalent of yelling "Fire!" in a crowded theater, where someone can cause mass panic by spreading misinformation, rumors or just plain lies. Some platforms have had to start cracking down – but often, the damage has already been done. For instance, YouTube removes videos that violate its COVID-19 policy, but other platforms have less stringent policies.

Another example is when people put themselves directly in harm's way for the purpose of promoting the event on social media. Not only can that put the individual in danger, but it also can potentially endanger the citizens or law enforcement members who step in to try to help or protect them.

Proceed with caution

The unfortunate reality is that there's a darker side to social media use. In certain cases, it can actually create threats to individual and large-scale public safety and security. This problem isn't going to be solved overnight, as the ongoing congressional hearings indicate.

Individuals need to take precautions about how they participate in social media, though that's certainly easier said than done. Confirmation bias typically causes people to seek out and spread information they already agree with and ignore the rest. This can lead to their unwitting participation in social engineering – and, if a social platform deems the information untrue or harmful, the person risks being banned.

In addition, even sharing what seems like harmless personal details can put individuals at risk from hackers who scrape social accounts for such details. The National Cybersecurity Alliance offers a list of tips that anyone can use to stay safer when using social media. These include creating separate passwords for each social account keeping security software updated.

But the onus isn't just on individuals; the platforms bear a lot of responsibility, as well. And slowly, we're seeing a certain degree of accountability, but there's a long road ahead before the gray area encompassing constitutional free speech and the role of private companies can be divided into black and white – if that's even possible. Until roles become clearer, caution and clear thinking are advised all around.

About the Author

Darren is a Law Enforcement veteran investigator who specialized in Cyber Special Operations and Open Source Intelligence. He has worked on some of the most high-profile investigations over the last 20 years within Europe and was an integral part of an elite unit responsible for over 200 global internet investigations in two years. He has also conducted special operations for major global events in the last eight years including the Olympics, and Global summits. Darren has consulted in North America with major Law Enforcement Agencies assisting them with cyber special operations policy, procedures and tactics. In his spare time Darren is a keen sportsman and writer. Darren can be reached online at https://www.linkedin.com/in/darren-millar-22479394/ and at our company website https://www.piiqmedia.com.

5 Tips to Prevent a Security Breach- Looking At Security From The Inside

By Mackenzie Jackson, Developer Advocate at GitGuardian

In recent years we have seen many new trends within security, this includes the concept of Shift Left, bringing security earlier in the development lifecycle and DevSecOps, the concept of tying together development, security and operations. Despite these shifts, security breaches still play a prominent part in our daily lifecycle and this leads us to ponder the question: **Is it actually physically possible to stop breaches?**

There is of course some debate on this. Katie Arrington, CISO for acquisition and sustainment at the pentagon was addressing contractors when she had them repeat after her ***"We are all going to get breached"***. While fearmongering and hyperbolic statements about cybersecurity are certainly exhausting, what security professionals know all too well is that the risk of a data breach can be reduced but we will never be able to get it down to 0%.

Does this mean we don't care about small incidents? No of course not, we must continue our effort to ensure attackers don't gain any access into our systems, but the point is that on top of that, we also need to be able to control where an attacker can go, if an incident occurs and we need to be alerted to it.

In this article, we will run through tips and tools that we, as developers and security professionals, can adopt to help not only prevent incidents but also prevent incidents turning into breaches. For this, we need an **inside-out approach**. What do I mean by an inside-out approach?

Assume insiders are a threat

This does not mean we should be suspicious of all our employees and become paranoid about who in the team may be a malicious actor. Instead, it is to take the approach of assuming that our internal accounts and networks can be breached and an insider is simply someone that has access to our internal systems, **even if they have accessed them through malicious means.**

Often we think about building security like we are building a giant wall around our infrastructure and our assets, this is sometimes referred to as the *wall and moat approach*. We can spend all our resources and time trying to secure this wall, this means our security defense is built with a single belief at its core:

No one on the outside can get in and insiders are not a threat.

Of course, it seems logical to think like this, but the result is that when our security wall is breached because we cannot guarantee we won't be, it violates the core assumption our entire security plan was built around, leaving us defenseless against insider threats. This allows an attacker to move laterally between our systems, services and infrastructure. Ultimately an incident turns into a breach.

We need to build security that assumes that insiders are a threat, this requires a change in thinking and ultimately an additional layer of security. In other words, we need to implement a zero-trust environment. Zero-trust security is a guilty-until-proven-innocent approach to network security that John Kindervag - formerly a principal analyst at Forrester Research and now CTO at Palo Alto Networks - first articulated in 2010. I advocate that its principles can extend past network security and into application security.

Okay sounds good, how do we actually achieve this though?

Had enough theory? Let's look at practical steps we can take to make this a reality.

- **Don't leave secrets in internal systems.**

There are many examples of breaches that originated with secrets such as credentials discovered in public spaces, such as GitHub. But what about internal systems? This is a great example of where security built on the concept of a fort around internal systems can fail. Code is a leaky asset and you can find secrets anywhere code is copied, git repositories, internal wikis, messaging systems etc. All of these systems are high-value targets for attackers. It only takes one compromised account to your internal git repository for an attacker to run a scan through its history and uncover a trove of sensitive information. These secrets can be used to move from git repositories to infrastructure and services.

Internal systems need to be cleansed of sensitive information like secrets. How? Well, secrets can be buried deep in history long forgotten or in debug logs making them very difficult to find. There is also a lot of information constantly running through these systems so checks need to be programmatically added to the development lifecycle.

Secrets detection can be added in two places, on the client-side, for instance as a pre-commit hook on a developer's machine, and on the server-side, after a commit has been made. Server-side detection is essential because you cannot rely on the fact that the client-side detection is not bypassed. But of course, the ideal scenario is that secrets do not make it to the server in the first place. In security we strive for the ideal scenario and plan everything else. Client-side detection can be made by using CLI secrets detection such as GitGuardian-shield which can be installed on developers' machines to catch and prevent secrets from being committed into version control systems.

- **Default to minimal permission scope for API keys and services**

Let's imagine that an attacker has been able to compromise your defenses and correctly authenticate themselves to your internal systems. This activity can be very difficult to detect as they appear to be valid users. By restricting access to services and reducing permissions to services and API keys for the minimal scope possible, you not only limit damage and restrict lateral movement, but you also provide greater visibility over when an API key is being used outside of its scope (by having the proper logging systems in place).

Default to minimal permission scope for APIs

When using external services, make sure the permissions of that API match the task it is fulfilling. This includes making sure you have separate APIs for read-only and read/write permissions as needed. Many APIs also allow you to have increased control over what data can be accessed, for example, the Slack API has a large range of scopes, using these scopes to meet the minimal requirements of the task is important to prevent an attacker from accessing sensitive data or moving laterally through systems. It is common for inexperienced developers to use master APIs allowing them to use one key throughout all their projects. But this increases the potential damage of a data breach.

Whitelist IP addresses where appropriate

IP whitelisting provides an additional layer of security against bad actors attempting to use APIs nefariously. By providing a whitelist of IP addresses from your private network, your external services will only accept requests from those trusted sources. It is common to include a range of acceptable IP addresses or a network IP address.

Network and service segmentation

Network and service segmentation is a highly effective strategy to limit the impact of network intrusion. So how do we restrict which services are allowed to talk to which services?

Network segmentation

Each host and network should be segmented and segregated at the lowest level that it is practical to manage. For a physical network, routers or layer 3 switches, divide a network into separate smaller networks using measures such as Virtual LAN (VLAN) or Access Control Lists (ACLs). Network firewalls are implemented to filter network traffic between segments, and host-based firewalls filter traffic from the local network adding additional security.

If you are operating in a cloud-based environment, network segmentation is achieved through the use of Virtual Private Clouds (VPC) and Security Groups. While the switches are virtualized the approach of configuring ingress rules and ACLs to segment networks is mostly the same as physical infrastructure.

Service segmentation

If you consider that network segmentation is concerned with securing traffic between zones, service segmentation secures traffic between services in the same zone. Service segmentation is a more granular approach.

Implementing service segmentation depends on your operating environment and application infrastructure. Service segments are often applied through the configuration of software firewalls, software-defined networks such as the overlay networks used by application schedulers, and more recently by leveraging a service mesh.

Like network segmentation, the principle of least privilege is applied and service to service communication is only permitted where there is an explicit intention to allow this traffic.

• Always encrypt data in transit and at rest

Data in transit, or data in motion, is data actively moving from one location to another such as across the internet or through a private network.

Data at rest is data that is not actively moving from device to device or network to network such as data stored on a hard drive, laptop, flash drive, or archived/stored in some other way. Data protection at rest aims to secure inactive data stored on any device or network.

Understanding that data in transit needs to be encrypted and protected is intuitive because the data is leaving the safety of the 'security fort'. But data at rest is an area where we again can fall victim to the assumption that because it is safely stored behind our fort it is not an issue.

Data at rest is stored physically, not in words on paper, but in a physical hard drive. We can be so focused on preventing cyber threats that happen in the cloud that we can overlook where the data is, physically, when it reaches its destination. This is why it is crucial to encrypt data when it is at rest so a malicious actor cannot gain access to it even in the case of a physical theft. Data that is stored in the cloud is also not exempt from this, *as I have to remind my Mum,* ***the cloud isn't a cloud, it is just someone else's computer you are borrowing*****.** How data is stored and the encryption method used is an important question to ask when deciding on a cloud storage solution, according to McAfee, only 9.4% of cloud providers encrypt their customer's data at rest. Data security on the cloud is a shared responsibility between you and your cloud provider and you, the customer, need to be in sync with the security your cloud provider does and does not grant.

Another mistake is using poor encryption protocols and hashing algorithms to protect sensitive data. The biggest example is the still widely used MD5 hashing protocol for protecting passwords. Now, hashing is different from encryption because it's a one-way function, meaning you can check if a password matches a hash but cannot reverse it. But due to an increase in computing power, it now only takes minutes to decipher MD5 hashes. The moral of this is that encrypting data at rest is not just a matter of encrypting data and then ticking the box. The encryption algorithm must equal its purpose and is a consideration that needs to be revisited as new technologies emerge.

• Keep your dependencies up to date

In modern software development, we rely on many different external building blocks and this creates a relationship of trust between our application and the services or dependencies it is using. The problem is these dependencies can be vulnerable to attacks, which means our application might also be vulnerable to these attacks.

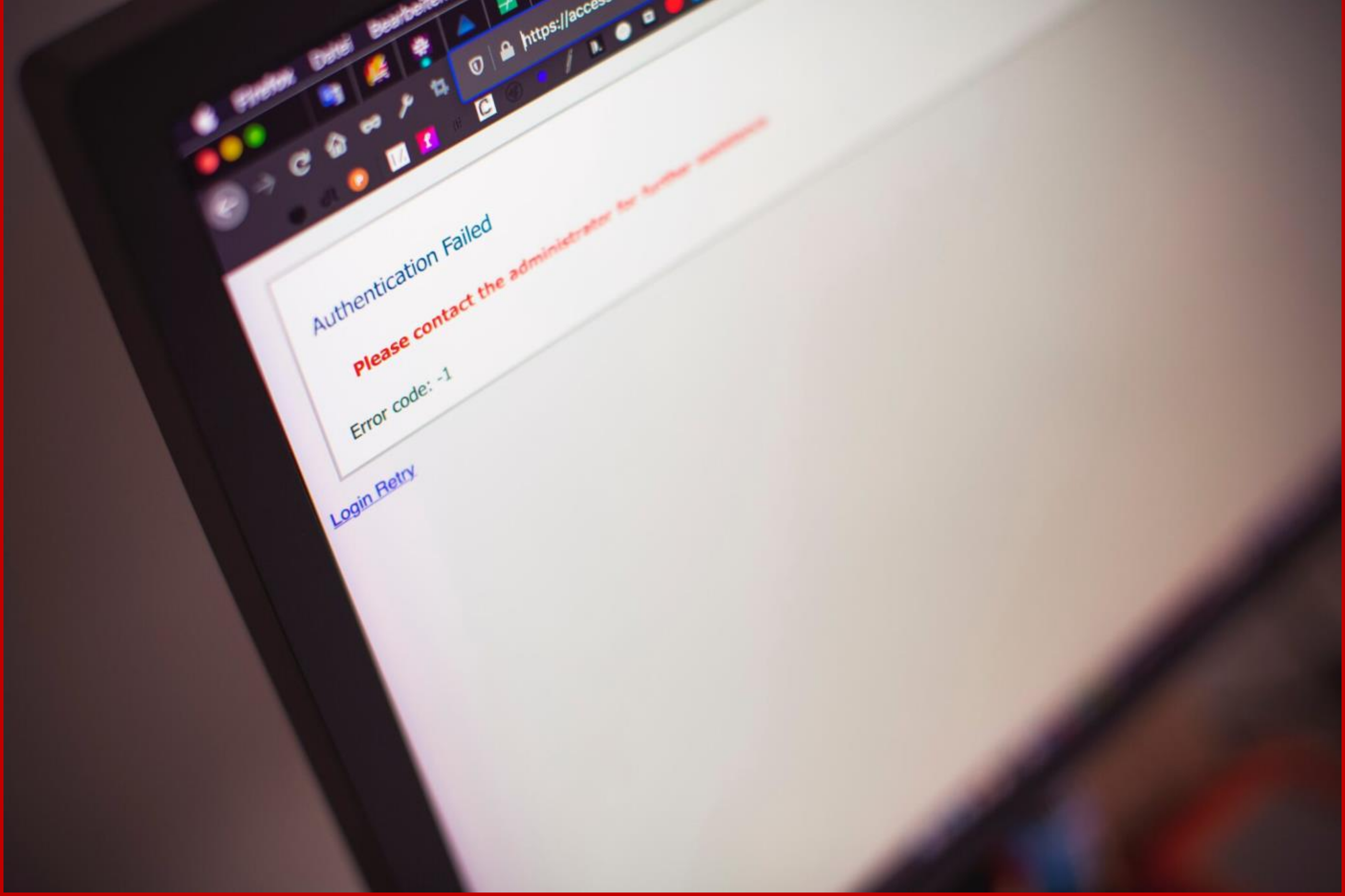
What makes these particularly harmful is that if your application is using a dependency that has a reported vulnerability, the details of that vulnerability are made public, usually after a patch is released. If you are using outdated dependencies, in many ways you are giving an attacker instructions on how to exploit your application. This is why dependencies should always be updated regularly. A challenging job when you consider that you may have thousands of different dependencies that may themselves have dependencies. Like secrets detection, this is another job for automation. Tools like Snyk and even GitHub, provide the ability to automatically check if dependencies are out of date and can automatically submit a pull request to update them.

Wrap up

Some of these may be obvious, we must remember as developers and security professionals to always build solid foundations of our security, this means apply thought to even obvious scenarios. It is always an interesting exercise to look at security from the inside and ask yourself that if someone was able to correctly authenticate themselves into your internal systems, could you detect them and could you stop them.

About the Author

Mackenzie Jackson is the developer advocate at GitGuardian, he is passionate about technology and building a community of engaged developers to shape future tools and systems.



Authentication Failed

Please contact the administrator for further assistance

Error code: -1

Login Retry

Maturity-Based Approach vs. Risk-Based Approach: What's the Right Answer?

By eSentire

The influx of cyber attacks within the past few years have painted a dire image for the C-suite and the boardroom. As cyber risks grow in number and complexity, business leaders are left wondering just how effective their security programs are. After all, we've heard it many times before: cybersecurity is not an IT problem, it's a business risk to manage.

There are many approaches to developing and managing a cybersecurity program. Currently, the rousing debate within the security industry appears to center on these two options: should organizations adopt a maturity-based approach or a risk-based approach?

The traditional approach to managing cyber risk is maturity-based, wherein organizations aim to achieve a desired level of maturity by implementing certain capabilities and controls. This approach is lauded as the industry favorite and paves the way for an organization to demonstrate the controls and defenses it has built based on standard industry framework, such as the Cybersecurity Maturity Model Certification (CMMC). To demonstrate a specific level of maturity, organizations must fulfill specific requirements outlined by the industry framework, such as:

- Implement phishing training exercises or conduct regular executive awareness briefings for security awareness training
- Enabling multi-factor authentication (MFA) and a strong password etiquette to demonstrate they are adhering to best practices for identity and access management

However, one drawback for some organizations is that maturity models may require a hefty financial investment if the focus is placed on building a multi-layer of defense against everything.

A risk-based approach, on the other hand, allows business leaders to prioritize "building the appropriate controls for the worst vulnerabilities, to defeat the most significant threats". Risk-based approaches tend to be significantly more cost-effective than maturity models since business leaders have the option to invest heavily in defenses for the vulnerabilities that affect the business's most critical areas.

A 2019 article by McKinsey & Co. argues that a risk-based approach is an advanced stage in an organization's cybersecurity journey, whereas a maturity-based approach is still foundational. Rather than chase maturity, business leaders should look inward to identify the set of gaps and critical vulnerabilities identified for their specific business and mitigate those first.

For example, if you identify that the end users in your organization are the weakest link (as is normally the case), you may want to go beyond conducting phishing training or sharing threat advisories to mitigate that risk. Under the risk-based approach, you would implement those practices *and more*, such as providing simulations and training sessions on good cyber hygiene and how to stay safe online. These additional activities might not be a priority for CISOs who are more concerned with checking off the requirements of a maturity model.

So the question remains, which approach should business leaders rely on to develop their security program? The reality is that while there isn't a definitive answer that can apply to every type of organization, there is merit in using a risk-based approach since it is geared specifically toward mitigating gaps and vulnerabilities, which can significantly help in reducing cyber risk.

To be successful in using a risk-based approach, here are some questions you can ask yourself:

1. **Does my executive team accept that cyber risk is an enterprise risk?**
   Many business leaders may consider cyber risks completely separate from other enterprise risks. Given the evolving threat landscape and acceleration towards digital transformation, this is a luxury.

2. **What are my business' "sources of value" and do I understand the specific risks that can impact those sources of value?**
   Every business has its own set of processes or workflows that are integral to business operations--these are the 'sources of value'. Retail businesses, as an example, must have a point-of-sale system in their storefronts and an online payment processing portal for e-commerce. Each value source comes with its own enterprise risk. Adversaries can inject malicious code within your website to steal your customers' credit card information. So, you must understand the specific sources of value for your business and/or industry, and map each to an enterprise risk. Only by doing this will your team be able to gauge the best way to protect your data.

3. **Have I identified all potential vulnerabilities that can impact my organization today?**
   Since your organization's attack surface is continuously evolving, you must have a deep understanding of any vulnerabilities--especially those tied to a value source--that can impact your organization. Once these vulnerabilities have been identified, you can create a roadmap to establish the protocols and controls needed to fix the vulnerabilities.

4. **Do I know the specific TTPs (threats, tactics, and procedures) that threat actors can use to target my business?**
   Based on the industry in which your business falls, the size of your team, and the type of data you have access to, your organization will face certain TTPs that another organization may not. TTPs also vary based on the software applications and tools used by your organization.

   Insurance firms may have access to financial and medical records and government-issued identification for their clients, whereas banks may only hold financial records for their customers. So, it's critical to identify the specific TTPs that any threat actor can leverage against your organization (i.e., which vulnerabilities are they most likely to target, what are the attack vectors commonly used, etc.) and identify controls to close those gaps.

5. **How am I planning to address the vulnerabilities that were discovered?**
   Once you've worked with your security provider to discover all vulnerabilities, you'll find that either you already have certain measures in place to fix them outright, or that you need to establish a new set of controls altogether. Perhaps it's a mix of both. Either way, you can now work to set up a roadmap to ensure that you've addressed all critical vulnerabilities and work cross-functionally with various teams to determine which controls are working and which controls aren't working.

As it stands today, it's inherently more difficult for organizations to get away entirely from maturity models since mapping processes and procedures to an industry framework is a standard practice within cybersecurity. However, it's also unwise for business leaders to focus so heavily on achieving a certain maturity level that they overlook reducing enterprise risk.

"Business leaders need to make sure that they are cyber risk aware and focused on reducing their cyber risk instead of focusing on a model that pushes towards a certain level of maturity, which can result in a roadmap they are forced to align to amidst a changing threat landscape," Tia Hopkins, VP, Cyber Risk Advisory and Solutions Architecture, states. "When you end up chasing a maturity model, you might have a scenario where you're focused entirely on implementing certain tools and technologies, when in reality the largest area of concern might be the users, which means the focus should have been on endpoint prevention and response or security awareness training."

The attack surface is ever-changing, and the threat landscape is continuously evolving. Ultimately, the goal for any strong cybersecurity program should be to continuously assess and reduce cyber risk.

To learn about the eSentire Cyber Risk Advisory program, please connect with a security specialist today at www.esentire.com

To learn more about how your organization can transition to a risk-based approach, please join us at Tia Hopkins' session on Quantifying Cyber Risk on August 5, 2021 (11:30am - 12:20pm EST) at Black Hat 2021.

About eSentire

eSentire Inc., is the Authority in Managed Detection and Response, protecting the critical data and applications of 1000+ organizations in 70+ countries from known and unknown cyber threats. Founded in 2001, the company’s mission is to hunt, investigate and stop cyber threats before they become business disrupting events. Combining cutting-edge machine learning XDR technology, 24/7 Threat Hunting, and proven security operations leadership, eSentire mitigates business risk, and enables security at scale. The Team eSentire difference means enterprises are protected by the best in the business with a named Cyber Risk Advisor, 24/7 access to SOC Cyber Analysts & Elite Threat Hunters, and industry-leading threat intelligence research from eSentire’s Threat Response Unit (TRU). eSentire provides Managed Risk, Managed Detection and Response and Incident Response services.

For more information, visit www.esentire.com and follow @eSentire.

Discovering Unknown Botnets with Command-and-Control Communications Analysis

By Howie Xu

Cloud-edge-based proxy security services like the Zscaler Zero Trust Exchange rely on Machine Learning models to detect, identify, and block malicious traffic. Zscaler (my employer) processes more than 160 billion data transactions per day, the vast majority of which are quickly recognized as benign. But it's the minority of remaining traffic (still a huge volume) that demands further analysis: How do we ensure nothing bad gets through?

Detection starts with domain analysis

Our Machine Learning-based traffic analysis begins with domain reputation assessment. (I wrote about that first-stage, lightweight model here.) Traffic emanates from domains. There are known and good domains and those are easily recognized. (For instance, BBC.com would be categorized as "News & Media.") However, data invariably arrives from new or unknown domains ("Misc/Unknown" category), and some portions of those can be malicious.

Here at Zscaler, we use unsupervised learning on those Misc/Unknown category URLs. (More on that in my earlier article.) We calculate a domain-reputation score based on components like lexical analysis, referral and sequence, popularity, and ASN/WHOIS reputation. From there, Machine Learning algorithms adjust score weights to ensure final reputation scores follow a Gaussian distribution. This approach “clears” much of the data traffic for safe passage, but identifies a smaller number of “suspicious” domains requiring further attention and deeper analysis.

In this article, we’ll do a deep dive on one critical analysis we perform on those unknown data sources: deconstructing communication methods to detect previously unknown botnets.

All about bots, botnets, and command-and-control communications

A **botnet** is a series of machines or devices, all connected together, with each running one or more automated scripts (or “bots”). Often, this network of bots is composed of compromised machines, effectively hijacked to work in tandem to launch cyber attacks via remote control. Botnets can be used to perform Distributed Denial-of-Service (DDoS) attacks, exfiltrate data, or send spam. The attacker controls the hijacked botnet device and its connection using command-and-control (“C2”) software.

Threat actors mask botnet activity to evade detection. Data traffic from recognized botnets can be blocked. Unknown botnets, as the name suggests, are those for which security experts do not yet have a recognizable “signature” for detection. As more and more botnet-launched attacks succeed, more and more new botnets pop up, and the harder it is for security experts to keep up.

Machine Learning offers great promise for detecting unknown botnets. Machine Learning technology can be applied to identify unknown botnets based on their network communication, specifically by detecting the C2 channel for the new botnet.

Command-and-Control channel detection is a supervised training exercise with multiple steps, including data collection and labeling, feature engineering and modeling, and human-in-the-loop and lab testing.

Data collection and labeling

A supervised learning framework needs data and associated labels. For Zscaler, the data is the 160 billion transactions it manages per day generated by its diverse customer base. As for labels, Zscaler maintains a large botnet and non-botnet domain/URL database, employing its domain “verdicts” as labels for Machine Learning model training. The domain/URL verdicts derive from various sources, including third-party threat intelligence feeds, Zscaler sandbox infrastructure, and human reviews.

Feature engineering and modeling

Detecting a botnet’s C2 traffic is challenging: It’s typically low in volume, and threat adversaries disguise it to look like normal traffic (e.g. sent to a seemingly reputable destination). Machine Learning models work most effectively when they are based on established heuristics or rules -- this enables data scientists to better leverage their own intuition.

It’s not quite that straightforward when we’re dealing with Command-and-Control traffic analysis. But looking at *multiple* aspects of network transactions with some rich context can deliver effective detection. Here at Zscaler, we examine network transaction domain details, including hostname, associated IP address, full URL string, user-agent string, and many more.

We extract the features based on spatial-temporal correlation over time among the network transaction domain hosts/users/companies. (In Machine Learning parlance, the “feature” is the useful and informative data “extracted” from the original network data transactions.) In this way, feature engineering is done by correlating the network events across time (temporal) and across the hosts, users, and companies (spatial).

For example, a botnet-infected host might trigger several different DNS requests to ping for a C2 server before establishing communication with it. In some cases, that behavior might appear normal if compared to a baseline associated with that particular host, but unusual if compared to the baseline established from a larger population of hosts.

After the features are obtained, we then train a tree-based machine learning model for each aspect (e.g., hostname-based transaction patterns, IP-based transaction patterns, URL, user-agent, etc.) and combine them together to produce a final prediction. (See Figure 1.)

Why not stack all the features together into a single predictive model? First, empirical evidence suggests that the “ensemble-type” architecture achieves higher accuracy. Second, the ensemble approach helps with the prediction’s “explainability”: When the model makes a positive prediction regarding a particular transaction related to a particular domain, we can assess each individual component score output by submodel and understand the logic behind the prediction.

Table 1 below shows the example of a positive prediction by the Zscaler model and its corresponding scores output by each of the submodels. The scores are in the range from 0 to 1, where the higher value indicates the more suspicious. In this particular case, the model called out the domain c8dd8ae6dc4dc644[.]xyz because the URL looks very suspicious -- the URL score is very high -- which somewhat matches with the human impression.

Domain	**Hostname-based pattern score**	**URL score**	**IP-based pattern score**	**User-agent score**
c8dd8ae6dc4dc644[.]xyz	0.36898	0.99981	0.74281	0.088025

Table 1: A positive predicted domain with associated submodel scores

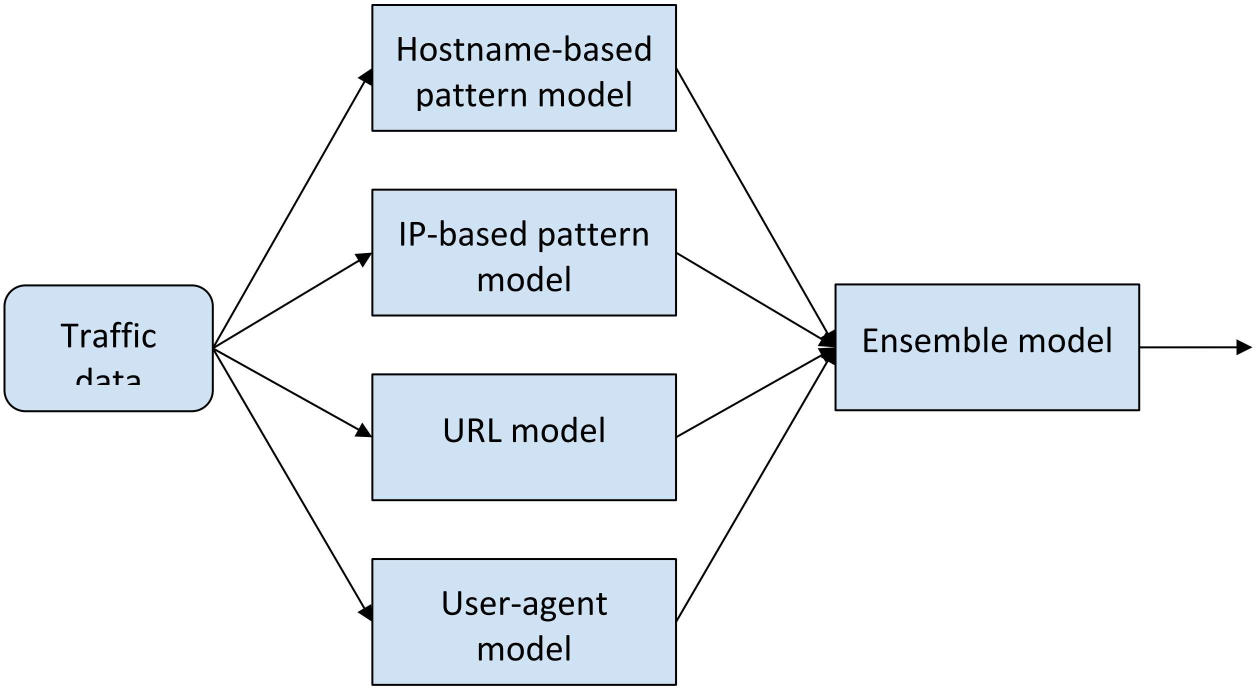


Figure 1. Machine learning model architecture for C2 activity detection

Human-in-the-loop and lab testing

Machine Learning is good at spotting suspicious C2 activity based on transaction data. Yet human review can still be necessary to identify and confidently call out malicious C2 activity. At issue: It's not feasible for human experts to review billions (or even, if the data is filtered, millions) of transactions per day. Instead, Zscaler employs a two-phase approach: The Machine Learning model outputs a shortlist of "high confidence" suspicious C2 domains based on transactions from within a specific time window, effectively filtering the transactions down to a manageable size for phase-two human review (and subsequent action). In the example above, "c8dd8ae6dc4dc644[.]xyz" was confirmed as a malicious C2 domain by security researchers.

Detecting the unknown: a process of continuous improvement

Machine Learning can detect and block unknown botnets via analysis of command-and-control channels. Zscaler leverages unsupervised learning techniques to shortlist suspicious domains for deeper analysis, and then uses supervised learning methods to detect botnet command-and-control channels with high confidence. Every day, the Zscaler Zero Trust Exchange blocks botnets that have never been seen before.

About the Author

Howie Xu Vice President of Machine Learning and AI. Howie Xu is Vice President of Machine Learning and AI at Zscaler. Previously, he founded and headed VMware's networking team for a decade, ran the entire engineering team for Cisco's Cloud Networking & Services, and was the CEO and co-founder of TrustPath, which was acquired by Zscaler in 2018.

.

EVENTS

Global Disinfo Summit

18 - 19 AUGUST 2021 | VIRTUAL CONFERENCE

ASSET PROTECTION IN THE AGE OF DISINFORMATION

Featured speakers

H.E. Dr. Mohamed Hamad Al Kuwaiti
Head of Cyber Security
UAE Government

Rand Waltzman
Senior Information Scientist
RAND Corporation

Elizabeth Linder
Founder and Chief Diplomatic Officer
Brooch Associates

Doowan Lee
Nonresident Senior Technical Advisor
Institute for Security + Technology

Ken Gamble
Investigations, Intelligence & Recovery Fraud and Cybercrime Specialist

Peter Naftaliev
AI Entrepreneur lecturer and consultant
2d3d.ai

Hassan Al Noon
Managing Director
Multiverse Innovation

Megha Kumar
Deputy Director of Analysis
Oxford Analytica

Dr. Petros Violakis
Assistant Professor, Homeland Security Program
Rabdan Academy

Christina Nemr
Director
Park Advisors

Jessy El Murr
Journalist, Media Expert and Host
Forbes Middle East

Selim J. Eddé
Director & Head of Government Affairs & Public Policy
Google Middle East and North Africa

Gold partner: Cyabra

Networking partner: Logically.

Key contributing organizations:

RAND CORPORATION · BROOCH ASSOCIATES · IST Institute for SECURITY + TECHNOLOGY · IFW GLOBAL · 2030 AI · PARK ADVISORS · اكاديميه ربدان Rabdan Academy · Oxford Analytica

Official media partners:

nation shield · sourceSecurity.com · MYSECURITY MEDIA · CYBER DEFENSE MAGAZINE WHERE INFOSEC KNOWLEDGE IS POWER · TECHx EVANGELIZING TECHNOLOGY

www.globaldisinfosummit.com

Strategic partner: MULTIVERSE

Organizer: اجتماعات ejtemaat Ejtemaat Knowledge Network

USE CODE: **CDM TO ACCESS YOUR COMPLIMENTARY PASS**

HAMBURG
ITS World Congress
11 - 15 Oct 2021
Experience Future Mobility Now
Experience Future Mobility Now
Preparations under way to ensure a safe and secure experience.

SMART GRID FORUMS

IEC 61850 Week 2021

Driving the rapid replacement of cybersecure IEC 61850 systems within the substation, inter-substations, to the control room, and across DER infrastructure

5-Day Hybrid Conference, Exhibition & Networking Forum
18-22 October 2021 | Sweden + Swapcard

150+ IEC 61850 leaders convene in Sweden on 18-22 October 2021, to review the latest implementations of IEC 61850 systems within the substation, inter-substations, to the control room, and across DER infrastructure

Recent research carried out by Smart Grid Forums among power grid operators worldwide, indicates that Covid-19 has injected urgency into utilities' digitisation plans with profound implications for substation automation teams. This year's 8th annual IEC 61850 Week 2021 hybrid conference will be held 18-22 October 2021 in Sweden and draw together pioneering IEC 61850 implementation leaders for a week-long review of the latest standardisation developments, pilot project results, large-scale implementation experiences, and future application explorations.

The focus will be on driving the deployment of next generation IEC 61850 architectures through more efficient specification, engineering, testing, operation, maintenance, and innovations in cybersecurity within a more rapid 'replacement' environment. Case-studies will focus on implementations of process bus and station bus architectures, with applications within the substation, inter-substations, from substation to control centre, and across distributed energy resources.

Monday 18th October: Specification Workshop
The week begins with a hands-on practical workshop providing utilities and suppliers with the opportunity to explore how they can leverage IEC 61850 specification guidelines to improve their collaboration, streamline the end-to-end specification process, reduce duplication of effort, and ensure clarity of utility objectives whilst leveraging supplier expertise.

Tuesday 19th to Thursday 21st October: Implementation Case-Study Conference & Exhibition
Over the course of these three days, participants will hear the latest lessons learnt from pilot projects and large-scale deployments of multi-vendor multi-edition IEC 61850 systems worldwide. With case-studies from Europe, Americas, Asia, Middle East and Africa, this is a unique opportunity to gain a global perspective on real-world deployment activity, future system and component requirements, and explore brand new partnership opportunities.

Friday 22nd October: Cybersecurity Workshop
The week wraps up with this deep diving seminar into the cybersecurity issues currently impeding the deployment of IEC 61850. With a thorough exploration of IEC 62351 both on a conceptual level and in terms of its application and evolution, participants will come away with a clear understanding of how they can tighten up system security today and what cybersecurity innovations they can plan to leverage tomorrow.

Due to ongoing travel uncertainties, this year's programme will be held in hybrid format, with an onsite experience offered to those who will be permitted to travel, and an online alternative for those who won't.

For more information please contact:

Mandana White, CEO, Smart Grid Forums

Smart Grid Forums Ltd

PO Box 63594, London, N19 9FT, United Kingdom

T: +44 (0)20 8057 1700 | registration@smartgrid-forums.com

#CYBERBYTE
@ROSSOWESQ

CYBER DEFENSE TV

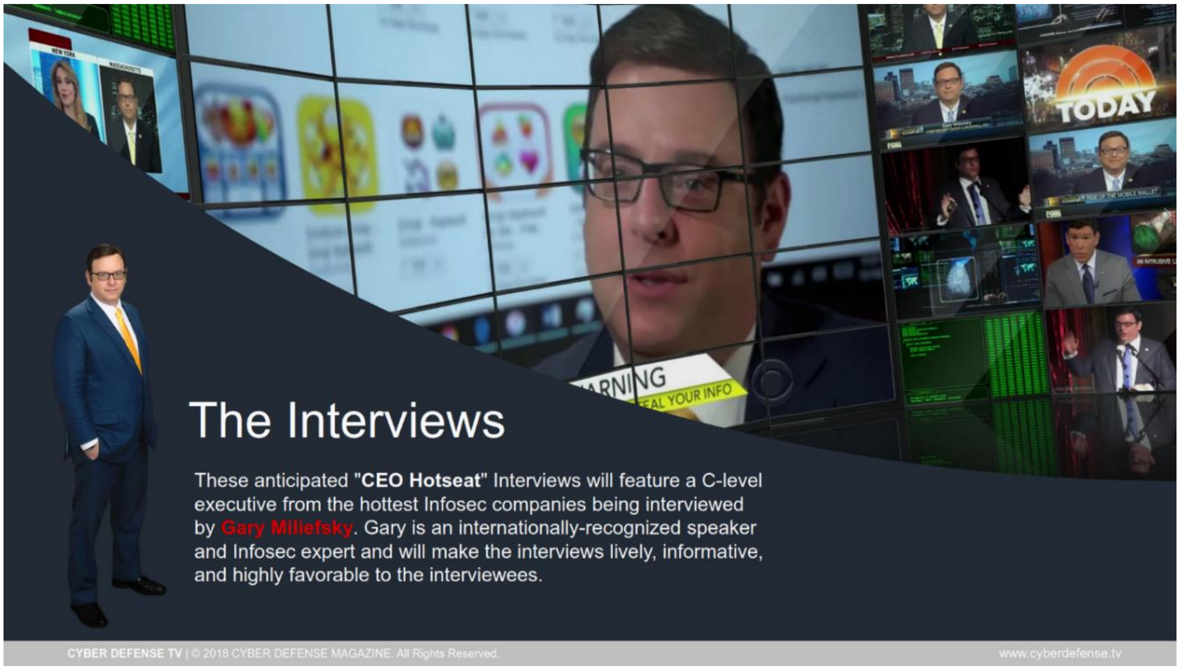
INFOSEC KNOWLEDGE IS POWER

You asked, and it's finally here…we've launched CyberDefense.TV

Hundreds of exceptional interviews and growing…

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

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



The Interviews

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

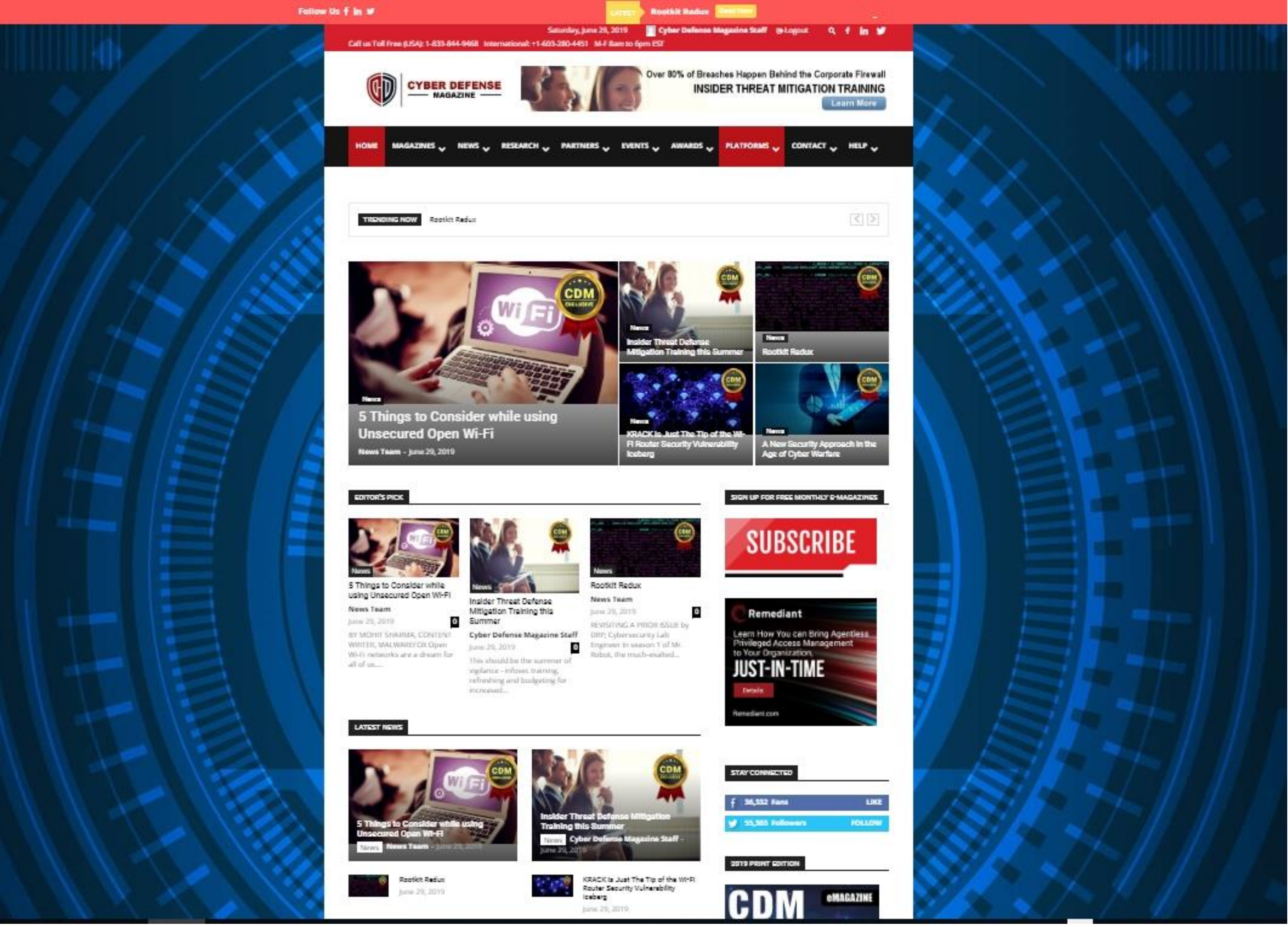
CYBER DEFENSE TV | © 2018 CYBER DEFENSE MAGAZINE. All Rights Reserved. www.cyberdefense.tv

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

Cyber Defense Magazine

276 Fifth Avenue, Suite 704, New York, NY 1000
EIN: 454-18-8465, DUNS# 078358935.
All rights reserved worldwide.
marketing@cyberdefensemagazine.com
www.cyberdefensemagazine.com

NEW YORK (US HQ), LONDON (UK/EU), HONG KONG (ASIA)
Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 08/02/2021
Books by our Publisher: https://www.amazon.com/Cryptoconomy-Bitcoins-Blockchains-Bad-Guys-ebook/dp/B07KPNS9NH (with others coming soon...)


Follow Us
LATEST
Rootkit Redux
Saturday, June 29, 2019
Cyber Defense Magazine Staff
Logout
Call us Toll Free (USA): 1-833-844-9468 International: +1-603-280-4451 M-F 8am to 6pm EST
CYBER DEFENSE MAGAZINE
Over 80% of Breaches Happen Behind the Corporate Firewall
INSIDER THREAT MITIGATION TRAINING
Learn More
HOME
MAGAZINES
NEWS
RESEARCH
PARTNERS
EVENTS
AWARDS
PLATFORMS
CONTACT
HELP
TRENDING NOW
Rootkit Redux
News
5 Things to Consider while using Unsecured Open Wi-Fi
News Team - June 29, 2019
News
Insider Threat Defense Mitigation Training this Summer
News
Rootkit Redux
News
KRACK Is Just The Tip of the Wi-Fi Router Security Vulnerability Iceberg
News
A New Security Approach in the Age of Cyber Warfare
EDITOR'S PICK
SIGN UP FOR FREE MONTHLY E-MAGAZINES
SUBSCRIBE
Remediant
Learn How You can Bring Agentless Privileged Access Management to Your Organization.
JUST-IN-TIME
Details
Remediant.com
LATEST NEWS
STAY CONNECTED
36,332 Fans
LIKE
55,303 Followers
FOLLOW
2019 PRINT EDITION
CDM
eMAGAZINE

5 Things to Consider while using Unsecured Open Wi-Fi
News Team
June 29, 2019
BY MOHIT SHARMA, CONTENT WRITER, MALWAREFOX Open Wi-Fi networks are a dream for all of us....

Insider Threat Defense Mitigation Training this Summer
Cyber Defense Magazine Staff
June 29, 2019
This should be the summer of vigilance - infosec training, refreshing and budgeting for increased...

Rootkit Redux
News Team
June 29, 2019
REVISITING A PRIOR ISSUE by DRP; Cybersecurity Lab Engineer In season 1 of Mr. Robot, the much-exalted...

5 Things to Consider while using Unsecured Open Wi-Fi
News News Team - June 29, 2019

Insider Threat Defense Mitigation Training this Summer
News Cyber Defense Magazine Staff - June 29, 2019

Rootkit Redux
June 29, 2019

KRACK Is Just The Tip of the Wi-Fi Router Security Vulnerability Iceberg
June 29, 2019

9 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 shooting for 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 https://www.cyberdefenseprofessionals.com this month…

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

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

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