CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

eMAGAZINE

INSIDE THIS EDITION

And much more...

JANUARY 2019

MORE INSIDE!

CONTENTS

@MILIEFSKY

From the

Publisher…

CyberDefense.TV welcomes you as a founding member, free, no strings, please join now.

Dear Friends,

First, let me wish each of you an incredibly blessed 2019!

We, at Cyber Defense Media Group are so thankful for your support – to our writers, our readers, our team members, our sponsors – to the executives who took time out of their precious day to be interviewed by me (we're at 42 CyberDefense.TV interviews and more being posted), you have our sincerest appreciation.

By the end of the first quarter of 2019, we will have six platforms online and operational. Some of them will be a big surprise to you and we hope you enjoy. Our goal is to be the #1 source of original InfoSec content – best practices, tips, tools, techniques and the best ideas from leading industry experts. We're on path to make this happen entering our 7th year in 2019 with over 7,000 original pages of searchable InfoSec content. While there are new 'copycat' brands out there on the market, you'll find they have very little original content and we hope to continue to keep our pace, so you'll independently see the incredible difference, in our value proposition. When you visit a content site on cyber security and you click a link, if the story takes you somewhere else, it's not original content – it's repurposed and republished because that organization chose to take a short-cut. We do not. Over time, we plan to be the largest repository of InfoSec information and knowledge in the world and we won't stop, ever. *With much appreciation to our all our sponsors – it's you who allow us to deliver great content for free every month to our readers…for you, our comarketing partners, we are forever grateful! Have an awesome holiday season and wonderful New Year!*

Warmest regards,

Gary S. Miliefsky

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

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

From the

Editor…

Welcome to 2019! We've made it. While we hear in the news 'the Russians are coming, the Russians are coming,' we've found that the Chinese are already here – whether it's in the hardware or software, the networking gear or your smartphone, they've been electronically breaking-and-entering at a pace that's unsurpassed in the industry. The amount of personally identifiable information (PII) records they continue to harvest is in the billions. This is the real untold story we expect to unfold in greater detail, this year – in the Chinese zodiac, the year of the Brown Pig – a year of prosperity and abundance and good fortune. Let's make it ours, when it comes to cyber defense – a safer, more secure & productive year.

Happy New Year!

To our faithful readers,

Pierluigi Paganini

@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

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

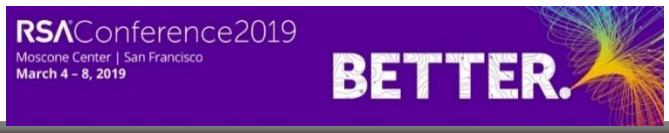
WE'RE CELEBRATING
6 YEARS OF EXCELLENCE!

Providing free information, best practices, tips and techniques on cybersecurity since 2012, Cyber Defense magazine is your go-to-source for Information Security. We're a proud division of Cyber Defense Media Group:

CYBERDEFENSEMEDIAGROUP.COM

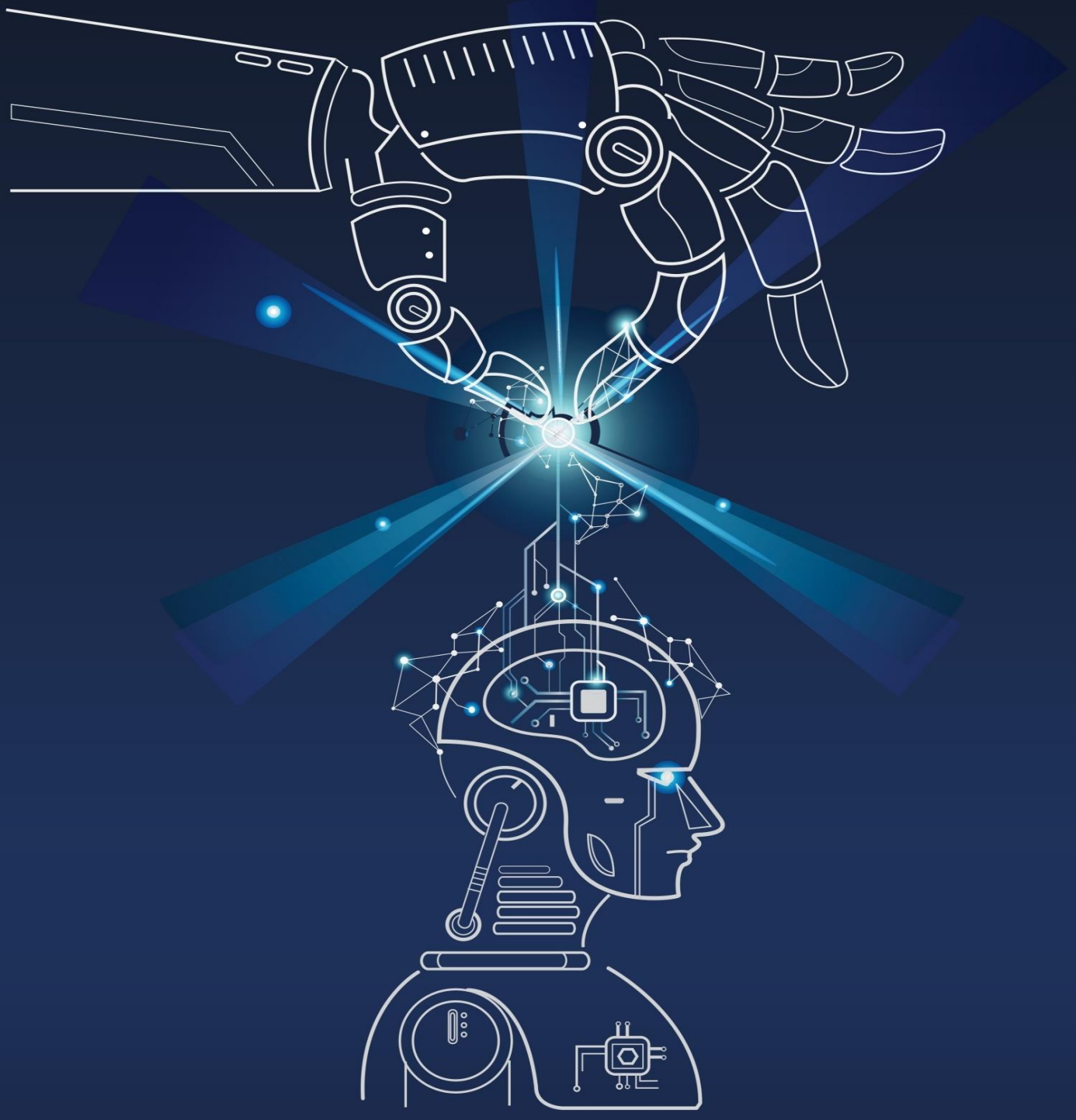
MAGAZINE **TV** **AWARDS**

SEE US IN MARCH 2019 AT…



SPONSORS

InfoSec Knowledge is Power
Free Cybersecurity Resources



www.cyberdefense.tv
www.cyberdefensemagazine.com

DON'T LET COMMUNICATION BE YOUR POINT OF FAILURE.

The **Vaporstream® Secure Communication Platform** lets organizations securely collaborate with confidence during times of crisis.

Vaporstream eliminates the vulnerabilities of the traditional communication and information sharing channels such as email and standard SMS. Our enterprise-grade, secure and compliant communication platform empowers business continuity and command of any crisis outside of your network, without worrying about information leaks to bad actors, the media or the competition that could impact your reputation or bottom line. Take control of communication during any crisis. **Learn how Vaporstream helps you keep communications secure, compliant and leak free.**

Vaporstream

Visit us at www.Vaporstream.com/security.

Connectivity with Salesforce, Google Drive, SharePoint, and More...Simplified

Wouldn't it be nice if your file transfer solution allowed for plug-n-play connectivity with the web and cloud applications you use every day?

THIS IS 100% POSSIBLE WITH

GO ANYWHERE®
Managed File Transfer

GoAnywhere is a managed file transfer solution that simplifies how you encrypt and automate your data transmissions. Together with GoAnywhere Cloud Connectors - powerful web and cloud integrations - you can streamline connections with these applications and more:

Dropbox

Google Drive

VOTIRO SECURED.

salesforce

SharePoint

Jenkins

Microsoft Dynamics 365

zendesk

Simplify Your Processes and More with Secure Cloud Integrations

Request a Demo: www.goanywhere.com/demo

Visuality Systems

Protect Your Product From Malicious SMB File Sharing Activities, Upgrade To An

Encrypted SMB VERSION 3

Secured Access To Remote Files

sanernow

Array of tools for Endpoint Security and Systems Management

- ✓ Vulnerability Management
- ✓ Patch Management
- ✓ IT Asset Management
- ✓ Compliance Management
- ✓ Endpoint Threat detection
- ✓ Endpoint Management

secpod

REAL-TIME CONTINUOUS DIAGNOSTICS & MONITORING

SHINE A LIGHT ON THE DARKEST CORNERS OF YOUR NETWORK

STIGs & Configurations

Continuous audit of policies & controls.

Threats & Vulnerabilities

Real-time discovery of Threats & Risk.

Asset Discovery

Automatic inventory & tracking of assets.

User & Entity Behavior

Monitoring of risky & unsanctioned activity.

Looking for the information you need to **Identify Risk**, **Direct Remediation**, and **Document Results**?

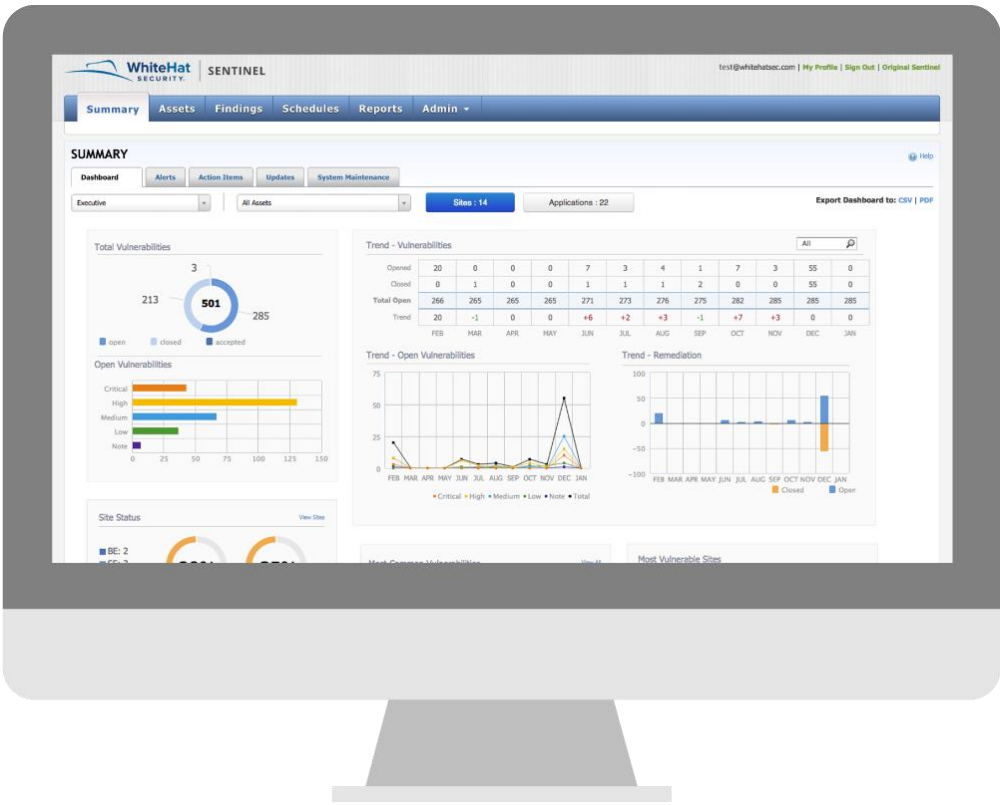
Look no further...

Get meaningful, actionable, and repeatable data, in real-time. AristotleInsight® is the world's first Continuous Diagnostics & Monitoring (CDM) Platform to bridge the gap between security frameworks and real-world IT Technologies.

Get the information you need, when you need it, with AristotleInsight.

AristotleInsight®
— Identify | Remediate | Document —

AristotleInsight.com | Call us at 866.748.5227



Your website could be vulnerable to outside attacks. Wouldn't you like to know where those vulnerabilities lie? Sign up today for your free trial of WhiteHat Sentinel Dynamic and gain a deep understanding of your web application vulnerabilities, how to prioritize them, and what to do about them. With this trial you will get:

An evaluation of the security of one of your organization's websites

Application security guidance from security engineers in WhiteHat's Threat Research Center

Full access to Sentinel's web-based interface, offering the ability to review and generate reports as well as share findings with internal developers and security management

A customized review and complimentary final executive and technical report

Click here to sign up at this URL: https://www.whitehatsec.com/info/security-check/

PLEASE NOTE: Trial participation is subject to qualification.

Your peers use managed file transfer to solve key business initiatives - but how?

IT professionals discover innovative uses for their secure file transfer solution every day. From tracking weather patterns in Alaska to eliminating third-shift staffing, MFT makes solving their organizational needs easy.

In The GoAnywhere Book of Secure File Transfer Project Examples, you'll discover 20+ ways your peers use managed file transfer to meet ambitious goals and requirements in their company, including:

- A distribution company that uses MFT to send barcode scans to a file repository.
- A healthcare organization that uses MFT to move faxes into an API for processing.
- A manufacturing business that uses MFT to check a server for firmware updates.

Find the inspiration and know-how for your next file transfer project.

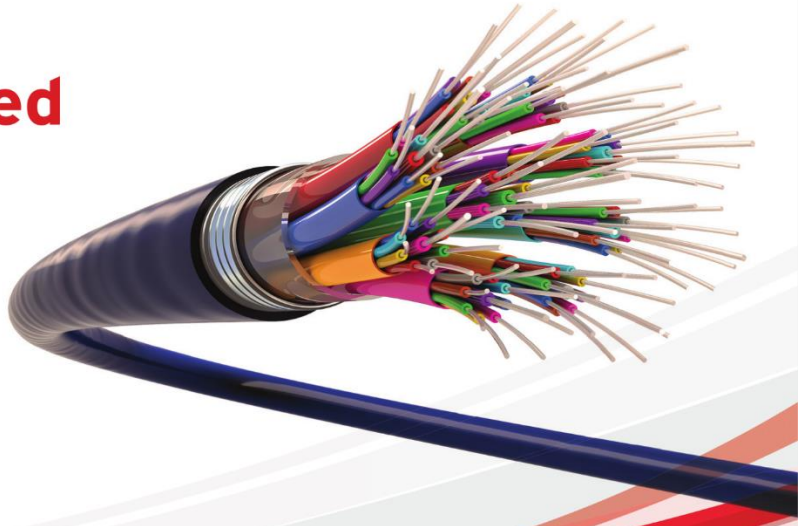
GO ANYWHERE®
Managed File Transfer

Visit ***info.goanywhere.com/use-cases-for-mft*** to get the free guide sent right to your inbox.

TREND MICRO

POWERED BY XGen SECURITY

Detect and prevent breaches at wire speed



Your enterprise is in the crosshairs of the increasingly complex array of ransomware, advanced threats, targeted attacks, vulnerabilities, and exploits.

Only complete visibility into all network traffic and activity will keep your network security ahead of today's purpose-built attacks which bypass traditional controls, exploit network vulnerabilities, and either ransom or steal sensitive data, communications, and intellectual property.

Trend Micro Network Defence detects and prevents breaches at wire speed anywhere on your network to protect your critical data and reputation.

NSS LABS RECOMMENDED

Proven capability

Trend Micro TippingPoint:
"Recommended" Next-Generation Intrusion Prevention System and 99.6% security effectiveness.

Trend Micro Deep Discovery:
"Recommended" Breach Detection System 4 years in a row and 100% detection rate

Industry leading threat intelligence

TREND MICRO SMART Protection Network™

TELUS®

Web App Digital Vaccine BY TippingPoint

ZERO DAY INITIATIVE

Please get in touch:
Bharat Mistry, Principal Security Strategist
Bharat_mistry@trendmicro.co.uk

www.trendmicro.co.uk/xgen-cyber

Hacking Experts

Providing security solutions, training and professional services to enhance cyber security knowledge. We make cyberspace safer for businesses.

TRAINING SERVICES

HACKER HOUSE™

AS SEEN IN

Forbes Bloomberg FOX NEWS CNN WIRED SKY NEWS The Register MOTHERBOARD

CYBER SECURITY EXPERTS LEADING DEFENCES AGAINST THE DARK ARTS

PENETRATION TESTING SERVICES
view >

RED TEAM AND ADVERSARY SIMULATIONS
view >

INFRASTRUCTURE SECURITY
view >

WEB APPLICATION SECURITY
view >

HARDWARE SECURITY
view >

WIRELESS SECURITY
view >

MALWARE ANALYSIS

MOBILE SECURITY TESTING

BLOCKCHAIN SECURITY

ARTICLES

3 Ways to Combat (Growing) Cyber Threat

By Emy R. Donavan, Global Head - Cyber, Tech and Media PI at Allianz Global Corporate &Specialty

Because global brands tend to bear the brunt of cyberattacks—and generate the most media coverage—the vast majority of brands and organizations can be forgiven for thinking that the odds of their company's computer networks getting hacked are pretty remote if not downright impossible.

Think again. And, if you know what's good for your company, flip the mental switch when it comes to thinking your company is too small or doesn't possess enough assets to appeal to hackers.

Regardless of the size of your company, the business sector or level of brand visibility, every company is vulnerable to a cyberattack. Hackers don't discriminate.

That was the major takeaway from a recent roundtable discussion focusing on how

Companies inoculate themselves against cyberattacks.

The roundtable was hosted by Allianz Global Corporate & Specialty. I took part in the discussion, along with Steve Martino, Cisco Senior VP and Chief Information Security Officer, and Gregory Falco, Stanford fellow, CISAC security researcher and MIT grad.

Growing Threat

Increasing connectivity, globalization and the "commercialization" of cyber-crime are driving greater frequency and severity of cyber incidents, including data breaches. And the threat is growing more acute.

Cyberattacks, even those which cause minimal damage, lead to discontinuity of business, which can lead to loss of revenue.

The numbers tell an unnerving story.

Each data breach cost companies $3.86 million on average in 2017, according to an annual data breach report sponsored by IBM. In the worst cases, "mega breaches" may cost the enterprise between $40 million and $350 million.

“Every company today is a tech company,” Martino said. “Some companies no longer have any physical assets; all risks have some tie to technology…this brings more and new exposure to risk.”

Falco stressed that cyber leadership needs to start from the top of the organization. “If leaders aren’t pushing and demonstrating good cybersecurity,” he said, “it is unrealistic to expect the rest of the organization to follow suit.”

He added that cyber risk should not exclusively be managed by a CISO because a cyberattack can cause serious economic and reputational damages to your business that expands far beyond your technology infrastructure. “Frankly, the CEO’s job is on the line and board members need to push leadership to adopt the latest advancements that are feasible for an organization to adopt.”

Last May Europe strengthened its digital responsibility requirements with the implementation of the General Data Protection Regulation (GDPR). GDPR standardized privacy rules across all 28 EU countries and strengthened individual rights to protect personal data.

While the U.S. currently does not have a single, uniform standard across all states similar to GDPR, awareness of cyber risk is high and many states have strict data protection laws in place that require companies to notify individuals of a breach. However, awareness is one thing. Being proactive in tackling the problem is another.

With that in mind, here are three concrete ways for companies to combat the cyber threat and mitigate any potential damage stemming from a data breach.

1. **Have a cyber security expert at the board level**. If you don’t have someone with tech/cyber security experience on the board, it’s incumbent upon companies to create a new board position or hire an IT consultant who can serve as a close adviser regarding cybersecurity strategy. Companies must have access to business professionals who understand the cyber threat and are aware of the known unknowns. The onus is on boards of directors to ramp up their cyber security budgets. Roughly 73 percent of organizations said it is "very common" or "common" to have just one person responsible for alerting the business to vulnerabilities, and also applying patches and updates to systems and software, according to a recent survey of 510 IT and cybersecurity leaders. For many companies, there’s still too much emphasis on traditional business risks and not enough on digital risk. That has to change.

2. **Sharpen employee awareness/cyber security training.** Often times, a data breach happens after an employee unwittingly clicks on a link in an email, unleashing malware into the entire organization. That’s why there’s a growing onus on organizations to provide cyber security training/awareness/education on an annual basis. The threat landscape changes fairly quickly and employees need to be abreast of these changes. Training doesn’t have to be overly complicated. Half the battle is making sure employees are able to sharpen their digital antennas and understand that some emails are not always what they

appear. Employees must be aware of protocols regarding who they report to when they spot something fishy in their inbox and how to address the situation quickly.

3. **Bolster your password management efforts**. There are all sorts of circuitous ways hackers can breach corporate computer system(s). For example, malicious actors online could hack into your Gmail account and use that access to get into your company's business network. Many people use the same computer password regardless for both their personal and professional accounts. Companies need to disabuse their employees that that's acceptable. Employees need to be conditioned not only to have unique passwords for different computers and different hand-held devices but to change the passwords frequently (and make sure changes in passwords are a significant departure from previous ones).

Considering the pace of technological change—and how hackers always seem to stay a few steps ahead of companies' efforts to stop them—organizations that continue to give cyber security short shrift could one day find themselves facing an existential threat.

Adding insult to injury, individual board members and/or C-suite executives who ignore (or downplay cybersecurity) could be on the hook if, following a breach, they are found to have abrogated their corporate responsibility. At that point, having to leave the company may be the least of their worries.

About the Author

Emy R. Donavan, Global Head - Cyber, Tech and Media PI at Allianz Global Corporate & Specialty Emy Donavan is currently serving as Global Head and CUO of Cyber, Tech & Media PI for Allianz Global Corporate and Specialty (AGCS). In July of 2018, she was also tasked to head Allianz SE's Cyber Center of Competence, which provides support and expertise on Cyber products for all Operating Entities of Allianz. She was promoted into these roles after serving as North American Head of Cyber for Allianz Global Corporate & Specialty (AGCS), as well as U.S. Head of E&O for Tech PI, Media, Miscellaneous E&O, and A&E lines. In July of 2016, she finalized AGCS's first-ever U.S. Cyber and Specialty PI policy wordings and was responsible for developing AGCS's North American Cyber guidelines, rates and policies until her promotion into the global role. In her new role, Ms. Donavan is responsible on for all Cyber, Tech & Media PI underwriting initiatives within AGCS, and for technical support of cyber underwriting initiatives across all Allianz entities. Ms. Donavan's prior experience spans more than 15 years of Cyber, Technology, and Specialty E&O-dedicated experience at several of the largest PI and Cyber carriers in the U.S. and international markets.Emy also enjoys opportunities to educate; she trains brokers, underwriters and clients on emerging risks in the Cyber marketplace through her formal job functions, speaking engagements, and occasional LinkedIn Pulse Blog (Cyber Underwriting 101). Ms. Donavan graduated from UC Berkeley with a BA in Rhetoric, focusing on legal writing and argument construction, and is a licensed CA surplus lines broker. Ms. Donavan is also a frequent speaker for PLUS, the American Bar Association, Advisen, the NAIC and other affiliation groups on Cyber & Professional Liability insurance topics and has been quoted in the Wall Street Journal and other major publications covering the cyber market. Emy Donavan can be reached at Emy.Donavan@agcs.allianz.com

The 5 Most Cringe-Worthy Privileged Data Breaches of 2018

By Morey J. Haber, Chief Technology Officer, Beyond Trust

Privileged attack vectors and stolen personally identifiable information (PII) obtained have been a constantly paired news item throughout 2018. In 2019, expect privileged attack vectors to continue to reign as the number one root cause of breaches for both consumer and business data theft.

Below, I have compiled my list of the top-5 most noteworthy breaches for this year (so far). My ranking may be surprising to some of the readers, and some of the incidents are not even that high profile, but the size, duration, and type of business all contribute to the ranking.

While Gartner has acknowledged that Privileged Access Management is the top security priority for 2018, many organizations are still in denial of their privileged account risks. These inadequately controlled cyber risks frequently stem from poor identity and password management hygiene. Organizations must learn to programmatically discover and manage their privileged accounts because the attack vector is not going away anytime soon.

Notable Mention: Orbitz

One breach that occurred in early 2018 is not officially ranked, but is notable because it has the distinction of being a completely Internet-based business, with no brick and mortar presence for customer interaction. It is a dot-com company and should have understood, just like Yahoo, that strong cybersecurity is critical.

In March, Orbitz announced that 880,000 payment cards were hacked in a breach that spanned almost two years, and over multiple systems. Two years! While the number of credit cards hacked is fractional compared to other incidents, it is the duration of compromise for a web-based company that gains them notable mention.

Although the forensic information published on the breach remains vague, it is known that the incident involved data submitted to a legacy and partner websites. Orbitz claims there is no direct evidence that the information was actually stolen, but this security professional wonders if penetration and vulnerability assessment tests were actually being performed on these websites, and the results scheduled for remediation in a timely manner. I suspect not.

Orbitz, said "We took immediate steps to investigate the incident and enhance security and monitoring of the affected platform". They also reported, "As part of our investigation and remediation work, we brought in a leading third-party forensic investigation firm and other cybersecurity experts, began working with law enforcement and took swift action to eliminate and prevent unauthorized access to the platform."

Orbitz's words on this subject warrant some scrutiny. The monitoring and security initially in place were insufficient, and "unauthorized access" implies yet another identity and privileged access attack vector. For a 100% web-based company, the front door is the web and shipping, and loading doors are partner connectivity. All of this must be secured just as in a physical building – something Orbitz did not adequately do to protect against unauthorized access. That little padlock in your browser indicating a secure connection for your transaction just did not matter for their incident since it was the other doors (websites) that got them in trouble.

Now, let's take a look at the breaches that made the top-five list for 2018:

#5 Adidas

Adidas announced in June that an "unauthorized party" gained access to customer data on Adidas' US website. While no details have thus far been publicly released regarding the attack and breach methodology, the company says that they believe only customers who purchased items from the US-hosted version of Adidas.com may have been affected by the incident.

While it is unknown if the attack vector involved a configuration flaw, vulnerability and exploit combination, or privileged attack, the threat actors did obtain contact information, usernames, and encrypted passwords. It is also unknown whether or not it was possible to decrypt the heisted passwords since the rest of the breach details do not fall under regional jurisdiction laws like GPDR, and were not publicly released.

So, as far as 2018 breaches goes, this lands squarely at the bottom of the top-5 list, but represents data that can be used for future phishing and privileged attacks. Leaked personally identifiable information (PII) forms the basis for future privileged attacks.

#4 Saks Fifth Avenue and Lord & Taylor

On April 1, 2018 (and not an April fool's joke), Lord & Taylor and Saks Fifth Avenue announced that their stores were the subject of a massive credit card data breach. This security incident is believed to have compromised 5 million customers' credit card information.

While the size is significant, what is perhaps even more shocking is the extended duration in which the security compromise was ongoing.

Clients who used a credit or debit card at any of the stores' retail locations between May 2017 and April 2018 were most likely affected. However, the breach was not identified or disclosed for almost a year!

Similar to Adidas, few details were publicly released regarding the attack vector. However, The New York Times reported that the attack was likely initiated by an email phishing scam sent to Hudson's Bay (Canadian-based owner of Saks and Lord & Taylor) employees. The threat actors reportedly targeted accounts with malicious software via a link, file, or other attack vector to infiltrate the environment.

It is important to note, the vast majority of malware can be stopped with simply the removal of administrative rights from an end user's workstation. That is basic privilege management. Hopefully, we all can learn from this example to identify phishing attacks and remove end user administrative rights. And, implement threat analytics to identifiable these types of incidents sooner!

#3 Under Armour

Scarcely a month after the Saks Fifth Avenue and Lord & Taylor breach, Under Armor learned that someone had gained unauthorized access to MyFitnessPal, a platform that hosts IoT device data for tracking a users' diet, exercise, and health. Upwards of 150 million MyFitnessPal users are believed to have had their information compromised.

CNBC reported at the time of disclosure that threat actors claimed responsibility for breaching individuals' usernames, email addresses, and hashed passwords. While the incident did not expose users' credit card information (unlike Saks and Lord & Taylor) due to architectural designs in data, process segmentation, and payment storage, it lay bare the cyber risks inherent of storing IoT data in the cloud.

Based on reports from Forbes and CNBC, the incident arose due to "unauthorized access" to user data. That alone reflects inadequate privileged access management and underscores this attack as another reason mature identity and privilege management capabilities and processes are critical for organizations to embrace.

#2 T-Mobile

Fast forward a few months to August and land on our second worst breach of 2018. T-Mobile announced that threat actors stole the personal data of approximately 2 million of its customers (3% of its clients). The leaked data was typical: usernames, billing zip codes, phone numbers, email addresses, and account numbers, as well as information on whether customers prepaid or postpaid their accounts.

T-Mobile's cybersecurity team reportedly "discovered and shut down an unauthorized capture of some information" after the breach. Those words are key. Was it a man in the middle attack (MITM), was data stolen from a database or log files, or did someone have inappropriate privileged access? The public may never know the full details, but the word "unauthorized" implies the threat actor did not have authorization to collect the privileged data in the first place. This brings us full circle back to yet another privileged attack based on poor identity and privilege management hygiene.

And, making things a little more grey, T-Mobile indicated that no passwords were compromised,

but recommended, "it's always a good idea to regularly change account passwords." That statement should make customers wary, since, in 2015, Experian, which processes credit applications for T-Mobile, was itself breached. That incident impacted 15 million customers! Compromised customer data in 2015 included social security numbers, drivers' licenses, and passports for T-Mobile customers. In retrospect, it appears T-Mobile did not learn its lesson three years ago.

#1 Starwood

In 2016, Marriott acquired the Starwood hotel chain, including leading brands like St. Regis, Westin, Sheraton, and W Hotels. Two years before the acquisition, an incident began that was only identified last week. So, for four years, "unauthorized access" occurred within the Starwood reservation system that ultimately involved the leaking of names, phone numbers, email addresses, passport numbers, birthdates, and reservation information (arrival, departure, and points) for an estimated 500 million customers. Additionally, a subset of those customers numbering in the millions may have also had their credit card numbers and expiration dates disclosed. The size, severity, duration, and breach lasting over a major acquisition puts the Starwood breach atop all others in 2018.

In an official statement from the company, "Marriott learned during the investigation that there had been unauthorized access to the Starwood network since 2014." And, "Marriott recently discovered that an unauthorized party had copied and encrypted information, and took steps towards removing it."

As the statement reveals, the threat actors had "unauthorized access" which implies inappropriate identity and privileged access to key systems that, strictly by the nature of the data, should have been segmented. For example, in line with PCI DSS standards, credit card access should never allow reassembly, even if encrypted, to allow association with the data owner.

The threat actor must have gained lateral access across zones and systems in order to perform the many types of operations needed to exfiltrate the data. Outside of poor incident monitoring technology, log monitoring, privilege management, and network and data segmentation, Starwood failed in an epic fashion to identify and contain the incident.

Considering the regency of the Starwood breach announcement, I expect there to be more revelations regarding the incident over the coming months.

Since the breach falls under the European GDPR regulations for some of its 1,200 properties, Starwood may incur significant financial penalties of up to four percent of its global annual revenue if found to be liable for breach rules. That is significant for any business and should be a strong message for every executive, employee, stock holder, and board member.

Final Word

Will 2019 bode any better with regard to improved security and data protection? Only if we really start to heed the security lessons of 2018 and years past.

About the Author

With more than 20 years of IT industry experience and author of Privileged Attack Vectors, Mr. Haber joined Beyond Trust in 2012 as a part of the eEye Digital Security acquisition. He currently oversees Beyond Trust technology for both vulnerability and privileged access management solutions. In 2004, Mr. Haber joined eEye as the Director of Security Engineering and was responsible for strategic business discussions and vulnerability management architectures in Fortune 500 clients. Prior to eEye, he was a Development Manager for Computer Associates, Inc. (CA), responsible for new product beta cycles and named customer accounts. Mr. Haber began his career as a Reliability and Maintainability Engineer for a government contractor building flight and training simulators. He earned a Bachelor's of Science in Electrical Engineering from the State University of New York at Stony Brook.

Cyber Attack Targets & Outcomes to Watch Out for in 2019

By Morey Haber, CTO, BeyondTrust

There are three jobs in this world where you can be completely wrong all the time and still not have to worry about being fired. One is a parent. Another is a weatherperson. And the last one is a technology trends forecaster. Having failed as a weatherman, and with the results of my parenting skills still up for debate, I have turned my mental prowess toward bold predictions on the state of data breaches, IT security, and cyber risks!

I have categorized this list of predictions into two categories—Attack Vectors/Targets, and Attack Outcomes. Attack vectors/targets include the mechanisms cyber attackers will use, as well as their ultimate objectives. Attack outcomes include how organizations will respond.

Attack Vectors/Targets

Privileged attacks continue

Privileged attack vectors will continue to be the number one root cause of breaches for both consumer and business data. While Gartner acknowledged that Privileged Access Management as the top security priority for 2018, many organizations are still in denial of their privileged account risks, which frequently stem from poor password management hygiene.

2019 will see even more high-profile breaches. Organizations must discover and manage their privileged accounts because the attack vector is not going away anytime soon, and ugly newspaper headlines will continue to plague boardrooms.

Well-known vulnerabilities will continue To dominate cyber-attack reports

The pattern of successful attacks through the use of well-known and entirely preventable vulnerabilities shows little sign of

abating. Organizations continue to focus their efforts injudiciously, ignoring the lower severity vulnerabilities with known exploits in favor of largely academic, high severity vulnerabilities. This leaves their systems vulnerable to becoming footholds, which can then open up pathways for further exploitation, resulting in major data exfiltration incidents.

Artificial Intelligence (AI) on The attack—Skynet is becoming self-aware!

2019 will see an increasing number of attacks coordinated with the use of AI/Machine Learning. AI will analyze the available options for exploit and develop strategies that will lead to an increase in number of successful attacks.

AI will also be able to take information gathered from successful hacks and incorporate that into new attacks, potentially learning how to identify defense strategies from the pattern of available exploits. This evolution may potentially lead to attacks that are significantly harder to defend against.

Industrial control systems come into focus

The next few years will see an increase in the attention that ICS/SCADA systems attract from cybercriminals and nation-state hackers. The opportunity to create ransomware scenarios directly affecting critical national infrastructure will draw attention from cyber criminals motivated both, by financial gain, as well as those who are looking to develop weapons in the evolving cyber-frontline.

Historically, Operational Technology (OT) teams have been reluctant to engage with IT security practices, but we are seeing this change as all teams recognize that cybersecurity is a critical aspect of business continuity.

The supply chain is at risk

Major security breaches will continue to dominate the news, but the latest form of attacks on organizations will come in the form of an attack on their supply chains.

Considering the recent Bloomberg article accusing China of embedding chips the size of a grain of rice into super micro servers, and previous attacks using embedded chips on printers purchased by the United States Government, the threat is very real.

Corporate attacks and corporate espionage will take on a whole new meaning as more supply chain attacks with embedded malware are discovered. But this is the tip of the iceberg in terms of cyber threats—the major devices targeted will be IoT and will range anywhere from consumer-based routers to home-based nanny cams. Expect the supply chain for many vendors, including those that produce personal digital assistances, to be a new target from threat actors who infiltrate environments and insecure DevOps processes.

Attack Outcomes

Android closes open access

Android will no longer be fully open and extensible. Google has already announced that only the “default” application can access calls and SMS texting data for the next release of Android, and the default application must be explicitly set in the configuration. No longer can multiple applications—including tools used for spam detection—be shared with your favorite calling and texting applications.

Expect Google to continue this trend to fight malware and spyware by closing more of the operating system in the name of security.

Monetizing data

Infonomics will begin to become mainstream and, just like other intellectual property, expect businesses to begin applying a value to the data and disclosing the information they have and what it costs "for sale".

If you think this is farfetched, consider the value of GPS data over the last 30 years. From the early days of MapQuest to dedicated GPS receivers, driving and transportation data has become a commodity.

However, if you start layering other data—like traffic, construction, etc.—used by the likes of Waze, you have a high-valued database that will become crucial for autonomous cars. There is real value there, and it will come at a price to car manufacturers. The data itself therefore has a value, and businesses will begin rating themselves more publicly on the Infonomics they possess. And not just too private equity firms or other businesses looking at merger and acquisition activities, or purchase of the information.

Millennials ruin everything—evolving definitions of privacy

The millennial generation will share almost anything on the Internet. Social media has proven that almost anything goes regardless of its perceived sensitivity. This implies that nearly an entire generation has a lower sensitivity to private data and that a "who cares" attitude for sensitive information is beginning its own movement.

In addition, as we become numb to data exposure, expect some push back from the youngest voting group regarding the data being exposed due to a hack. If most sensitive personal data is public (like name, email, address, birthday, etc.) and only the most important information protected (national ID numbers, bank records, credit cards), the value is diminished for anything already being exposed today and the "who cares" movement has begun.

Expect data classification to evolve based on the youngest users, and what we consider private today will not be private, or of a concern, tomorrow.

Centralized information brokers emerge

In an effort to protect and control the exposure of personal data, information 'brokers' will begin to emerge. These services will provide centralized mechanisms that allow granular sharing of data so that only the essential data is shared for whatever service you are signing up to.

The EU has been working on digital identity in this form for several years and may well be the first to bring that into full effect, but others will follow in providing a mechanism by which our data is decentralized. This will help limit individual data exposures when systems are compromised and allow more control by individuals over their data and who has legitimate access to it.

In closing, as in any cyber defense strategy, I first recommend getting the basics right—secure your privileged accounts, eliminate excessive user privileges, ensure secure remote access to critical systems, patch the vulnerabilities with known exploits, and report, report, report.

About the Author

With more than 20 years of IT industry experience and author of Privileged Attack Vectors, Mr. Haber joined BeyondTrust in 2012 as a part of the eEye Digital Security acquisition. He currently oversees BeyondTrust technology for both vulnerability and privileged access management solutions. In 2004, Mr. Haber joined eEye as the Director of Security Engineering and was responsible for strategic business discussions and vulnerability management architectures in Fortune 500 clients. Prior to eEye, he was a Development Manager for Computer Associates, Inc. (CA), responsible for new product beta cycles and named customer accounts. Mr. Haber began his career as a Reliability and Maintainability Engineer for a government contractor building flight and training simulators. He earned a Bachelor's of Science in Electrical Engineering from the State University of New York at Stony Brook.

Best Practices for Data Protection

By Eitan Bremler, Co-founder and VP of Product, Safe-T

As more companies pursue digital transformation, they may also increase vulnerability to cyber-attacks. That is because the practice often includes cloud migration, new platforms and technologies and moving more apps and functionality to the web; all of which can expand the attack surface, increasing exposure to unauthorized network access and data breaches. However, it *is* possible to move forward in a safe way. Adequate network and data protection infrastructure can allow integration of new technologies, while maintaining or even decreasing the increased attack surface that often comes with it.

Here are some best practices to help an enterprise keep their data safe from breaches and leaks:

Secure sensitive data

Users should get authenticated out-of-band before gaining access to a server or service. Out-of-band-authentication (OOBA) is a security measure that requires users to verify their identities through a separate channel. It is also sometimes referred to as two-factor authentication. However, this measure is unfortunately underutilized, creating a situation in which workers can save their credentials to reduce login steps. Anyone walking by can easily get into such a system. Sure, in-person attacks are rare, but exploitation of remote access tools can result in easy entry for a hacker who knows where to look.

Control data usage

By controlling access to specific locations and files on the network, businesses have a better chance of preventing insider attacks and data exfiltration. These data leaks aren't always necessarily malicious, or even intentional. Employees can email themselves files from work to open on a home device where security may not be as robust. Through access restrictions such as locking certain files, BYOD policies, and preventing sensitive file email transfer, these leaks and the risks they cause can be avoided.

Reduce the attack surface

Organizations are under constant threat of attack, and as their network perimeters grow larger and more porous, traditional authentication, encryption, and access mechanisms can be bypassed by even inexperienced hackers. Enterprises can mitigate the risk of external threats to applications and services while protecting access to on-premises, mobile, and hybrid cloud environments by reducing the attack surface of their network. But the best way to reduce network attack surface and intrusion vulnerability is to hide the network entirely, via the latest Software-defined Access solutions. This removes the need for white lists and blacklists. Instead, users are given access on a case-by-case basis. Muhammad Ali famously said, “His hands can’t hit what his eyes can’t see,” which is a valuable lesson that companies should apply to data access and security.

In the digital-age when better enterprise technologies become more available, securing networks and the data they protect must continue to be the highest priority. By applying proper security methods like out-of-band authentication, user access rights, and even hiding the network entirely, organizations can fortify their most valuable assets and information against the threat of intrusion and theft becoming increasingly apparent.

About the Author

Eitan Bremler is responsible for overall global Marketing and Product Management activities of Safe-T including product strategy and roadmap, product marketing, positioning, go-to-market and corporate marketing. Eitan brings to Safe-T more than 15 years’ experience in marketing, product marketing and product management roles. Prior to joining Safe-T, he held multiple product management and product marketing positions at Radware and Radvision an Avaya company. Prior to working for the RAD group, he served as an officer in the Israeli Intelligence Corps unit 8200.Eitan has diverse technological, field engineering, product management and marketing experience including design, implementation and launching networking, collaboration, and security solutions.

December Patch Tuesday

Updates for Windows, Office, .Net Framework, Adobe, Firefox and More

by Chris Goettl, Manager of Product Management, Security, Ivanti

If you saw the Patch Tuesday forecast for December, the reality turned out to be fairly close to what I predicted. There are only a few surprises and additional concerns to note.

December Patch Tuesday Summary:

- Microsoft released a total of 17 updates resolving 39 unique vulnerabilities. They resolved one zero-day and one publicly disclosed vulnerability. Affected software includes Windows, Office, SharePoint, .Net Framework, Exchange Server, and the browsers of course. There is also a Flash update for IE that was released earlier, but make sure you include this in your maintenance as it resolves some zero-days from Adobe.
- Adobe released a critical Acrobat and Reader update resolving 87 unique vulnerabilities. Adobe also led up to Patch Tuesday with a November 20 and December 5 release of Adobe Flash Player resolving two zero-day vulnerabilities.
- Mozilla released updates for Firefox and Firefox ESR resolving 11 unique vulnerabilities.

Microsoft resolves one zero-day vulnerability in the Windows kernel (CVE-2018-8611) which can allow an attacker to execute an Elevation-of-Privilege, enabling the culprit to run arbitrary code in kernel mode. The attacker would first have to log on to the system then run a specially crafted application to take control of the affected system. This vulnerability exists in all currently supported Windows operating systems from Windows 7 to Server 2019. Exploitation has been detected on older OSs already, but the Exploitability Index is rated as a 1 for Windows 10 and Server 2019.

Microsoft has resolved a publicly disclosed vulnerability in .Net Framework (CVE-2018-8517) that could allow a denial-of-service in .Net Framework web applications. The vulnerability can be exploited remotely without authentication by issuing a specially crafted request to the vulnerable application. The vulnerability is rated as Important likely due to complexity to exploit, but it has been publicly disclosed, meaning enough information has been revealed to the public to give a threat actor a head start on creating an exploit to take advantage of the vulnerability. Public disclosures increase the odds a vulnerability will be exploited.

Ensure you have deployed the latest Adobe Flash Player updates.

Leading up to Patch week Adobe has resolved two zero-day vulnerabilities in Flash Player. On 11/20 CVE-2018-15981 was resolved in APSB18-44. The vulnerability has been seen in live exploits by crafting a Flash .swf file to take advantage of the vulnerability and install malware.

On December 5 another Flash zero-day (CVE-2018-15982) was resolved in APSB18-42, which has been observed in a widespread campaign that was exploited through ActiveX embedded in a Microsoft Office document.

Priorities:

- Microsoft operating system updates are urgent this month with the nasty zero-day vulnerability in the Windows kernel (CVE-2018-8611).
- Adobe Flash for Desktop, IE, Chrome and other variations are urgent with two zero-day vulnerabilities. Systems can have multiple instances of Flash Player, so ensuring you can update all of them is very important. CVE-2018-15981 was resolved in APSB18-44 and (CVE-2018-15982) was resolved in APSB18-42.
- Adobe Acrobat Reader and Acrobat resolve a high number of vulnerabilities and should be updated as soon as possible.
- Mozilla Firefox resolves several critical vulnerabilities and warrants some attention as well since the browser is an easy user-targeted entry point for attackers.

In other news:

Oracle CPU in January – Keep in mind Java SE 8 is reaching the end of public updates in January 2019. Java SE 11 is the next planned long-term support release. If you have not already started, that is the ideal migration path for long-term support. If you cannot move yet, Oracle will be making private updates available for an additional cost.

About the Author

Chris Goettl, is director of product management, security, Ivanti. Chris is a strong industry voice with more than 10 years of experience in supporting, implementing, and training IT Admins on how to implement strong patching processes. He hosts a monthly Patch Tuesday webinar, blogs on vulnerability and related software security topics, and his commentary is often quoted as a security expert in the media. Chris can be reached online at chris.goettl@ivanti.com, on Twitter @ChrisGoettl and at Ivanti's website: www.ivanti.com.

Could Censys serve as a threat intelligence collector?

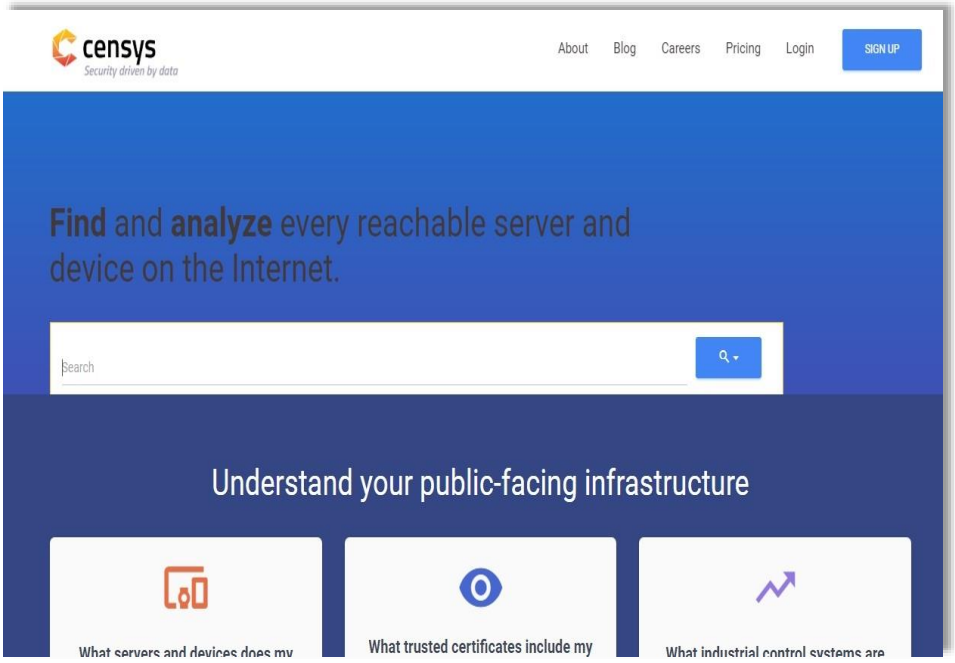
By Milica D. Djekic

The fact is so many visible web search engines could offer you a chance to explore the internet widely and the similar case is with the Censys crawler being located at the web address as follows www.censys.io. This emerging technology would provide you an opportunity to deal with the security driven by data and it would be a quite suitable crawler for finding almost anything being accessible through the surface internet. In case you need the Censys to gather the threat intelligence – it would be possible in case you smartly choose an appropriate keyword. Once you experience this security tool you would see how far away you can get with so. The point is the Censys would give you an option to discover so many IP addresses being correlated with so many different keywords, so do not get surprised if you get an access to some organized crime or terrorist visible web nest. It's well-known that once you obtain someone's IP address – there would be nearly limitless opportunities to make a breach to such a system using some of the hacking tools. The aim of this effort is not to discuss how we could develop the good attack strategy, but rather it should suggest us how we could discover the web vulnerabilities applying such a security crawler. So many security researchers would use the Censys to search hard for threat's forums, discussion groups and websites. They would commonly find a plenty of helpful information that could guide some defense forces to obtain more useful findings and make a decision on how they could tackle some concerns. From that perspective, the Censys is a powerful security tool and at some level – it could serve as a great threat intelligence collector. The fact is that so many threats' activities would not get accessible through the visible web and we would need to rely on the deep web in order to see what is happening there. So, how could Censys serve for those purposes?

As it's well-known, the majority of threat intelligence could get found below the surface and the Censys itself can grab only data being the part of the visible web. It would use the quite popular Z-map algorithm and it would cope with the wide search only. In other words, this sort of search engine would not go below the internet surface. For instance, the deep web browsers such as Tor would deal with the deep search and they would get capable to look for the .onion websites being the part of the well-encrypted and anonymous project. So, our question here would be if we could correlate such a powerful crawler as Censys is with some kind of a deep web crawling. If that would get feasible – we could call the Censys the real threat intelligence collecting service. We believe that one day we would get such a sophisticated search engine that would get able to detect the IP addresses of the well-hidden parts of the internet. At this stage, it's still a quite good idea and we hope that the brilliant minds that have created the Censys could go a step deeper. Well, it appears that the Censys is quite capable to gather the findings about the threats at the visible level and we need more hard work as well as strategic approaches in order to make the deep web solutions getting demystified.

Once the criminals and terrorists lose their well-hidden oases – the world would get a safer place and in our opinion, the crawlers as a Censys could provide us with such an option. Why is that the fact? First, if you get the security tool that could discover the both – surface and deep IP addresses – you would get no difficulties to trace the bad guys and expose them in order to conduct some sort of the case. It's well-known that the systems as a Tor are role-based, so in order to get an access to someone's communications – you would need to get permissions to login to such an account. Maybe we could learn from each other. How? Well, for a certain keyword being with the Censys – you would get some kind of data being helpful for a security research. Also, if you get the access to someone's anonymous account you would need the feedback information in order to get his location with the web. In other words, what we need is a tool that would offer us an opportunity to see the both – someone's communications as well as his IP address. Dealing with someone's IP address means that you can locate that machine and expose such a system for the investigative purposes. We know that the modern technology would go so, so far away and so many intelligence communities would cope with such a sort of capabilities. What we need at this stage is something as a Censys that would serve as a deep threat intelligence gathering tool. The point with the Censys is that it's publically available and at this level – it can offer a lot to the security researchers. If the guys from the Censys project make so significant improvements and get how they could scan the deep internet as well – that would be the good news to the security community, so far. In our belief, that could get quite possible as the security researchers already know a lot about the both technologies.

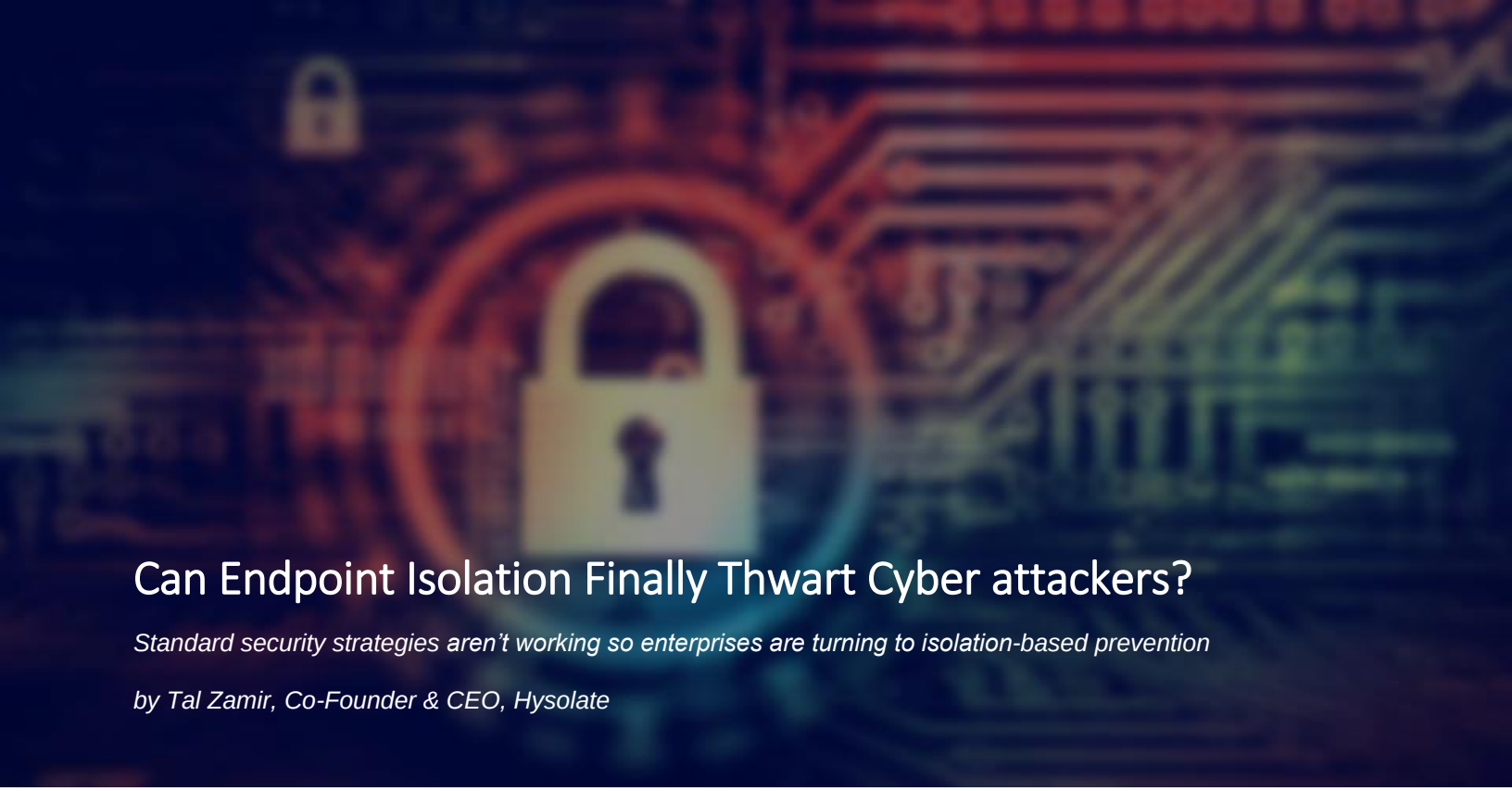
The Censys is the young and quite promising project that could get developed in full to serve



as a powerful threat intelligence collector. We believe that such a security tool deserves a lot of attention and support in order to get better, stronger and deeper. At some stage, the Censys could get recognized as a quite convenient IoT search engine, but in the practice – it would deal with a plenty of security applications. As it's still at its beginning – we believe that the next decade of its development and deployment would bring us a lot of new ideas and the folks from that project would know how to make their solution getting much smarter and more effective.

About The Author

Milica D. Djekic is an Independent Researcher from Subotica, 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 and Cyber Security Summit Europe being held in 2016 as well as CyberCentral Summit 2019 being one of the most exclusive cyber defense events in Europe. She is the member of an ASIS International since 2017 and contributor to the Australian Cyber Security Magazine since 2018. Her fields of interests are cyber defense, technology and business.



Can Endpoint Isolation Finally Thwart Cyber attackers?

Standard security strategies aren't working so enterprises are turning to isolation-based prevention

by Tal Zamir, Co-Founder & CEO, Hysolate

Endpoints are a favorite target for cyber attackers. They're also the Achilles heel of any enterprise's security strategy. As studies show, endpoint vulnerabilities are only getting worse as attackers get more sophisticated and employees unwittingly expose their devices to risk. Clearly, the standard security strategies of years past (e.g. using antivirus scanning and restricting web browsing and external devices) can't thwart these attacks. That's why organizations are changing their focus to isolation-based prevention.

In recent years, four isolation approaches have emerged: Virtual Desktop Infrastructure (VDI), remote browsing, application sandboxing and virtual air gap. Many organizations are struggling to understand which is best for their company. Here's an overview of the four methods' pros and cons.

1. VDI: Centralizes Management but Easy to Compromise

VDI entails accessing server-hosted desktop images from remote thin or thick clients. It gained Traction because it makes IT provisioning and management easier. In addition to employees using VDI, some businesses use it to allow third-parties "controlled" access to corporate assets. Others use VDI servers as "jump hosts" for IT admins and privileged users when managing the enterprise crown jewels.

But VDI is far from the Holy Grail when it comes to endpoint security:

- Malware can still compromise software on the VDI desktop image and lead to organizational risk, such as malicious emails exploiting a vulnerability on the VDI operating system.
- Attack vectors on thick client and personal devices, including external hardware, Internet access or other applications, can be easily exploited to compromise the machine and control the VDI session.[1, 2]
- User productivity takes a hit. VDI sessions require an active network connection with sufficient bandwidth to the VDI server. It doesn't allow offline

work and, when online, performance is often visibly slow.

2. Remote Browsing: A Partial Solution

Technically similar to VDI, remote browsing allows Internet use via a browser application running on a locked-down virtual machine in the cloud. It prevents exploitation of browser-based vulnerabilities on the local machine, which is valuable.

Challenges remain, however:

- It leaves attack vectors exposed. As the name suggests, remote browsing doesn't cover attack vectors such as applications, external hardware and OS vulnerabilities, through which attackers can gain full control of the endpoint device.
- Browser performance suffers. End users get a slower and less interactive experience as content is displayed as an image or video stream on the local workstation.
- User experience is degraded**.** Browser interoperability and other applications' browser plugins affect productivity. For example, many leading conferencing applications don't work well with remote browsing. The Internet connections go through an additional network hop, adding latency to website interactions.

2. Application Sandboxing: Limited In Coverage

Application sandboxing isolates prominent attack vectors by executing each application in its own sandbox using virtual machines (VMs) or other application isolation techniques. It contains threats coming from the sandboxed application and prevents them from affecting the OS. Unlike remote browsing, there's no network-associated overhead.

However, while great in theory, application sandboxing can cause more problems than it solves:

- Sandboxing applications doesn't protect against vulnerabilities in the many unsupported applications, the underlying OS, middleware, malicious external hardware and networks, etc.
- There's significant performance overhead, since each instance of the application runs in a separate VM or other containerization solution. With numerous applications running on a typical user's endpoint, this can lead to slow machine performance.
- Separating applications into VMs creates inherent interoperability issues among applications that are reliant upon interacting within a single OS. Because every application is customized to run in the sandbox VM OS, each new version has to be explicitly adapted for that sandbox platform. This makes it time-consuming and costly to keep applications up to date. It often results in delayed security application patches and, therefore, increased risk.

4. Virtual Air Gap: Full Isolation

Virtual air gap is an emerging approach that is akin to physical air gaps, where there are separate physical machines dedicated for classified usage. Virtual air gap uses a single physical machine to deliver the same top-grade security. Each endpoint device is split into multiple isolated virtual OSes. It works by creating a security platform that runs below the OS on the endpoint hardware itself. With virtual

air gap, each environment runs locally, side-by-side with full separation.

Virtual air gap removes some of the obstacles other approaches introduce:

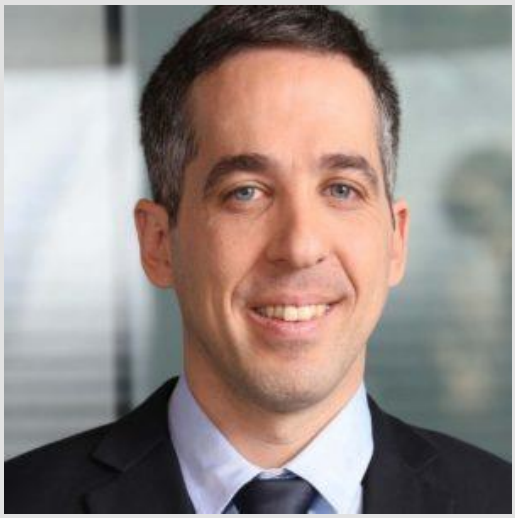
- Attackers who penetrate the endpoint's corporate or personal virtual desktop, in which IT may have enabled Internet and external device access, cannot see or control the sensitive VM**.** Compromises within the exposed environment, via any attack vector, remain contained within that VM. The other VMs are unaffected.
- Virtual air gap approaches fully isolate access to sensitive resources without limiting the user's freedom**.** Users do their jobs without restrictions or lag times hampering productivity.
- Compatibility issues are rare since all applications within each OS run "as is." Interactions that involve multiple VMs, such as content transfer, are granularly controlled via policy.

With endpoint cyberattacks becoming more sophisticated, it's clear that existing security solutions are no longer adequate for protecting enterprises. Isolation approaches are promising – just make sure you evaluate them for comprehensiveness, security capabilities, impact on user productivity, and best fit with your business.

[1] A Practical Attack Against VDI Solutions

[2] Pentests in Restricted Environments

About the Author



Tal Zamir is co-founder and CEO of Hysolate. He is a passionate entrepreneur and veteran R&D leader with 15 years of experience in the cyber and IT domains. Tal started his official career in the Israeli Ministry of Defense, in which he pioneered multiple mission-critical cyber products. He then joined the leadership team of Wanova – a desktop virtualization startup that was later acquired by VMware. He holds multiple US patents as well as an M.Sc. degree in Computer Science from the Technicon. Tal can be reached at Tal@hysolate.com and on Twitter @TalZamir and at Hysolate's website www.hysolate.com

Application Isolation and Control – A Modern Defense for New Threats

By Fraser Kyne, EMEA CTO, Bromium

The detection method for preventing malware is fundamentally flawed, yet it is still the de facto standard in cybersecurity. Day after day, organizations scramble to protect against a growing number of threats, but all it takes is one piece of malware to go undetected to wreak havoc on IT systems.

Ironically, this was predicted by Alan Turing more than 80 years ago. His work proved no standard algorithm could ever predict an outcome for every possibility without falling into a logical paradox because of the halting problem. The halting problem proves that an algorithm cannot predict from a general description of a program and an input whether the program will finish running or execute forever.

The same logic applies to malware detection. A standard algorithm cannot be relied on to correctly identify every single threat that comes knocking because the volume of threats is large and varied, with previously unseen threats emerging every day.

A detection-based approach deployed by IT teams is akin to casting out a net, where the net will either be so large that it tangles itself, or it won't be cast wide enough and will invariably allow some things to be missed. IT teams are trying to solve this problem by adding more layers to their detection solutions, but all this is doing is casting more nets plagued by the same problems.

Detection-based solutions can Over-complicate security landscapes

Hackers are resourceful, utilizing new tactics – such as polymorphic malware and zero-day exploits – to bypass detection-based software and break into critical IT systems. For example, in the Locky ransomware campaign, hackers customized the malware to execute after the fake document was closed, making it much harder to spot and bypassing the majority of detection-based AV solutions.

Instead of focusing on detection, organizations that are serious about security are starting to rely on segmentation. By segmenting networks and applications, businesses are seeing that they can prevent malware from causing harm and keep data and networks safe.

Segmentation offers businesses protection, but it relies on PCs or applications only having access to limited areas on the network. Early iterations failed to achieve a great uptake, because adding new PCs to this system can be incredibly expensive and time consuming during deployment.

Segmenting IP and sensitive data could also still leave users at risk if they don't isolate the applications that are being used to access this data. Without a solution to these problems, network segmentation has largely failed to get off the ground and detection has persisted as the leading cybersecurity approach.

By focusing on isolation, security Is simplified and end users are protected

Everybody wants to be able to use technology to do more with less. In this instance, it means deploying more effective and reliable cybersecurity solutions. However, detection involves the complex process of "preventing, detecting, and responding", where multiple layers of security are deployed to identify malware before it hits. However, these layers simply aren't sufficient to protect against the volume and sophistication of the ransomware and targeted phishing attacks that are prevalent today. As you might expect, it also creates a tremendous expense.

While there are a few choices available that provide isolation, solutions that do this using virtualization are effectively bullet-proof. While no one can promise 100% protection, virtualization that starts on the chip, stops Meltdown, dramatically limits Spectre and works online or offline, can protect what's targeted the most: endpoints.

Real solutions with a virtual defense

Isolation through virtualization works by allowing applications to open and carry out each task in its own self-contained virtual environment. This means that every tab that is opened in a browser, every Office or PDF document attached to an email, or any file that runs an untrusted executable, will be opened in an entirely isolated virtual environment that's running on the hardware itself. The result is that any threat caused by an action in this environment won't have access to anywhere else on the system and can be easily removed by simply destroying the virtual environment.

This allows users the freedom to download files and open documents, safely, knowing that they are no longer the last line of defense – giving users the ability to click with confidence. In fact, end users can let the malware run, because it doesn't do any damage, and it allows IT teams to get detailed threat analysis. Users can get back to work; recruiters and HR teams can open emailed CVs, marketers can carry out research even if they click on a phishing link, and R&D teams can share downloaded resources without the fear of being stung by malicious files or links.

For organizations using this new approach, there is less worry. Virtualization-based security is being adopted by the giants: HP and Microsoft now use virtualization-based security to protect users. This is just the tip of the iceberg and marks the beginning of a virtualization revolution in security, where users no longer fear opening links and attachments and organizations can let their teams focus on innovation without worrying about making a security mistake.

About the Author

Fraser Kyne, EMEA CTO, Bromium Fraser Kyne is the EMEA CTO at Bromium. Fraser's role has encompassed a wide range of both engineering and customer-facing activity. Prior to joining Bromium Fraser was a Technical Specialist and Business Development Manager at Citrix Systems. He has been a speaker at various industry events on topics such as virtualization, security, desktop transformation and cloud computing. Fraser can be reached online at @Bromium and at our company website http://www.bromium.com.

Three Common Security Mistakes and Best Practices to Eliminate Them in the New Year

By Zach Malone, security engineer, FireMon

During this time of year, we see endless articles projecting predictions for the year ahead. And while predictions can help organizations prepare for potential new technologies, processes and other developments that might impact their business, they can also be wrong. That's why there's tremendous value in looking into the rear view mirror this time of year, rather than guessing what's around the next corner. By assessing common trends that emerged over 2018, you can make the necessary changes and investments to make 2019 a truly happy new year.

With this in mind, here are three common security mistakes that organizations made in 2018, along with best practice recommendations to help you avoid or eliminate them in 2019.

1. Operating with a "Business Trumps Security" Mentality.

From increasingly sophisticated cyber-criminals, to an ever-expanding attack surface, to complicated IT infrastructures, there's no question that today's cybersecurity landscape is complex. So complex, in fact, that some organizations are opting to bypass security altogether rather than devote the time, resources and budget required to implement security properly.

The tug of war between the business and security is especially apparent within DevOps. With the emergence of agile development and continuous delivery, DevOps teams can now develop and bring new apps and services to market faster than ever before. But, security hasn't been able to keep up. As a result, security is often a "bolt on" at the end of application

development processes, if it's considered at all, and the process of provisioning policy rules for new IT assets often slows deployment by days or even months, causing many DevOps teams to perceive security as a "roadblock" to IT deployment.

Best Practice Recommendation: In most organizations today, business trumps security, but neglecting security because it slows down business practices is not practical or beneficial. To align DevOps and security teams and move security from an afterthought to the forefront, organizations must:

- Develop a DevSecOps model, where security teams are fully integrated into the DevOps process from the start, rather than being left as an afterthought. This model allows security professionals to become part of the overall DevOps workflow, creating and implementing security functions, policies and controls throughout the application development cycle.
- Adopt an "intent-based" approach to security, which templatizes and automates how security policies and rules are generated and applied to new IT assets based on the "intent" of each. By understanding the intent of all network assets, security professionals can templatize rules and policies, and automatically apply them to new DevOps deployments.

The combination of DevSecOps and intent-based security greatly increases the probability that IT assets have the right rules and profiles assigned and that DevOps teams can move as fast as they need to without introducing new security risks – in other words, organizations can finally achieve security that moves at the speed of business.

2. Failing to Report on Security in a Way Business Leaders Can Understand.

Security teams often struggle to demonstrate the value their investments and operations bring to the business, prompting many C-level executives to see security as nothing but a cost center. This is problematic for two reasons: 1) security professionals are often left out of business strategy, making it more difficult for them to secure corporate data and systems, and 2) when costs need to be cut, security is often first on the chopping block, leaving organizations vulnerable to attack and subject to compliance fines.

Best Practice Recommendation: Security is a business problem, and one of the best ways to get executives to understand this is by implementing metrics and key performance indicators (KPIs) that illustrate how security spend is mitigating the organization's security and compliance risks – and doing so in a way that business leaders can understand. For example, showcase how a particular security investment helps the organization adhere to industry regulations, such as PCI DSS, HIPAA or GDPR, and avoid compliance fines, which, in some cases, can total millions of dollars. Or, demonstrate how security investments mitigate the risk of a data breach, along with its associated consequences, such as reputational damage and a loss of customers.

It might also be helpful to compare security to insurance policies to help business executives better understand its purpose. People purchase home insurance so they're covered in the event their house is damaged in a burglary, from a fire, from a natural disaster, etc. Most people know the chances of ever needing to cash in on their policy is low, but they don't want to take the risk of going without protection. Security investments work in much the same way. Security teams hope to evade the attention of cyber-criminals, but they want the tools in place to mitigate risk

and make sure their organization is protected in the event of an attack.

3. Mistaking Technology as Security Policy.

Organizations often fall into the trap of defending against new cybersecurity threats with technology procurement. They'll buy the latest and greatest point solution and consider it their security "policy." Not only does this result in complex, costly and difficult-to-manage infrastructures, but it introduces tremendous security and compliance risks.

Best Practice Recommendation: Security policy should extend beyond technology to also include people and processes:

- Technology – Rather than implementing "a tool for every threat," organizations should consider a more holistic approach to security that focuses on using a subset of security tools that are specifically designed to address the organization's unique risk profile.
- Processes – Security policies must include clear, prescriptive processes that help the organization continuously validate that technology is working, learn and follow security best practices, and maintain the desired state of security.
- People – Having a written policy is only worthwhile if it's followed by all personnel – from C-level executives, down to entry-level employees. If executives aren't setting a good example by following security best practices, then the rest of the staff will assume security isn't a priority. A company's security policy should be as important as its mission statement, and it should permeate all aspects of an organization's corporate culture.

Learning from the Past

To stay one step ahead of the bad guys, organizations, vendors and other security organizations need to work collectively and learn from each other. By assessing security wins and weaknesses (both their own and their colleagues') from the previous year, organizations can improve upon their security programs and start 2019 with the upper hand over cyber-criminals, who have held the reins for far too long.

About the Author

With more than a decade of experience, Zach Malone is a seasoned security engineer specializing in cybersecurity, compliance, networking, firewalls, IoT, IPSec, system deployment and orchestration. At FireMon, Zach delivers technical demonstrations and proof-of-concept evaluations to move prospective customers from service assessment to purchase. Prior to joining FireMon, Zach was a security engineer at Cadre Computer Resources Co., where he helped organizations of all sizes design, implement, support and test security products and operations. Before that, he served as a Diamond/Escalation engineer at Check Point Software Technologies and a network administrator at Choate Professional Communications and Infrastructure. Zach attained the CISSP certification in April 2018.Zach can be reached online at firemon@threeringsinc.com and at our company website: www.firemon.com.

Strength through Simplification: Taming Cybersecurity Complexity in 2019

By Zach Malone, security engineer, FireMon

Cybersecurity in 2018 can be best described in one world: complex. Yes, complexity has infiltrated every phase of the cybersecurity landscape this year, from bloated and expensive IT infrastructures, to sophisticated cyber-attack methods, to complicated compliance mandates. The aftermath of the complexity epidemic has caused countless data breaches, exacerbated the cybersecurity skills shortage, and left organizations of all sizes struggling with ineffective security programs.

It's time we right the ship that has been taking on water for years. And I believe 2019 will be the year that cloud providers, security vendors and organizations will all make great strides toward simplifying, yet strengthening, security. Here are three predictions detailing how this will unfold in the New Year:

1. Cloud providers will adopt a "security By default" approach to reduce user error.

In 2018, cloud providers provided tools to secure their infrastructure, and vendors provided tools to secure their products. But there were two problems: 1) lack of an instruction manual and 2) Access defaults set to "wide open." As a result, as more and more organizations moved data, services and workflows to the cloud, configuration errors (which is a polite way of saying "human error" or "lack of knowledge") emerged as the leading cause of cloud breaches.

Configuration errors typically happen in one of two ways: 1) misconfigured cloud-native security controls due to the data owner's lack of knowledge about how to use them properly, and 2) misconfigured internal enterprise security controls, which is common when product and DevOps teams prioritize time-to-market over

Security. (And this gets us back to the two sets of tools with no instruction manual!)

Cloud providers are starting to take steps toward providing users with a deeper understanding of their offerings and related security controls. And, in 2019, we'll also see them implement a "security by default" approach, in which they take the security controls already built into their platforms and ensure they are "on by default."

Simplifying security in this way should reduce human error, along with associated vulnerabilities and gaps in security defenses.

2. Organizations will revert back to Security basics.

In a threat landscape dominated by sophisticated cyber-criminals, advanced malware and an ever-expanding attack surface, many companies have become so overwhelmed with cybersecurity that they are dazed into inaction. Other organizations knowingly opt to risk a data breach or compliance fine rather than put proper security defenses in place, because of the associated complexity and costs. And in other cases, companies have security programs in place, but the complexity of their infrastructure creates vulnerabilities and security gaps that actually introduce risk, rather than mitigate it.

The key to overcoming any of these situations is to start simple, and, in 2019, we'll see organizations prioritize policies and processes that focus on the tried and true basics, such as "AAA": Authentication, think User Directory and Multi-Factor Authentication; Authorization, which handles the permissions a user should have once authenticated; and Accounting, which watches and verifies the integrity of the user's account from internal and external changes.

3. Companies will favor all-in-one security devices over standalone point products.

Most organizations have overbought security technology, resulting in a cacophony of tools that are ineffective or redundant. Realizing this isn't the best approach for security or the business, in 2019, we'll see organizations move to simplify their security infrastructures by replacing endless point solutions with the optimal mix of multi-function security tools and services.

From a vendor perspective, this means that point solutions will continue to evolve into multi-purpose devices. Firewalls are a great example of this progression. The traditional firewall was designed with a singular focus: to protect a company's assets from the outside world. However, thanks to cloud computing, virtualized application deployments, containerization of applications and other new technologies made possible by digital transformation, a concrete corporate perimeter no longer exists, and firewalls have had to adjust, both in purpose and technology.

Today's next-gen firewalls are now responsible for providing organizations with visibility into and control over hybrid environments, automating change and policy management, and ensuring continuous compliance, among a host of other responsibilities. Contrary to what many may think, firewalls are not dead – but they have changed.

Less is more

Cyber-crime attacks are getting more frequent and more effective. To gain the upper hand over malicious actors, we must replace security complexity with a simplified, streamlined approach to infrastructure and operations. Only then can we make cybersecurity programs simpler, stronger and more effective at reducing risk.

About the Author

With more than a decade of experience, Zach Malone is a seasoned security engineer specializing in cybersecurity, compliance, networking, firewalls, IoT, IPSec, system deployment and orchestration. At FireMon, Malone delivers technical demonstrations and proof-of-concept evaluations to move prospective customers from service assessment to purchase. Prior to joining FireMon, Malone was a security engineer at Cadre Computer Resources Co., where he helped organizations of all sizes design, implement, support and test security products and operations. Before that, he served as a Diamond/Escalation engineer at Check Point Software Technologies and a network administrator at Choate Professional Communications and Infrastructure. Malone attained the CISSP certification in April 2018.Zach can be reached online at firemon@threeringsinc.com and at our company website: www.firemon.com.

Cybersecurity for Kids

Sitting on the couch: Talking about security with the kids.

by Pedro Tavares, Founder of CSIRT.UBI & Cyber Security Blog seguranca-informatica.pt

Talking about cybersecurity is crucial these days. Children are born in a cyber age and they represent a weakness from the security point-of-view. Due to that, it's essential to provide them with cyber-knowledge, show what kind of information is available online and how they should protect themselves — after all, education begins early in our lives. This is a concept that many children may not care about, or even understand.

Now is the moment to sit down on the couch with your little ones and start a conversation about online security, for they are now entering a phase of greater independence. We will show them how to keep personal information protected and only expose the strictly necessary information online.

1. Integrity check

Sometimes we like to tell stories, talk about serious subjects or even tell nonsense stuffs.

— "Have you ever said something very bad to a friend and have regretted it?"

Over time, everything was resolved and forgotten.

In the digital world things do not work out that way. We should consider carefully whether or not we should leave certain information displayed online, because when the information is available on the Internet, it will be available for all people to access.

— "Imagine you write nonsense about a teacher. Remember that he can easily to obtain your post and that can have negative repercussions on your future life."

2. Do you know the person you're talking to?

The Internet is a dangerous channel and as proof we can speak about personification. At the moment we have a conversation with another

person over the Internet and it isn't possible to identify if the person on the other side of the computer screen is the person we would most like.

— "If an unexpected message comes from someone you know, be careful. It could be someone representing that person".

[Source]

3. Save your data

We must protect our personal information when using online applications or services, such as a computer game, social networks including Facebook, Twitter or Reddit, and even any kind of website where information can be exposed. Information such as our full name, data of birth, the place where we pick up the bus to go to school, where we live and even what places us typically go to can be used for the most strange purposes by cyber criminals.

Rule of thumb: — ***"If anyone asks for details, don't trust them." Talk to other people you trust, expose the strange situation."***

4. Do not be lazy with your password

It may seem like the easiest thing to do - except enter it and memorize it, right? - But using the same password across all services and applications is a bad idea.

Many services are being hacked; it is a constant. Moreover, many services are hacked because criminals use leaked passwords from other services (called credential stuffing).

— "So, if you use the same password in a hacked online game and in your social network account, you can have your social network account blocked the next day because your profile has also been hacked."

— "Using a strong, complex and difficult guessing password for each system or application you use in your day to day life is the solution. Never use the same password to access two different systems."

5. Use Two-Factor-Authentication (2FA) to keep hackers away

Currently, a large number of online platforms and services, such as e-mail, social networks,

gaming platforms, etc., already have this functionality called multi-factor or second factor of authentication - and therefore, we must strengthen our security with other authentication factors in addition to a simple password.

2FA appears in the form of an additional form where we have to enter a Personal Information Number (PIN) that is sent to us by e-mail or to another device, such as our smartphone, or can be generated by other third-party software such as Google Authenticator.

— "Even if this functionality is not mandatory by the system, we should use it (if available)."

6. Think before you download it

What we don't want is that our computer or our smartphone becomes compromised and used by others. For this reason, before downloading any kind of Internet, be it files, computer game cracks, web browser extensions, applications, or other software, we must validate if they are reliable.

— "We should look at the rating assigned to the program, comments from other users - even an Internet search should be done to validate if the program is trustworthy."

7. Do not share accounts with friends

This may sound natural, but do not share your passwords with friends or colleagues. If your friend is hacked you can also be! Or even, if you and a friend with whom you shared accounts or accesses create a confront /discussion, he can access your account and change the password at some point of anger.

The solution is simple: ***— "If you or a friend of yours wants to use the same service or application you are using, each of you should have your own account and own password."***

8. Always logout

If you use a public computer or some other type of shared device, such as in a public library, shop, or lab, remember to sign out of any accounts you have logged in, otherwise unauthorized people can access your information.

— "Before you leave, make sure you always log out of third-party devices."

Final Thought

Children are living in a constant digital transformation. These tips are just part of the conversation we should have with the little ones. Of course, there are other types of controls to set the limits of browsing, access and even transactions, as we see fit, and this can be very useful.

Nevertheless, these methods are not infallible, and one day the smaller ones will have access to a wider digital world. That is why it is vital that, when that day comes, they are well equipped with the knowledge they need to take control safely.

About the Author

Pedro Tavares is a cybersecurity professional and a founding member and Pentester of CSIRT.UBI and the founder of seguranca-informatica.pt.In recent years he has invested in the field of information security, exploring and analyzing a wide range of topics, such as pentesting (Kali Linux), malware, hacking, cybersecurity, IoT and security in computer networks. He is also a Freelance Writer. Segurança Informática blog: www.seguranca-informatica.pt

LinkedIn: https://www.linkedin.com/in/sirpedrotavares

Contact me: ptavares@seguranca-informatica.pt

The Challenge of Real-Time Cyber Protection

Appropriate Response Mechanisms When a Data Breach Occurs

By John Attala, Director, North America, Endace

There's a huge imbalance between attackers and defenders when it comes to protecting the corporate network. Defenders must protect against a myriad of threats while an attacker only needs to find one vulnerability to gain a foothold into the network. Once past the layers of real-time protection, sophisticated attackers can take their time to accomplish their objectives – whether that is disruption, intellectual property theft or fraud – remaining undetected, often for months.

Inevitably, a skilled attacker will make their way past real-time defenses, however good. The challenge is being able to detect them quickly when they do and respond before they have the time to cause major damage.

Assume Breach

In 2014, Microsoft coined the phrase 'Assume Breach,' which advocates assuming that a breach has already occurred and acting accordingly. It emphasizes detection and response rather than focusing exclusively on prevention. This message, albeit slowly, seems to be starting to filter through.

Last year, Gartner reported that enterprise security spending is shifting from purely prevention towards detection and response, and predicted spending on enhancing detection and response capabilities would be a key priority for security buyers until the end of 2020.

However, judging by the number of breaches being reported, it appears this shift may still not be happening quickly enough. Organizations are regularly failing to detect intruders in time to prevent serious breaches from occurring.

And when businesses do report a breach, it frequently transpires their initial assessment of the breach's impact was under reported. The media is full of stories reporting yet another revised estimate of the scope of a breach. It is not uncommon for breach revisions to continue for months after the initial report.

So why are these breaches happening? And what can be done about them?

The Tyranny of the Urgent

In many cases, the sheer volume of alerts that real-time security tools are generating is overwhelming security teams. So much so, the industry has invented the term "alert fatigue" to describe the problem.

According to McAfee Lab's Dec 2016 Quarterly Threat Report:

"*Most organizations are overwhelmed by alerts, and 93% are unable to triage all relevant threats. On average, organizations are unable to sufficiently investigate 25% of their alerts, with no significant variation by country or company size.*"

In the introduction to his report "A Day in the Life of a Cyber Security Pro" EMA researcher, David Monahan, says:

"Because of the time needed to manually investigate each alert to determine whether it is really critical or a false positive, teams are falling behind on alerts - creating a huge backlog of unworked tickets. This is a strong reason why dwell time for breaches is over six months."

Monahan goes on to say that almost half of alerts generated by security tools (46%) are automatically classified as "critical", one third (31%) turn out to be false positives, and over half (52%) are mis-prioritized.

Curing Alert Fatigue

Put simply, the solution to alert fatigue is to improve the accuracy of the alerts being generated and reduce the time it takes to investigate them.

This means reducing or eliminating false positives and providing better context about alerts so they can be triaged and prioritized accurately. It requires knowing what vulnerabilities attackers might target, and what "crown jewels" most need to be protected so that teams can prioritize response to attacks focused on these.

SIEM (Security Event and Event Management) tools can help, combining information from multiple sources and correlating it with the alerts raised by security tools to give a holistic picture of events. Increasingly, SIEM tools can include data such as Threat Intelligence (TI) feeds and data from vulnerability scans to help identify attacks against vulnerable systems.

AI-based security tools too are following a similar approach, typically ingesting data from multiple sources to help give security analysts greater context around the security events that are detected, and even enabling automated response to many threats – which frees security teams up to focus on more serious threats and to proactively hunt for evidence of intrusions.

The Need for Definitive Evidence

Improving the context around security alerts helps security teams reduce the "noise" and focus on the important threats. But investigating alerts still takes far too long. The problem is that assembling the relevant data to reconstruct events simply takes too long. And investigations are often inconclusive due to lack of data.

This is where full packet capture data can help. Packets provide an indelible record of what an attacker does while they are on the network. Unlike log files, which can be deleted or doctored by an attacker, packet data can be recorded without an attacker knowing it is happening. In the event of data being exfiltrated by an attacker, stolen data can be accurately identified from the packets – allowing security teams to be certain what was taken and who was affected.

In addition, historical network history can be "played back" to detection tools to look for evidence of past intrusions. This adds to the investigative capability teams have and allows them to conduct systematic threat hunting or

scan for evidence of “zero day threat” attacks that might have occurred before new detection rules were available.

Accelerating Investigation and Response

The real benefit of network history comes from integrating it into existing security solutions such as monitoring tools or SIEMs. This allows analysts to pivot directly from an alert to the related recorded packets, streamlining the investigation process and reducing investigation times from hours or days to minutes.

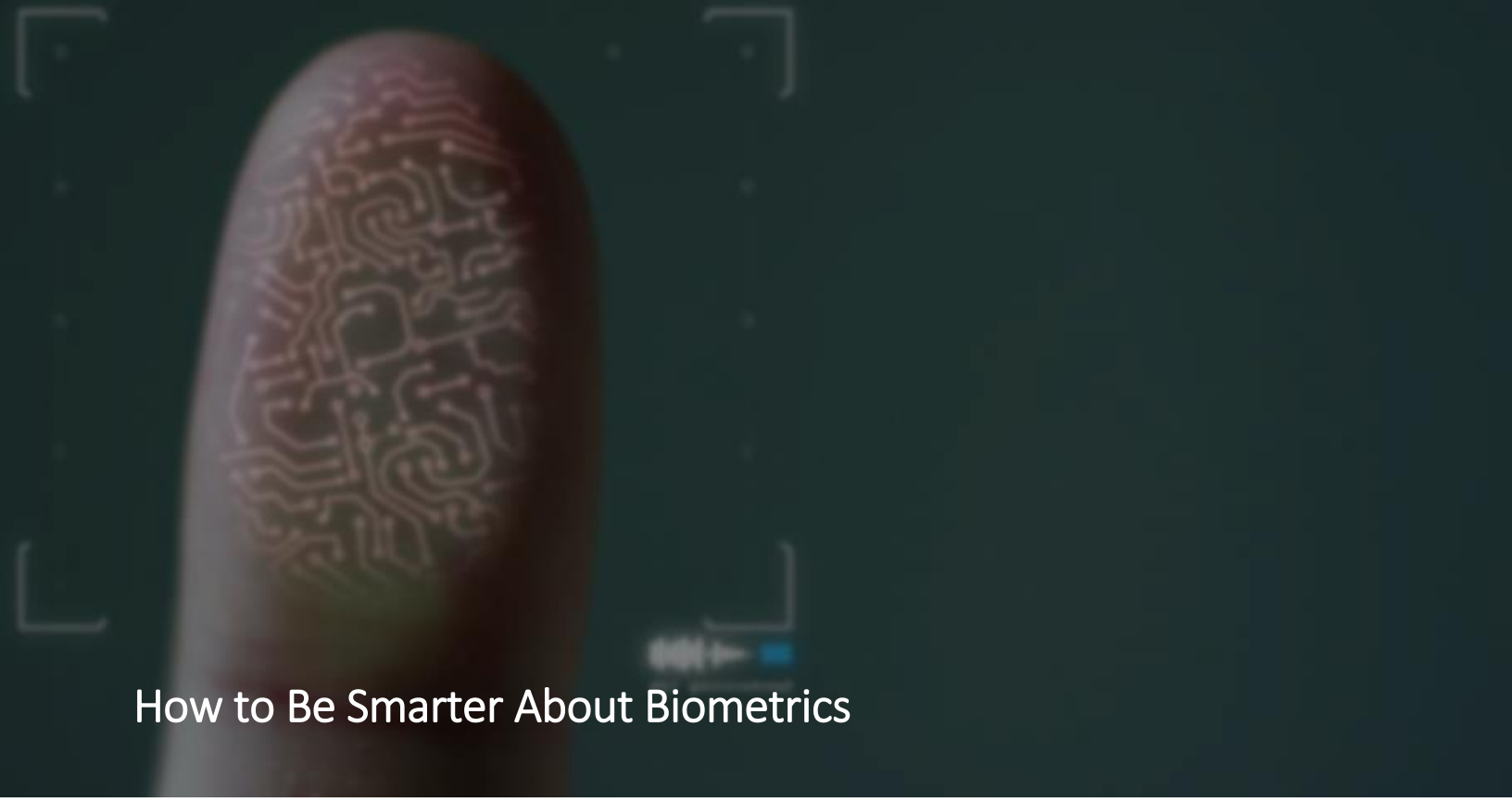
Context and Evidence: The Ultimate Investigation Toolkit

Enriching security tools with context and definitive evidence is a proven recipe for reducing the risk of security breaches. Just as DNA and CCTV have revolutionized criminal investigations in the physical world, packet capture delivers definitive evidence that can revolutionize the cybersecurity investigation process.

And, when a breach occurs, having packet data at hand ensures organizations can quickly and accurately assess the damage, identifying who is affected and responding appropriately.

About the Author

John Attala is the Director - North America for Endace, a world leader in high-speed network monitoring and recording technology. As the North America sales leader, John has played a pivotal role in launching and building Endace’s network monitoring business within the North America. He has more than 20 years’ experience in selling networking and security solutions to Fortune 1000 companies and government accounts—bringing a deep understanding of the market, delivering a consultative, solution selling approach to solve complex problems and improving network security across the globe.John can be reached at Twitter (https://twitter.com/endace) and LinkedIn (https://www.linkedin.com/in/john-attala-8408a9a/) and at our company website (http://www.endace.com) and LinkedIn (https://www.linkedin.com/company/endace/).



How to Be Smarter About Biometrics

Facial recognition—one of the most popular methods of biometric enrollment and customized marketing—will bring us to ultra-surveillance, targeted assassinations and Black Mirror-style oversight…..at least this is what critics of the technology would have you believe. Yet we don't see such dystopian outcomes in commercial authentication and identity verification today. So why are these critics so concerned, and what can security professionals do to alleviate their concerns?

By 2024, the market for facial recognition applications and related biometric functions is expected to grow at a 20% compounded rate to almost $15.4 billion. Already, almost 245 million video surveillance systems have been deployed worldwide, and that number is growing. Video facial recognition technology isn't going away.

Yet as the technology keeps expanding to new segments and use cases, ethical concerns have not settled down—in fact, they've proliferated. Early concerns focused on the surveillance itself: should human beings be watched 24/7? As the Use of CCTV data in criminal investigations proved to have value, though, these concerns have grown to focus on the data that a video stream provides and the inferences that can be drawn from that data.

Machine learning and new predictive techniques, when used to analyze a video stream, can produce findings well beyond facial identity. They can infer emotional state, religious affiliation, class, race, and gender and health status. In addition, machine learning methods can determine where someone is going (travel trajectory), where they came from (national origin), how much they make (through clothing analysis), diseases they suffer from (through analysis of the vocal track) and much more.

Yet like all technology, these techniques are imperfect. They don't always recognize faces accurately: false positives and false negatives happen. Some algorithms get confused if you wear a hat or sunglasses, grow a beard, or cut your hair differently.

Even worse, training data used to develop many early facial recognition algorithms was originally mostly Caucasian, so people of African and Asian descent were not recognized as accurately, which resulted in biased conclusions.

Biometrics themselves are not a foolproof system. Some facial recognition systems can be "hacked" with dolls, masks and false faces. Recently, Philip Bontrager, a researcher at NYU, revealed that he had created a "DeepMasterPrint" fingerprint, which could combine the characteristics of many fingerprints into one "master print" that could log into devices secured with only a single fingerprint authentication routine.

So, the critics of biometrically-based recognition and authentication have a right to be concerned about the weaknesses of an early–yet–broadly deployed technology. A single finger on a pad or a single face seen by a camera should be insufficient to grant access. Biometrics are hackable, and over time it's clear that we'll find increasing exploits that take advantage of known and unknown weaknesses.

Two recent developments that are changing the game for everyone who relies on biometrics magnify the importance of these concerns. This time, artificial intelligence researchers, activists, lawmakers and many of the largest technology companies also express concern.

These two developments, happening simultaneously, are:

1) **Machine Learning in Real-Time:** The advent of machine learning techniques that can act very quickly to make inferences from video data and provide them in near real-time, with convincing conclusions (especially to untrained observers). Not only is the tech really fast—it looks good, too.

2) **Autonomous System Integration:** The merging of these video surveillance conclusions with autonomous systems, so a conclusion from a facial recognition system can lead an autonomous system to take immediate action—no human interaction required.

How might this be used? Let's look at an example. Today's autonomous systems can already take action. For example, when you walk into a room, a home system camera can recognize you and set the lights (or music) to your preferred setting. Alexa can order stuff for you, a car can drive itself, or a building can lock its doors on its own.

Of course, then, activists and tech leaders are concerned that we will give these systems power over human life and agency. What if Alexa calls the cops on your son? What if a system relies on a false recognition to take lethal action? What if the door locking mechanism also incapacitates an intruder? What if they incapacitate a legal resident by false face recognition?

These scenarios, to a limited extent, have already happened. Last March, a self-driving Uber car, which had "human recognition algorithms" built into its video system, failed to recognize a pedestrian and killed her. News reports already indicate that the Chinese government is using such techniques to track minority populations and assign risk factors to citizens, without their knowledge or consent.

Activists point to this use of surveillance and facial analysis technology as an example of how trust can degrade in a society and how specific attitudes might be tracked by unscrupulous players—even in democratic societies with free press and freedom of movement.

Businesses also have their reputations—and their stock prices—negatively affected by unethical activity. More than one company has

discovered that when they violate the trust of partners or customers, business collapses overnight.

However, some moves are afoot to provide protection against bad actors. This month, the Algorithmic Justice League and the Center of Privacy & Technology at Georgetown University Law Center unveiled the Safe Face Pledge, which asks companies not to provide facial AI for autonomous weapons or sell to law enforcement, unless explicit laws are passed to protect people. Last week, Microsoft said that facial recognition married to autonomous systems carries significant risks and proposed rules to combat the threat. Research group AI Now, which includes AI researchers from Google and other companies, issued a similar call.

The problem that the Safe Face Pledge is trying to solve is that autonomous systems don't truly have agency: if a system takes action, there is no one to hold accountable. An autonomous system doesn't lose its job, get charged with a felony or get a report in the file. This is a problem of accountability: who is ultimately responsible?

IT professionals and security experts now fall into the uncomfortable position of pondering the philosophical implications of tech deployment and mediating between the needs of a business and the need to act ethically. Fortunately, there are some simple steps that can be taken to navigate this tightrope.

Three distinct cautionary actions can protect your systems against charges of bias or overreach:

1) **Use Multiple Biometrics:** Don't rely on one low fidelity biometric for high security authentication. Enroll multiple fingerprints via a high-fidelity enrollment mechanism like a certified FBI channeler—not a single smartphone scanner. Even better is to use a two-factor biometric solution that includes scanning of multiple fingerprints, facial and fingerprint, or voice and facial and fingerprint.

2) **Safe Face Pledge:** It's worth checking out the Safe Face Pledge website (safefacepledge.org) to understand the implications of marrying facial recognition to autonomous systems (even a door lock could be autonomous!) and to prevent risks to your employer—or the larger population. Ensure you have educated your business decision-makers on the evident problems with the proliferation of this technology without safeguards.

3) **Put a Human Being in the Loop:** Be very cautious about allowing an autonomous system to take action based solely on a single biometric identifier. . This technology, in many regards, is still in its infancy and can't be fully trusted. Always put a human being in the loop. A person needs to be involved and ultimately be held accountable for decisions that have an impact on your business.

With these protections in place, it's possible to deliver the clear differentiator of real-time facial recognition and autonomous technology to accelerate your business, while simultaneously protecting your business and accelerating your trust with partners and customers.

About the Author

Ned Hayes is the General Manager for SureID, and a Vice President at Sterling. He was educated at Stanford University Graduate School of Business and the Rainier Writing Workshop. He has also studied cyborg identity and robotic ethics at the Graduate Theological Union at UC Berkeley.Learn more about Sterling's SureID: https://www.sureid.com/ LinkedIn: https://www.linkedin.com/company/sureid-com/Twitter: @SureID

Ned is a technologist, identity researcher and author. His most recent novel was the national bestseller The Eagle Tree**,** which was nominated for the Pacific Northwest Booksellers Award, the PEN/Faulkner, the Washington State Book Award and was named one of the top 5 books about the autistic experience.He co-founded the technology company TeleTrust and was the founding product lead for Paul Allen's ARO team at Vulcan. He has also provided product direction for new technology innovation at Xerox PARC, Intel, Microsoft and Adobe and has contributed to a variety of technology patents for these companies

Robert Hannigan: "Engineering-based industries are often not very good at cyber security"

Olexander Hryb, Event Producer at the Institution of Engineering and Technology, met Robert Hannigan, former Director of GCHQ and Executive Chairman of BlueVoyant cyber security, to talk about the main cyber security threats today and what we can do about them.

The UK's Parliamentary Joint Committee on the National Security Strategy published a report in November 2018 saying that UK's national critical infrastructure (CNI) is not sufficiently protected from cyber threats, so how would you describe severity of hostile nation-state actors' offensive intent?

On the one hand, we shouldn't panic about nation-state attacks – they are not the biggest problem in cyber security. But it is true that the US and UK Governments have, over the last couple of years, published details of nation-state attacks against our critical national infrastructure.

The biggest problem is if a nation state is going to do hostile things, it's going to choose our critical national infrastructure; it's going to choose our utilities and energy sector and transport. Those are the kinds of sectors they will go for, and we have indeed found them on some of those networks.

What would be your message to the asset owners of private CNI?

There are two main messages: one is to change the culture in your organization around cyber security; to try to do for cyber what has been done so successfully for health and safety, for example, over the last ten years – to get everybody to take it seriously; to take the risk management process seriously and drive that down through the organization.

The other thing is to understand the supply chain, which is difficult.

What would be your message to the cyber defense community?

I think UK defense has things to learn from the private sector on cyber security, and it has things to teach. UK defense has a key role in our broad defense, and that includes cyber. But it has a long way to go on developing the skills it needs; a lot of those skills are out in the private sector.

What can professional Institutions, including the IET, do to better facilitate cyber defense, considering existing cyber skills shortage and general public cyber hygiene ignorance?

I think the IET and other institutions can do really important work in increasing the pipeline of talent through education, and we need a new generation of cyber security experts. It can help raise awareness.

But particularly in the engineering community, it's always surprising that engineering-based industries are often not very good at cyber security, for a whole range of reasons. But the IET, as a professional body representing engineers, can do a great deal to raise that awareness in the engineering community.

Why you are looking forward to attending the IET's Cyber Security for Industrial Control Systems conference?

The main reason to attend is to share experiences. How do you change the culture in large organization's running the CNI in this country? What's the best practice? What's the experience been – failures and successes – in doing that?

It's a great way to network with other people; we're all facing the same threats and the same problems, and some people have got further towards the solutions than others. It's a great chance to share that.

About the Author

Robert Hannigan will be giving a keynote talk at Cyber Security for Industrial Control Systems, taking place in London on 7 – 8 February 2019. The conference will also include talks from the RAF, Thales, Atkins, Michigan Technological University, Pen Test Partners and the UK's Ministry of Defense. You can see the conference programme and book your ticket at www.theiet.org/cyber-ics

Technology Takeover: How to Secure IoT Environments

By Julian Weinberger, NCP engineering

Internet of Things (IoT) devices continue to transform office environments around the world. From intelligent air conditioning units and smart lighting, to digital assistants and even app-based access control, IoT is having a tremendous impact on business efficiency and productivity. Smart thermostats, for example, can learn worker preferences and automatically maintain an optimum room temperature. As a result, energy savings of up to 60% are possible.

Smart equipment is commonly used to manage everyday tasks such as lighting, booking meeting rooms and hot desking – often via an app on smartphones. Building access is also changing. Conventional keys and code locks will soon be replaced by electronic access control units that allow managers to set their own access parameters. Many of these systems can track usage over time and integrate with other systems to give an overall picture of energy usage or security.

Security Challenges

Most businesses recognize the value of their data and do whatever they can to protect it. Security technology such as a firewall, anti-virus software and network monitoring is commonly deployed to detect threats and keep out attackers. However, these security investments are easily undermined by the introduction of IoT systems. Security measures built into most IoT devices still fall short of the required business standards for protecting proprietary data.

The risk of confidential company data or personally identifiable information (PII) being intercepted by unauthorized parties is extremely high. Symantec found that the number of attacks on IoT equipment rose by 600% last year. Concerned that businesses may be opening themselves up to targeted cyberattacks, the FBI released new advice to help recognize when IoT equipment is compromised and how to mitigate the effects. According to a recent public service announcement from the FBI, “Cyber actors actively search for and compromise vulnerable Internet of Things (IoT) devices for use as proxies or intermediaries for Internet requests to route malicious traffic for cyber-attacks and computer network exploitation.”

Unfortunately, there is no obvious way of knowing when IoT equipment has been compromised. The only option is to regard any

sudden changes in network activity as suspicious. Suspicious activity can include an unusually high uptick in monthly broadband usage, rising Internet bills, a drop off in network performance, anomalous Domain Name Service (DNS) queries or data syphoning off to unfamiliar destinations. As cyberattacks remotely probe devices for weak points, it's important to know if all IoT devices in the office – from CCTV and thermostats to routers and smart building access devices – have the latest firmware updates, robust authentication measures, and strong passwords in place. Network separation of IoT devices is one of the best ways to keep IoT devices away from any of your regular IT infrastructure.

Defense-in-Depth Strategies

To reduce the risk of IoT security compromises, there are many elements to consider. Companies should keep IoT equipment as self-contained as possible so that it is isolated from the main business network. Firewalls should also be set to block traffic from unrecognized IP sources and to disable port forwarding. Another precautionary measure is to switch devices off and on again at regular intervals in order to remove any malware stored in the device memory.

Perhaps the most effective way to mitigate cybersecurity risks is to secure IoT devices with a virtual private network (VPN). A VPN encrypts all traffic entering and leaving IoT devices, rendering the data unintelligible to anyone trying to intercept it. A professional, enterprise grade VPN typically uses military-grade encryption and can manage deployments comprising many thousands of IoT devices remotely.

An example of a common assault against IoT equipment is a distributed denial-of-service (DDoS) attack. A DDoS attack is a malicious attempt to disrupt the normal operation of a digital device by bombarding it with an overwhelming amount of Internet traffic or hacking the IoT device to make it a part of a DDoS attack. VPNs help protect against this kind of attack by shielding the IP address by replacing it with a proxy address. Many other endpoints with the same VPN service will share the same proxy address. This makes it much harder for cyber criminals to pinpoint any individual target device. An IP address shielded in this way also stops intruders being able to track user activity. It also reduces the number of available attack vectors, helping IT support teams to focus defense efforts and increase the chances of malicious activity being quickly detected and stopped before any harm is done.

In summary, government authorities remain concerned about the vulnerability of IoT devices in the workplace. After all, as soon as an IoT device goes live on the Internet it becomes susceptible to viruses, malicious programs, or hackers. Although the FBI issued advice on what to look for and how to mitigate IoT attacks, ensuring that IoT devices are completely protected requires a multi-layered security strategy. A virtual private network is an essential part of a company's defense-in-depth strategy to protect data in IoT environments. As VPNs encrypt and protect the IoT data as it travels from device to platform, attacks are either repelled or the data is completely indecipherable to any outside party that intercepts it.

About the Author

Julian Weinberger, CISSP, is Director of Systems Engineering for NCP engineering. He has over 10 years of experience in the networking and security industry, as well as expertise in SSL - VPN, IPsec, PKI, and firewalls. Based in Mountain View, CA, Julian is responsible for developing IT network security solutions and business strategies for NCP.

The Solution to Cyber Workforce Shortfalls

As malicious software exposures increase, and skilled adversaries continue to meet with success at stealing information, qualified cybersecurity professionals remain scarce.

Regent University's multi-tiered training pipeline is primed to fill the gap

The international shortage of qualified cybersecurity professionals continues to grow at an alarming rate. The Cybersecurity Workforce Study released by ISC^2 in October reported that the cybersecurity workforce gap has increased to nearly 3 million globally, with 498,000 of those job vacancies in North America.

Further, it has been reported that 25 percent of the applicants vying for those positions are not qualified to fill them because they lack practical experience and technical skills.

"Everyone is fighting for the same resource pool," said Stephanie Butts, executive director of Regent University's Institute for Cybersecurity in Virginia Beach, Va., adding that executives competing for those professionals should take a hard look at their IT and cyber defense teams and ask themselves some questions. "Is our staff equipped to face the challenges that are coming down the pike? What is our staff communicating about their ability to prevent, detect and respond to cyber threats?"

While many IT professionals receive commercial certifications, research has shown that they often don't acquire the in-depth skills needed to effectively perform a cyber-defense role.

"What we've seen are privileged users, the actual cyber defenders with the keys to the kingdom, who have the certifications but don't have a total understanding of cyber-defense principles and have had very little hands-on practice," Butts said.

While executives have increased their understanding of how cybercrime can impact

business, many don't understand the vulnerabilities that result from having an underqualified staff. In that regard, they have a false sense of security thinking that the technology they have invested in is protecting their enterprise on its own. While having the right tools is an essential component to an overall strategy, having people with the right skills to use the tools is paramount to success in protection the value chain.

"As long as things are running smoothly, many executives think that their cyber defense is solid. This is a fallacy because in reality cyber is not typically operationalized and IT departments struggle to compete for the necessary downtime to apply patches. As result, the practice of good cyber hygiene quickly turns into normalizing deviations opening the business up to vulnerabilities. Then they get exploited and look at each other and say, 'What happened?'"

Regent University's Institute for Cybersecurity is uniquely positioned to address those problems by closing the gap between classroom theories by providing practical, real-world proficiency.

The institute, home to one of the most powerful and agile cyber simulation laboratories in the region, offers a training pipeline to develop cybersecurity proficiency. The Regent Certified Cyber Practitioner (RCCP) program includes three six-day courses that transform IT professionals into strong cyber defenders by providing trainees with the hands-on experience needed to face tomorrow's cybersecurity challenges.

At the basic level, security and networking essentials are covered with approximately 30 percent of class time involving labs integrated into the range platform as well as actual live-fire scenarios to reinforce security and networking principles.

The intermediate course offers more complex security-based principles including the Cyber First Responder (CFR) curriculum and practical labs integrated into the range platform, as well as actual range live-fire scenarios representing approximately 40 percent of class time.

In the advanced course, approximately 70 percent of class time is spent on the range working through live-fire scenarios as well as a unit on threat hunting and a capstone project on day six creating a comprehensive incident response report based on one of the more challenging scenarios. Regent focuses on incident response reporting that is on par with an internal report produced by a Fortune 500 cyber defense team.

"Our live-fire simulation training provides the tools and capabilities commonly deployed in enterprises found across commercial and Department of Defense entities. We walk trainees through attack scenarios ripped from the headlines and conduct intrusion analysis," Butts said. "We take it a step further by teaching them how to write a comprehensive incident response report so they have the deliverable to communicate the risk to senior leaders and executives."

Regent's courses are offered by a world class trainer holding the SANS GIAC Security Expert (GSE) certification, ensuring that training is delivered by recognized experts in the field.

“Our facilitators share a passion to promote and create a workforce with a solid understanding of theory and the technical skills to be smarter than the adversary and to stay ahead of the threat,” Butts said.

As an academic institution, Regent also offers associate, bachelors and master’s degree NSA-accredited programs in cybersecurity.

Regent University's Institute for Cybersecurity is disrupting and transforming the Cyber Defense industry with a state-of-the-art training platform and world-class trainers. To learn more about commercial training offerings, visit regent.edu/cyber or contact the institute at 757.352.4215.

Source: Regent University


EVENTS

connect:ID 2019

TECHNOLOGY · SOLUTIONS · POLICY

Walter E. Washington Convention Center, Washington, DC, USA

THE PREMIER ARENA FOR NEXT GENERATION IDENTITY SOLUTIONS

IDENTITY RE-IMAGINED

- Through a world-class exhibition connect:ID 2019 will bring together identity technology innovators, industry distributors, and solution providers with thought leaders and policy makers in markets where next-generation secure ID is needed.
- At connect:ID 2019 join: **1500 Event Attendees** | **500 Conference Delegates** | **125+ Exhibiting Organizations** | **150 Speakers** | **3 Conference Streams** | **From over 40 countries**

Exhibition
April 30-May 1, 2019

Conference
April 29-May 1, 2019

Event powered by

science media partners

IBIA International Biometrics+Identity Association

www.connectidexpo.com

12TH OPERATIONAL ENERGY SUMMIT

January 28-30, 2019 | WASHINGTON D.C.

WHY YOU CAN'T MISS OUT ON OPERATIONAL ENERGY SUMMIT 2019!

- Discover the military's operational energy priorities and its implications on the industry.
- Learn about the military's interest in intelligent grids to better inform your strategies
- Discuss DoD's initiatives for cutting operational energy waste and pitch solutions
- Build relationships with military and industry thought leaders to give your company an edge

Executing Future Operational Energy Strategies

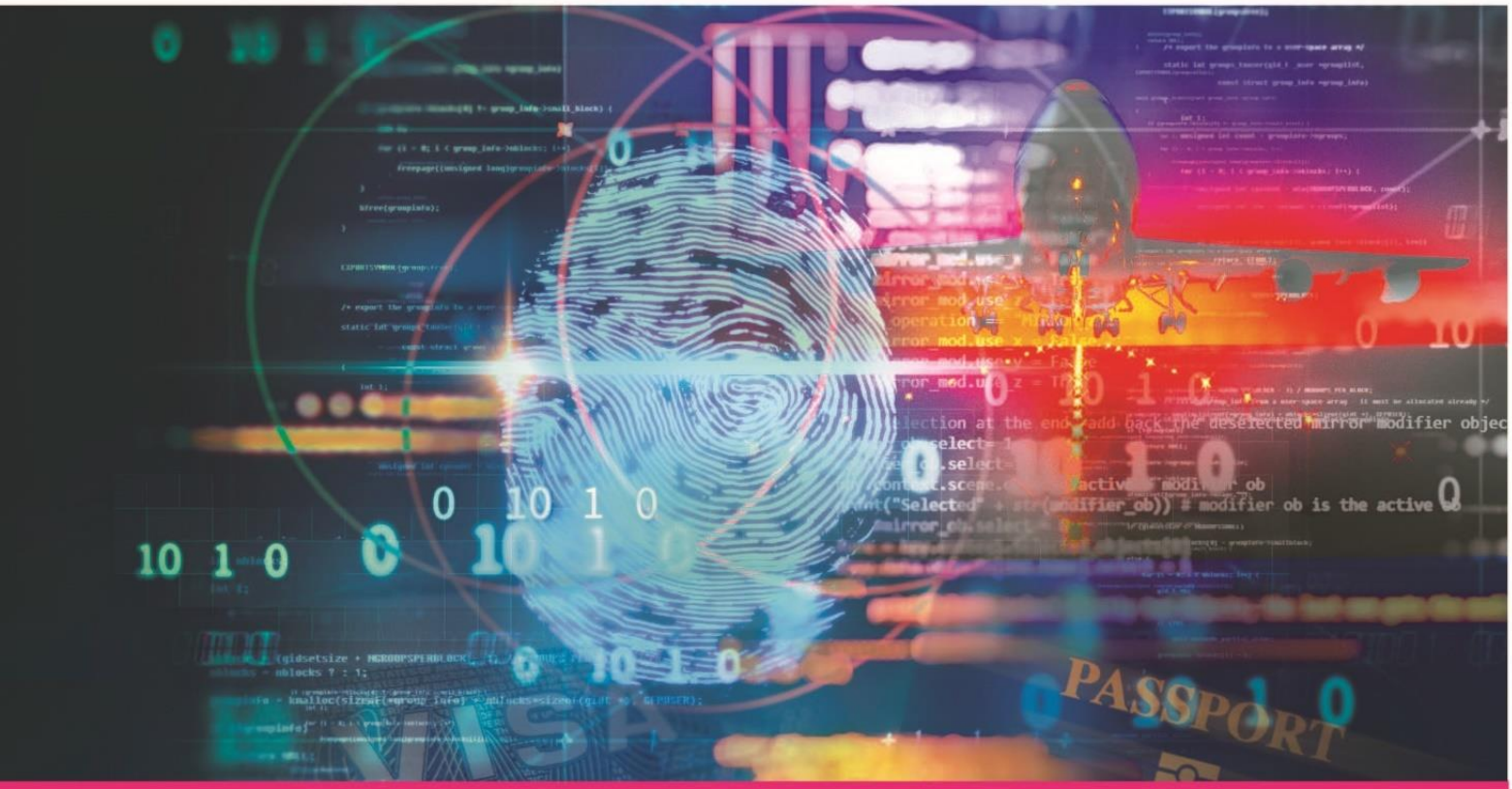
No Cost Passes Available For Active U.S. Military And Federal Government Employees

OperationalEnergySummit.iqpc.com | 1-800-882-8684 | idga@idga.org

IDENTITY WEEK

GLOBAL • TRUSTED • VISIONARY

SDW2019 | PLANET BIOMETRICS 2019 | DIGITAL:ID 2019



EXPLORING NEXT-GENERATION GOVERNMENT, COMMERCIAL & CITIZEN IDENTITY SOLUTIONS

- Identity Week comprises of three world-class events: Digital:ID, Planet Biometrics and SDW - all focused on the concept of identity.
- At Identity Week 2019 join: **3000+ Event Attendees | 500+ Conference Delegates | 200+ Exhibiting Organizations | 250+ Speakers | 3 Co-located Events | From over 80 countries**

IDENTITY WEEK
3 Days • 3 Exhibitions • 3 Conferences
11-13 June 2019
ExCeL, London, UK

Created by

science media partners

SPARK SOMETHING TERRAPINN

www.terrapinn.com/identityweek

DGI EUROPE

Geospatial Intelligence for National Security

28-30 January 2019, Royal Lancaster London

WHERE THE FUTURE OF THE GLOBAL GEOSPATIAL INTELLIGENCE INDUSTRY IS DEFINED

QUOTE **CDM19** TO **GET 15%** OFF YOUR TICKET TO ATTEND*

Source. Analyse. Automate. Share.

THE CONFERENCE FOR GLOBAL GEOSPATIAL INTELLIGENCE LEADERS

JOIN 650+ GEO INT LEADERS INCLUDING:

Lt General James Hockenhull, Chief of Defence Intelligence, **UK MoD**

Jennifer Schnarre, Associate Director for Capabilities, **National Geospatial-Intelligence Agency (NGA)**

Scott Dewar, Director, **Australian Geospatial Intelligence Organisation (AGO)**

Major General Raul Escribano, Deputy Assistant Secretary General for Intelligence, **NATO HQ**

Brigadier Lars Corneliusson, Director of Military Intelligence, **EU Military Staff**

Colonel Orest Babij, Commander, **Canadian Forces Intelligence Group**

Pascal Legai, Director, **European Union Satellite Centre**

Commander Heather Quilenderino, Commanding Officer, **US Naval Ice Center**

PRINCIPAL PARTNER

esri THE SCIENCE OF WHERE

SPONSORS

Raytheon · DigitalGlobe A MAXAR COMPANY · mapbox · earthi · MAPLARGE · planet. · e-geos

* Discount applies to military/ government bookings only

IoT ASIA | 27-28 March 2019

Hall 1, Singapore EXPO

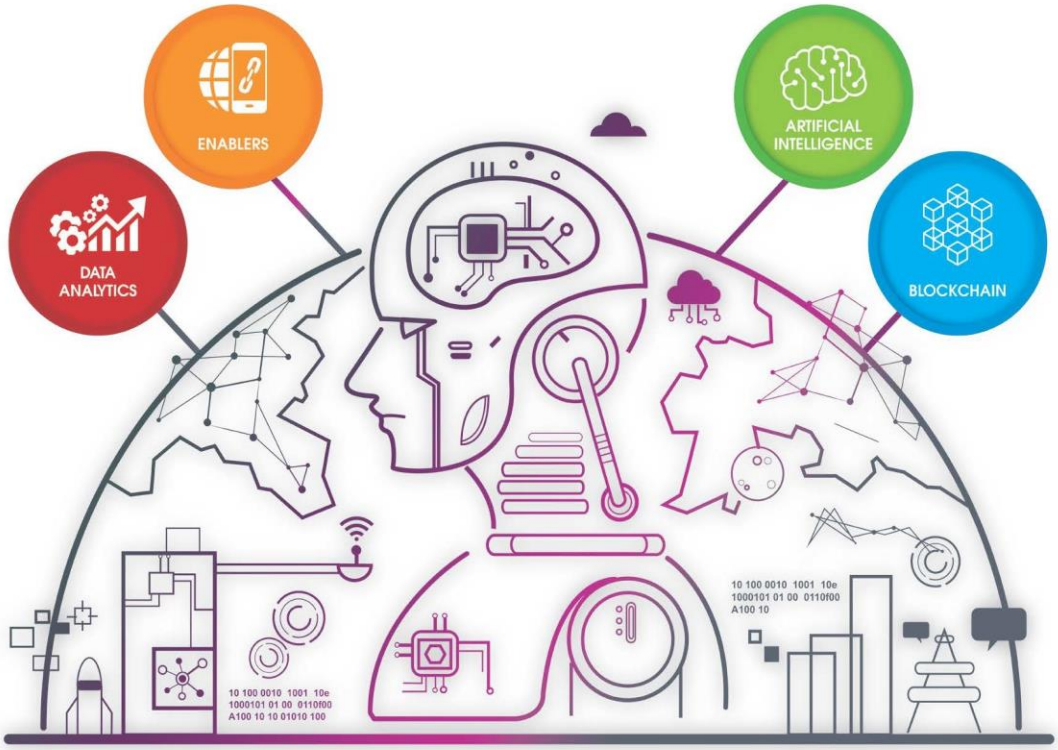
INTERNATIONAL EXHIBITION & CONFERENCE ON THE INTERNET OF THINGS

TRANSFORMING BUSINESSES, GOVERNMENT AND SOCIETIES

SHOWCASE your latest innovations and strengthen your business partnerships

BUILD Value Chains across the IoT Ecosystem

GAIN key insights from best practices and case studies from Industry Leaders



BUILDING VALUE CHAINS

SMART CITIES // INDUSTRIAL IoT

Artificial Intelligence Blockchain Data Analytics Enablers Data Analytics Blockchain

Enablers Artificial Intelligence Data Analytics Blockchain Artificial Intelligence Data Analytics

ENABLERS Artificial Intelligence Data Analytics Blockchain Data Analytics Blockchain Artificial Intelligence Data Analytics Blockchain **ARTIFICIAL INTELLIGENCE**

Artificial Intelligence Data Analytics Enablers Blockchain Data Analytics Artificial Intelligence Data Analytics Enablers

DATA ANALYTICS Data Analytics Blockchain Artificial Intelligence Blockchain Artificial Intelligence Data Analytics Enablers **BLOCKCHAIN**

Artificial Intelligence Data Analytics Blockchain Data Analytics Artificial Intelligence

JOIN US AT THE 6TH EDITION OF IoT ASIA 2019

Interested to Exhibit or Sponsor? Contact us at sales.iotasia@singex.com

www.internetofthingsasia.com • #iotasia

Organised by

SiAA

SingEx

Industry Accolades

ufi Winner of the Marketing Award 2016

2015/16 #IoT Awards

Singapore Experience Awards 2015 Recipient

2014/15 Internet of Things Awards

13th ITS EUROPEAN CONGRESS

FULFILLING ITS PROMISES

Brainport Eindhoven, the Netherlands | 3-6 June 2019

Join Europe's biggest event on Intelligent Transport Systems & Services


BOSCH
Invented for life
Bosch and Genetec.
End-to-end security,
day after day
Find out more at **boschsecurity.com**

ACI
Active Communications International

The 3rd Next Generation Cyber Security for Utilities

Staying a Step Ahead of Increasingly-Sophisticated Cyber Threats

February 13 - 14, 2019
Denver, CO

FEATURING AN EXCLUSIVE TOUR OF
TRI-STATE GENERATION & TRANSMISSION
FEBRUARY 12, 2019

INTRODUCTION

With the value of damages caused by cyber-attacks growing rapidly every year, adopting a new and comprehensive approach to cyber security is more important than ever. Among essential facilities that feel this pressure, few feel it more than our utilities. Cyber incidents have the potential to bring regional economic growth to a grinding halt, especially when they target the lifeblood of our modern civilizations. With threats becoming more sophisticated and gaining better resources, security professionals must continue to adapt and develop their methods of defence and response to ensure the uninterrupted production of our power.

SPECIAL DISCOUNT FOR SUBSCRIBERS

As a supporting partner to 3rd Next Generation Cyber Security for Utilities, ACI are offering Cyber Defense Magazine subscribers a 15% discount on delegate registration until 31st January 2019.

To claim please contact Cheryl Williams on
+44 203 141 0623 • cwilliams@acieu.net

QUOTE DISCOUNT CODE: CYu3MKT

SPONSORS INCLUDE

BURNS McDONNELL

For commercial and sponsorship opportunities please contact Kristina Gyulavári on
+1 929 331 6835 • kvari@acieu.net

BAPCO

The Annual Event 2019

TCCA Critical Communications Europe 2019

12 - 13 MARCH 2019
RICOH ARENA, COVENTRY

TWO EVENTS ONE LOCATION

REGISTER NOW

WWW.BAPCO-SHOW.CO.UK/REGISTER

Reasons to Attend

Bringing together the BAPCO and TCCA events creates an unrivalled opportunity for all those involved in the sector to come together in the UK to network, learn and discuss everything to do with critical communications and public safety solutions.

THE 2019 EVENT IS THE MUST-ATTEND ANNUAL EVENT FOR THOSE INVOLVED IN PUBLIC SAFETY COMMUNICATIONS AND WILL ENABLE THEM TO:

- Network with the communication industry's biggest suppliers
- Compare and source new comms methods, products and services
- Receive free expert advice on the implementation and management of equipment and technologies
- Attend best-practice workshops and pose questions to the experts at the industry's forefront
- Learn how to increase service efficiency and reduce costs
- Do business, make new contacts, and place orders face-to-face

New for 2019

DRONE ZONE

SHOWCASE THEATRE

Our Sponsors

PLATINUM SPONSOR

MOTOROLA SOLUTIONS

GOLD SPONSORS

APD

FREQUENTIS

SILVER SPONSORS

tait communications

3tc SOFTWARE THAT EMPOWERS

@BAPCOEVENT
@CRITCOMMSSERIES

BAPCO ANNUAL CONFERENCE AND EXHIBITION
TCCA CRITICAL COMMUNICATIONS SERIES

WWW.BAPCO-SHOW.CO.UK
WWW.CRITICAL-COMMUNICATIONS-WORLD.COM

automotivecybersecurity.iqpc.com

AUTOMOTIVE CYBERSECURITY

DETROIT

March 27-29 2019

The 9th Automotive Cybersecurity Detroit is a one of a kind networking experience that brings top cyber security experts together with leaders in the automotive industry to discuss challenges in the near and not too distant future.

We will feature key influencers and decision makers from OEMs, Tier 1's, Disruptors, and other external transport industries as we navigate the most critical opportunities and challenges for vehicle cyber security: ECU security, over the air updates (OTAs), V2V/V2I communications, securing embedded systems, and much more!

Attendees Include:

CATERPILLAR

intel

nexteer AUTOMOTIVE

Visteon

LEAR Where Passion Drives Possibilities

MAGNETI MARELLI

APTIV

DELPHI

DURA Automotive Systems

MITSUBISHI MOTORS

veoneer

To learn more, contact Nuria.Frances@iqpc.com or 212-885-2694

2019 CYBER INVESTING SUMMIT™

EXPLORE THE FINANCIAL OPPORTUNITIES AND STRATEGIES AVAILABLE IN THE CYBERSECURITY SECTOR

MAY 16TH, 2019 | NEW YORK

10% OFF ADMISSION CODE CDMCYVEST19

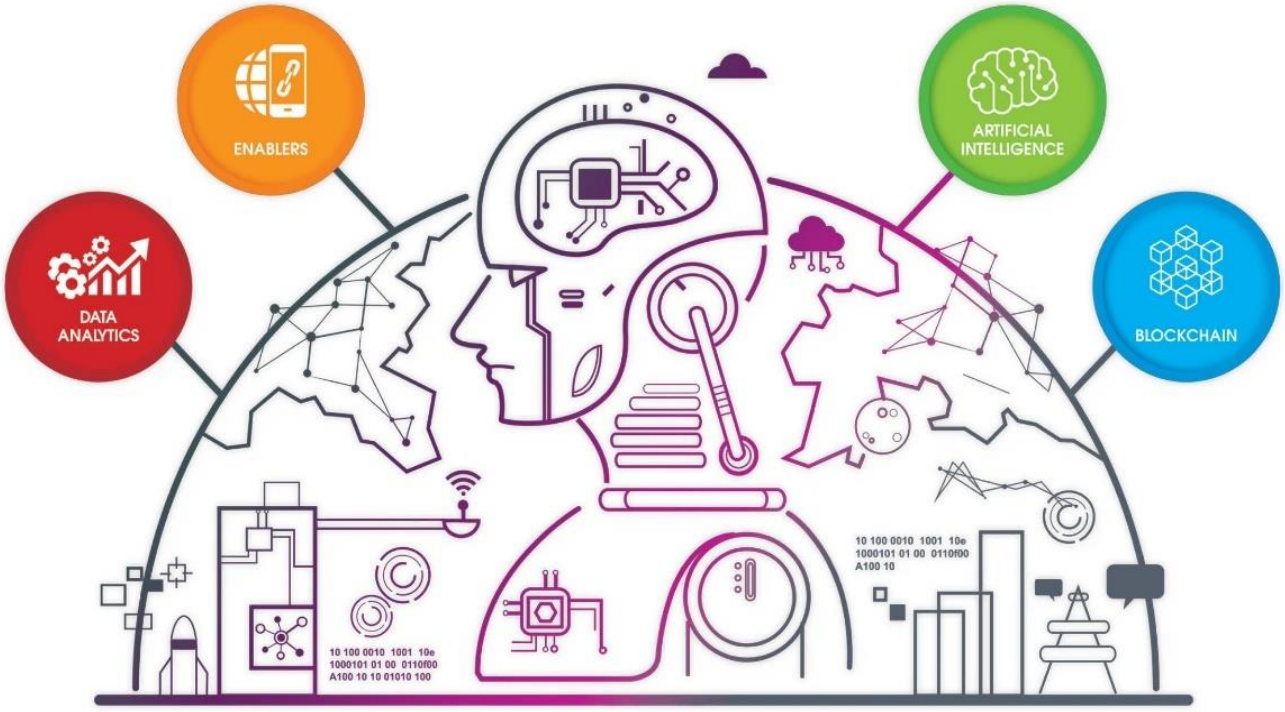
CYBERINVESTINGSUMMIT.COM

IoT ASIA | 27–28 March 2019

Hall 1, Singapore EXPO

INTERNATIONAL EXHIBITION & CONFERENCE ON THE INTERNET OF THINGS

TRANSFORMING BUSINESSES, GOVERNMENT AND SOCIETIES



BUILDING VALUE CHAINS

SMART CITIES | INDUSTRIAL IoT

ENABLERS

ARTIFICIAL INTELLIGENCE

DATA ANALYTICS

BLOCKCHAIN

Gain key insights from best practices and case studies from Industry Leaders.

REGISTER NOW!

www.internetofthingsasia.com • #iotasia

Organised by

SiAA

SingEx

Industry Accolades

ufi Winner of the Marketing Award 2016

2015/16 #IoT Awards

Singapore Experience Awards 2015 Recipient

2014/15 Internet of Things Awards

Simplify and Secure Your File Transfers

It's easy to protect and audit your file transfers. With GoAnywhere Managed File Transfer in your toolbox, you can...

- ☑ Comply with industry security standards like PCI DSS
- ☑ Streamline manual processes
- ☑ Encrypt file transfers with modern technologies
- ☑ Move data safely between on-premises and the cloud

See what GoAnywhere MFT can do in your organization.

www.goanywhere.com/managed-file-transfer

GO ANYWHERE®
Managed File Transfer

RSAConference2019

San Francisco | March 4–8 | Moscone Center

BETTER.

Follow your passion—all the way to RSAC 2019.

What makes you tick? Multifactor authentication? Blockchain? No matter what speaks to you, RSA Conference 2019, March 4 – 8, has what you need to stay on top of the topics affecting your organization—and the industry at large.

- Interactive demos from Splunk, Red Canary, Oracle and hundreds more exhibitors
- Hands-on tutorials, trainings and on-point conversations you won't find anywhere else
- Sharp and relevant keynotes from expert speakers such as **Emily Heath**, VP & CISO, United Airlines; **Stuart McClure**, Chairman & Chief Executive Officer, Cylance Inc.; **Bruce Schneier**, Chief Technology Officer, IBM Resilient, IBM Security | Fellow, Harvard Kennedy School; and our closing speaker, actress, writer and producer, **Tina Fey**.
- Over 550 sessions and seminars that address the issues that matter to you

It doesn't get more up your alley than that. Register today to secure your spot at the Conference that's into everything you are. But hurry—Passes and savings will go fast.

Register now: **www.rsaconference.com/cyberdefense-us19**

Follow us: **#RSAC**

Official Partner

NECTEC
a member of NSTDA

CYBER INTELLIGENCE ASIA

NOVOTEL SIAM SQUARE HOTEL | BANGKOK, THAILAND
27 TH – 28 TH FEBRUARY 2019

Esteemed Speaker Line-up:

Allan Cabanlong, Assistant Secretary, Cyber Security and Enabling Technologies, **Department of Information and Communications Technology (DICT), Philippines**

Wasawat Chawalitthamrong, Head of Crime Relating to Submission of Bids to Government Agencies, **Department of Special Investigations, Thailand**

Chalee Vorakulpipat, Head of Cybersecurity Laboratory, **National Electronics and Computer Technology Center (NECTEC), Thailand**

Fazlan Abdullah, Head, Government Engagement, **CyberSecurity Malaysia**

Budi Rahardjo, President, **Indonesia Computer Emergency Response Team (ID- CERT)**

Dr. Haji Mingu bin Haji Jumaan, Director, **Sabah State Computer Services Department, Malaysia**

Rana Shahzad, Forensics Expert, Cybercrime Division, **Federal Investigation Agency, Pakistan**

Martijn van der Heide, Specialist, **Thailand Computer Emergency Response Team (ThaiCERT)**

Kitisak Jirawannakool, Information Security Specialist, **Thai Bankers Association**

Virag Thakker, Senior IT Compliance Officer, **Agoda**

SPONSORSHIP OPPORTUNITIES AVAILABLE!

To book a stand in our exhibitor hall please contact us at events@intelligence-sec.com or +44 (0)1582 346 706

Sponsors & Exhibitors

Resecurity

For more information visit – www.intelligence-sec.com

Book your place by:
w: www.intelligence-sec.com I e: events@intelligence-sec.com I t: +44(0)1582 346706

INTELLIGENCE-SEC

COMEX
TECHNOLOGY
SHOW 2019

CYBERTECH

THE EVENT FOR THE CYBER INDUSTRY

28-30.1.2019

TEL AVIV

CYBER.

WE LIVE IT. BREATHE IT.

Cybertech Worldwide. Creating Business Opportunities Across Borders.

SAVE THE DATE FOR CYBERTECH TEL AVIV 2019!

Join us on **January 28-30, 2019**, at the Tel Aviv Convention Center for the **BIGGEST CYBER EVENT** of the year!

>> **15,000** Attendees >> **170** Speakers
>> **210** Companies >> **90** Start-Ups
>> **160** Delegations from over **70** countries

Come LEARN, NETWORK, and MAKE BUSINESS with the cyber industry's most prominent players.

Top executives. Government officials. THOUSANDS of great business networking opportunities. All at the forefront of global innovation!

Register today at http://cybertechisrael.com | For more information, please contact cyber@cyberconference.com.

YALE CYBER LEADERSHIP FORUM

THE LAW, TECHNOLOGY, AND BUSINESS OF CYBER SECURITY

February 28–March 2, 2019 • Yale University • New Haven, Connecticut

Learn effective approaches to recognizing, preparing for, preventing, and responding to cyber threats.

"The experience gained from attending the Forum was indispensable and highly effective in understanding and mitigating the overall and ever-emerging cyber security threat landscape!"

— Randall S., Cyber Threat Intelligence Liaison Officer, U.S. Department of Energy

Scholarships and discounts are available for a limited time.
Apply by January 25 to qualify.

WEB *cyber.forum.yale.edu* **EMAIL** *cyber.forum@yale.edu*

Your peers use managed file transfer to solve key business initiatives - but how?

IT professionals discover innovative uses for their secure file transfer solution every day. From tracking weather patterns in Alaska to eliminating third-shift staffing, MFT makes solving their organizational needs easy.

In The GoAnywhere Book of Secure File Transfer Project Examples, you'll discover 20+ ways your peers use managed file transfer to meet ambitious goals and requirements in their company, including:

- A distribution company that uses MFT to send barcode scans to a file repository.
- A healthcare organization that uses MFT to move faxes into an API for processing.
- A manufacturing business that uses MFT to check a server for firmware updates.

Find the inspiration and know-how for your next file transfer project.

GO ANYWHERE®
Managed File Transfer

Visit ***info.goanywhere.com/use-cases-for-mft*** to get the free guide sent right to your inbox.

Meet Our Publisher: Gary S. Miliefsky, CISSP, fmDHS

“Amazing Keynote”

“Best Speaker on the Hacking Stage”

“Most Entertaining and Engaging”

Gary has been keynoting cyber security events throughout the year. He’s also been a moderator, a panelist and has numerous upcoming events throughout the year.

If you are looking for a cybersecurity expert who can make the difference from a nice event to a stellar conference, look no further email marketing@cyberdefensemagazine.com

CYBER DEFENSE TV

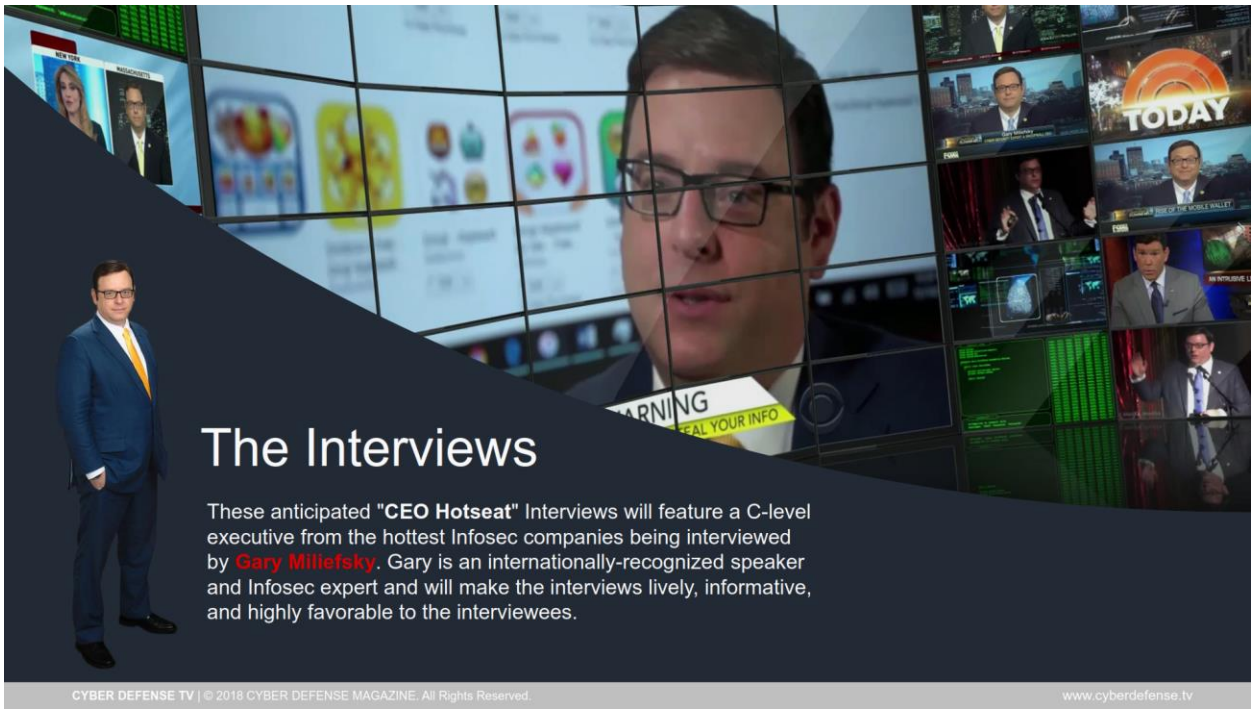
INFOSEC KNOWLEDGE IS POWER

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

At least a dozen exceptional interviews rolling out each month starting this summer…

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

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



Free Monthly Cyber Defense eMagazine Via Email

Enjoy our monthly electronic editions of our Magazines for FREE.

This magazine is by and for ethical information security professionals with a twist on innovative consumer products and privacy issues on top of best practices for IT security and Regulatory Compliance. Our mission is to share cutting edge knowledge, real world stories and independent lab reviews on the best ideas, products and services in the information technology industry. Our monthly Cyber Defense e-Magazines will also keep you up to speed on what's happening in the cyber-crime and cyber warfare arena plus we'll inform you as next generation and innovative technology vendors have news worthy of sharing with you – so enjoy. You get all of this for FREE, always, for our electronic editions. Click here to sign up today and within moments, you'll receive your first email from us with an archive of our newsletters along with this month's newsletter.

By signing up, you'll always be in the loop with CDM.

Marketing and Partnership Opportunities

Banners, E-mails, InfoSec Awards, Downloads, Print Editions and Much More…

Job Opportunities

Send us your list and we'll post it in the magazine for free, subject to editorial approval and layout. Email us at marketing@cyberdefensemagazine.com

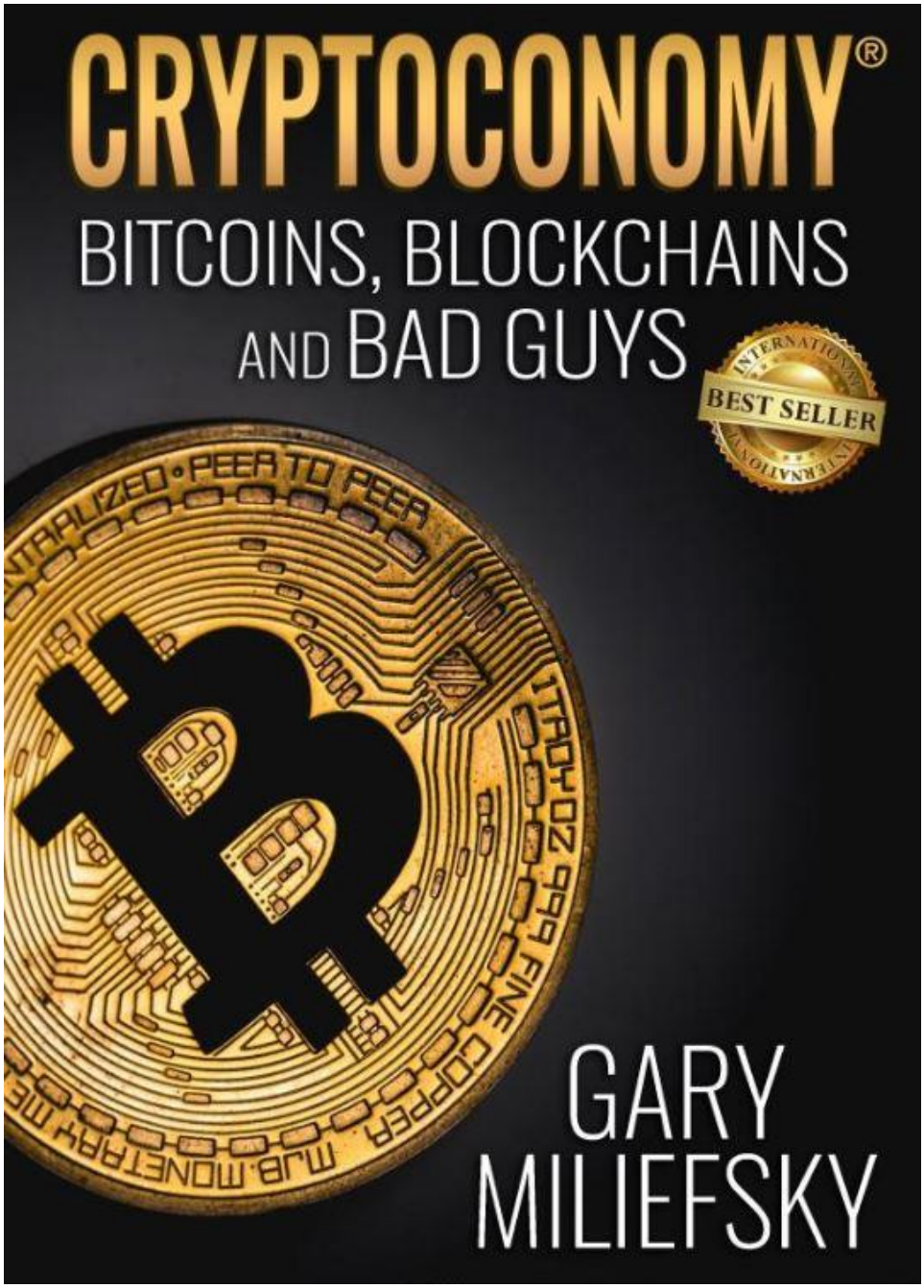
Cyber Defense Magazine

PO Box 8224, Nashua, NH 03060-8224.
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: 01/01/2019

TRILLIONS ARE AT STAKE

No 1 INTERNATIONAL BESTSELLER IN FOUR CATEGORIES



Regent University's Institute for Cybersecurity is disrupting and transforming the Cyber Defense industry with a state-of-the-art training platform and world-class trainers. To learn more about commercial training offerings, visit regent.edu/cyber or contact the institute at 757.352.4215.

Learn more about this program: https://www.regent.edu/institutes/cybersecurity/industry-training/

Space is limited, so register today: https://regent.emf360.com/explore/search

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

ALWAYS FREE
NO STRINGS ATTACHED

Does Your Organization Need MFT Software?

Determine if a secure file transfer solution is right for your situation.

Managed File Transfer (MFT) solutions improve and streamline critical file transfer processes, including encryption, automation, data security compliance, and trading partner collaboration.

But is this solution right for you?

GO ANYWHERE®
Managed File Transfer

You might benefit from MFT if:

1. You need to audit your file transfer activity.
2. You need to comply with data security laws and regulations.
3. You use traditional methods (e.g. FTP or legacy scripts) to send data.
4. You need to easily and securely exchange data with trading partners.

GoAnywhere MFT is a secure file transfer solution that's quick to implement and user-friendly for all.
See for yourself how MFT can help your organization with these four needs and more. Try a 30-day trial today.

Benefit from MFT Today. Start Your Trial. **www.goanywhere.com/trial**


BOSCH
Invented for life
Bosch and Genetec.
End-to-end security,
day after day
Learn more

HERJAVEC GROUP

The sea of connected devices is a dangerous place.
You want a **Shark** on your team.

Top Ranked MSSP & Global Cyber Operations Leader

- ✔ Advisory Services
- ✔ Identity Services
- ✔ Technology Architecture & Implementation
- ✔ 24/7 Managed Security Services
- ✔ Threat Management
- ✔ Incident Response

Robert Herjavec
Star of ABC's Shark Tank
CEO & Founder of Herjavec Group

CYBER DEFENSE GLOBAL AWARDS
CYBER DEFENSE MAGAZINE
2018
WINNER

- Security Company of the Year
- Identity and MSSP Leader