CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

CDM INFOSEC AWARDS 2018

2018 PREDICTIONS

Ransomware

Cryptocurrencies

Nation State Actors

GDPR

IOT Devices

Mobile Malware

Cloud Security

CyberBullying

Cyber Insurance

ANNUAL
CDM
EDITION
2018

Welcome Aboard!

We're honored to bring you our 6th Annual edition of Cyber Defense Magazine (CDM), exclusively in print at the RSA Conference (RSAC) 2018. It's thrilling to our team to know we're 4 years away from coming to RSAC for a decade. And what a decade it has been – we've seen RSAC grow from a few thousand attendees to nearly 50,000 this year – it's literally the biggest INFOSEC show on earth.

Throughout the years, we've watched an evolution of the personal computing and internet revolution whereby new attack and exploit vectors have taken over the scene. Look at the IoT vulnerabilities exploited to create botnets and Distributed Denial of Service (DDoS) attacks. How about the ShadowBrokers leak of EternalBlue leading to the creation of the world's first RansomWorm – WannaCry?

While cybercrime continues to grow, nearly exponentially, there's also been an explosive growth of innovative and new approaches to fighting back against their breaches and data theft. For example, the concept of Honeypots has evolved into deception-based cyber security. The science fiction character 'Hal' from 2001 Space Odyssey, the artificially intelligent computer running a spacecraft is becoming a reality in the field of computer science, where an incredible amount of research has now gone into using a.i. with machine learning and large data sets collected and stored in the cloud, to attempt to get one step ahead of the next threat.

With nearly 600 INFOSEC vendors on the Expo show floor, here at RSAC 2018, you won't find a better place to discover the most innovative, cutting edge, next generation solutions to help you defeat cybercriminals. The days of having a firewall, vpn and antivirus as the three pillars of a secure environment are far from over yet so much more is needed today. You need multifactor authentication, strong encryption, better key management, auditing and penetration testing tools, vulnerability, change configuration and patch management. You need more training, not only for yourself, but for your easily spear phished employees. You need new deception-based security countermeasures and proactive a.i. enhanced threat intel. You need better and faster backup and restore processes and data loss prevention. For all these things, welcome to RSAC 2018 – you've come to the right place.

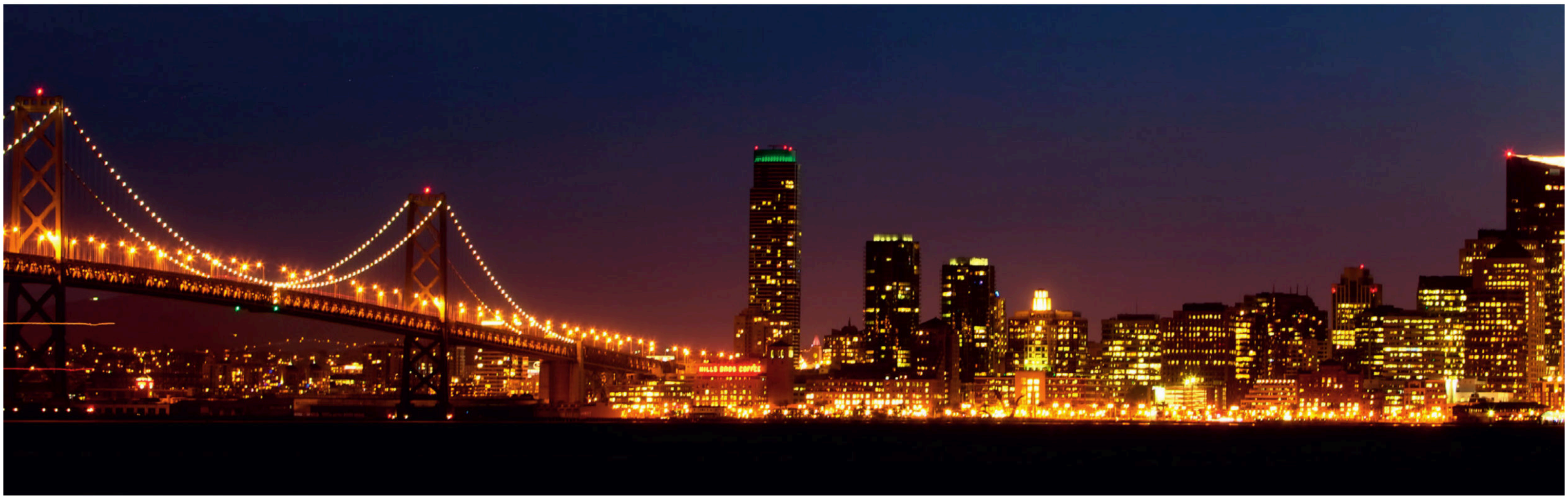
Read on and you'll learn from thought leaders. Inside our annual edition, we have great articles and interesting stories about the activities of two Managed Security Service Providers who are here to help augment your cybersecurity posture and offset risk and regulatory compliance issues when it comes to data protection. We even have an interesting perspective from the SMB protocol experts on how WannaCry could have been avoided. We also share our predictions on cyber threat vectors for the year and so much more. To our faithful readers, we thank you. Enjoy!

Sincerely,

Pierluigi Paganini

Pierluigi Paganini
Editor-in-Chief.

CYBER DEFENSE MAGAZINE
THE PREMIER SOURCE FOR IT SECURITY INFORMATION



CONTENTS

CYBER DEFENSE MAGAZINE is distributed electronally via opt-in e-Mail, HTML, PDF and On-line Flipbook formats. All electronic editions are available for free, aways. No strings attached. Annual print editions of CDM are distributed exclusively at the RSA Conference each year. Key contacts:

PUBLISHER
Gary Miliefsky
garym@cyberdefensemagazine.com

PRESIDENT
Stevin Miliefsky
stevinv@cyberdefensemagazine.com

VICE PRESIDENT OF BUSINESS DEVELOPMENT
Raul Pavao
raulp@cyberdefense.tv

EDITOR-IN-CHIEF
Pierluigi Paganini
pierluigi.Paganini@cyberdefensemagazine.com

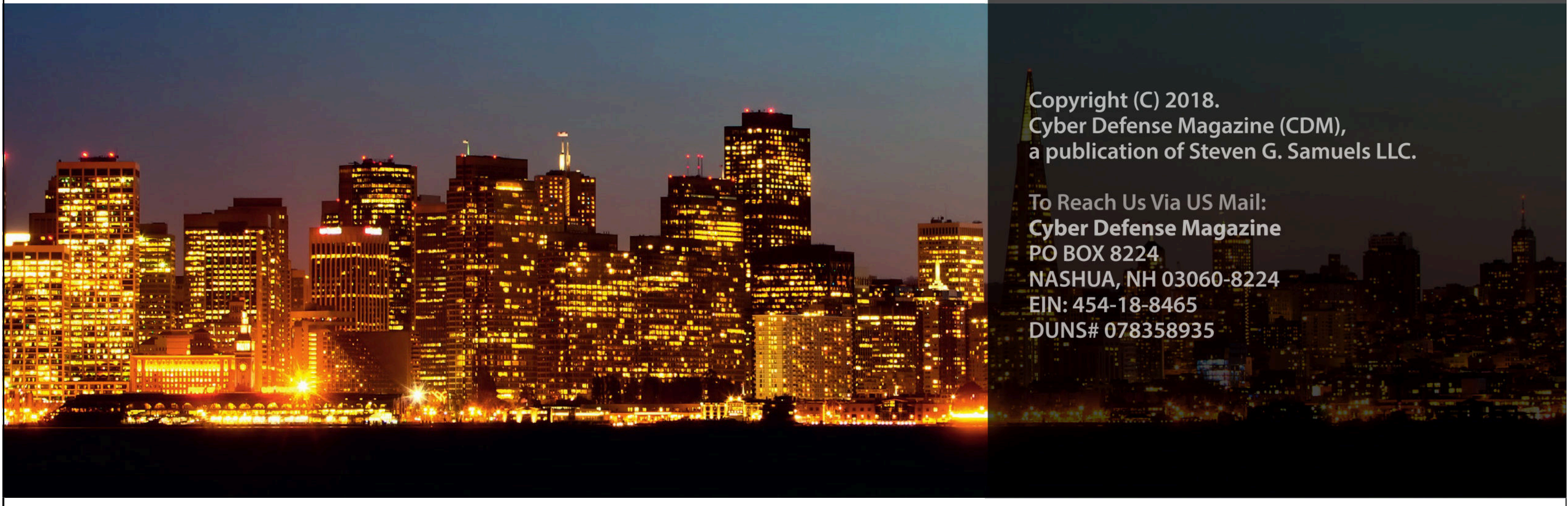
MARKETING & ADVERTISING
Sarah Brandow
sarahb@cyberdefensemagazine.com

CHANNEL PARTNERSHIPS
Jessica Quinn
jessicaq@cyberdefensemagazine.com

CONTRIBUTORS
Jennifer Arcuri
Archie Argawal
Eyal Benishti
Justin S. Daniels
Dr. Galina Datskovsky
Jorge L. Fernandez
Derek Harp
Linda Gray Martin
Sherban Naum
John "Lex" Robinson
Yan Ross
Lou Ryan
Tal Widerman

Interested in writing for us:
marketing@cyberdefensemagazine.com

CONTACT US:
Cyber Defense Magazine
Toll Free: +1-833-844-9468
International: +1-603-280-4451
New York (USA/HQ): +1-646-586-9545
London (UK/EU): +44-203-695-2952
Hong Kong (Asia): +852-580-89020
Skype: cyber.defense
eMail: marketing@cyberdefensemagazine.com



To Reach Us Via US Mail:
Cyber Defense Magazine
PO BOX 8224
NASHUA, NH 03060-8224
EIN: 454-18-8465
DUNS# 078358935

Welcome Letter – RSAC 2018

Forward by
Linda Gray Martin,
Director & General Manager,
RSA Conference

It's that time of year again, when RSA Conference, the world's leading cybersecurity Conference, returns to San Francisco. We bring together professionals from all areas of security—from CISOs to engineers—to give attendees the perspectives and insights they need to stay ahead of the cyber curve.

Taking place April 16-20, 2018, RSA Conference is one of the largest of its kind, with close to 50,000 security professionals coming together with hundreds of media, analysts and exhibitors in one place to talk security.

For more than a quarter of a century we've been dedicated to advancing the field of cybersecurity, and today more than ever, our community finds itself taking center stage as cyberthreats are at an all-time high. Nearly half the world's population is online and information is spreading at warp speed. We're becoming increasingly dependent on the latest and greatest gadgets, which means more of our personal lives are becoming digital, whether we like it or not. Businesses and governments alike feel like they are hanging in the balance and unsure about what steps they must take next to protect their information. With that mindset, professionals in need turn to those of us that can make a difference to stop these threats.

Last year saw an inordinate amount of cybersecurity incidences. From massive breaches to WannaCry ransomware that hit hundreds of thousands of victims globally, including public organizations and large corporations, the heat certainly was raining down on IT professionals. And let's face it, these meltdowns directed all eyes on us and sparked major discussions in board rooms across the world.

But we can leverage this attention to come together as a whole and collaborate on new innovations and approaches to information security. We can make security a lasting board room discussion by capitalizing on our newfound stature to make sure the right policies are being implemented, the right priorities are being set and the right decisions are being made.

This year at RSA Conference, experts in protecting and defending against cybercrime will travel to the Bay Area or join us virtually to discuss common challenges, best practices and new products and approaches to help keep our organizations safe from these attacks. We'll be exploring why **Now Matters** as cyberthreats loom larger than ever, with more opportunities for cybercriminals to strike.

It's time to let the world know what can be done. To inspire businesses, and the entire planet, about the future of cybersecurity. We hope that you can make this year's Conference and leverage the opportunity to connect with industry professionals about the threats facing our industry **right now**. We look forward to seeing you there!

Linda Gray Martin,
Director & General Manager,
RSA Conference

RSA® Conference2018
San Francisco | April 16 – 20 | Moscone Center

WatchGuard
Smart Security, Simply Done.

Make sure to stop by Booth #923

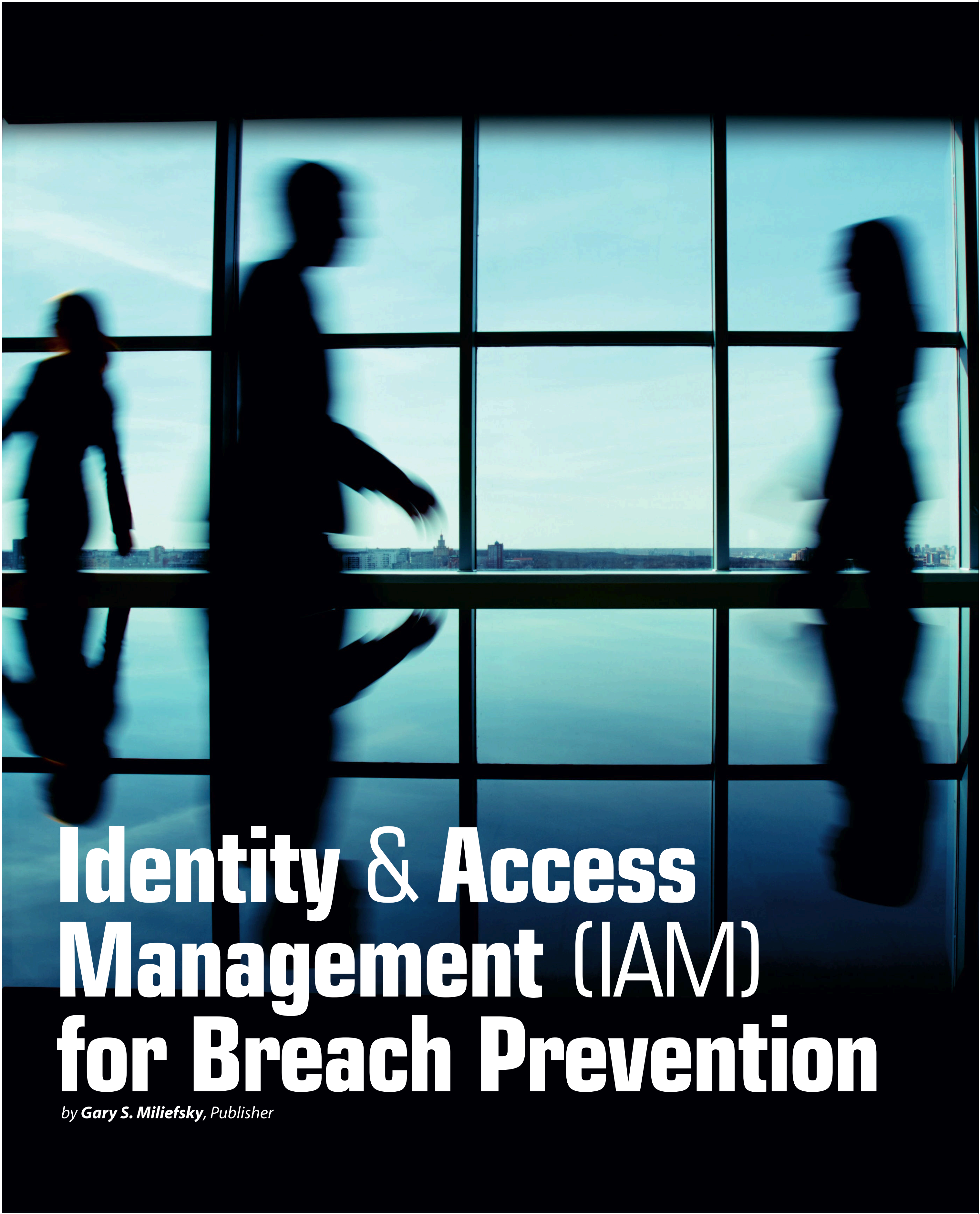
Check out **Marc Laliberte's** RSA Session
Friday, April 20th at 11:30am – 12:15pm
Moscone South 308

Lost in the Ether:
How Ethereum Hacks are Shaping the Blockchain Future

With over $80 billion in total market cap, Ether is the second largest cryptocurrency, only behind Bitcoin. In the last two years, cyber criminals have exploited code flaws, web app vulnerabilities, and social engineering to steal over $100 million in Ether cryptocurrency. This session covers Smart Contracts and the Ethereum Virtual Machine, as well as a history of how these heists have shaped Ethereum.

Specializing in network security technologies, Marc's industry experience allows him to conduct meaningful information security research and educate audiences on the latest cyber security trends and best practices. With speaking appearances at IT conferences and regular contributions to online IT and security publications, Marc is a security expert who enjoys providing unique insights and guidance to all levels of IT personnel.

Marc Laliberte
Security Threat Analyst



Identity & Access Management (IAM) for Breach Prevention

by **Gary S. Miliefsky**, Publisher

As you may recall, I've been keeping a keen eye on Robert Herjavec and Herjavec Group (HG) as an innovator in the Managed Security Service Provider (MSSP) space, starting with my exclusive interview and coverage of Robert Herjavec, which is available online www.bit.ly/CDMRHG. I've enjoyed watching Robert and HG evolve. What I've learned from watching Robert over time is that he knows how to bring in the right people at the right time. As a leader, you look for the best you to surround yourself with. In this case, with Identity and Access Management (IAM) becoming very hot topic in the INFOSEC arena and the consensus that many successful breaches have been enabled by poor IAM hygiene, Robert knew he had to help enterpises fix this problem. Enter IAM executive, Ketan Kapadia, Herjavec Group's VP of Identity and Access Management and keep reading for my recent interview with him about HG's initiatives in the IAM space.

Ketan Kapadia is Herjavec Group's Vice President of Identity & Access Management. He is an accomplished, results-driven executive with experience in information security, consulting, product management, and Identity Management and Access Governance. As VP of IAM at Herjavec Group, Ketan is responsible for driving the direction and delivery of HG's Identity Services which include: Assessment, Design, Deployment and IAM Managed Services. Prior to joining Herjavec Group, Ketan founded Aikya Security Solutions Inc; he also held an executive role as the Director and Chief Architect at Aveksa (acquired by RSA Security LLC). So, who better to speak with about leveraging IAM to stop breaches than Ketan?

My first question for him is about the state of security. Why are there so many breaches after we've seen a plethora of new products and technologies hit the market to help organizations defend against the next cyber threat?

Why is IAM So Important in 2018 and Beyond?

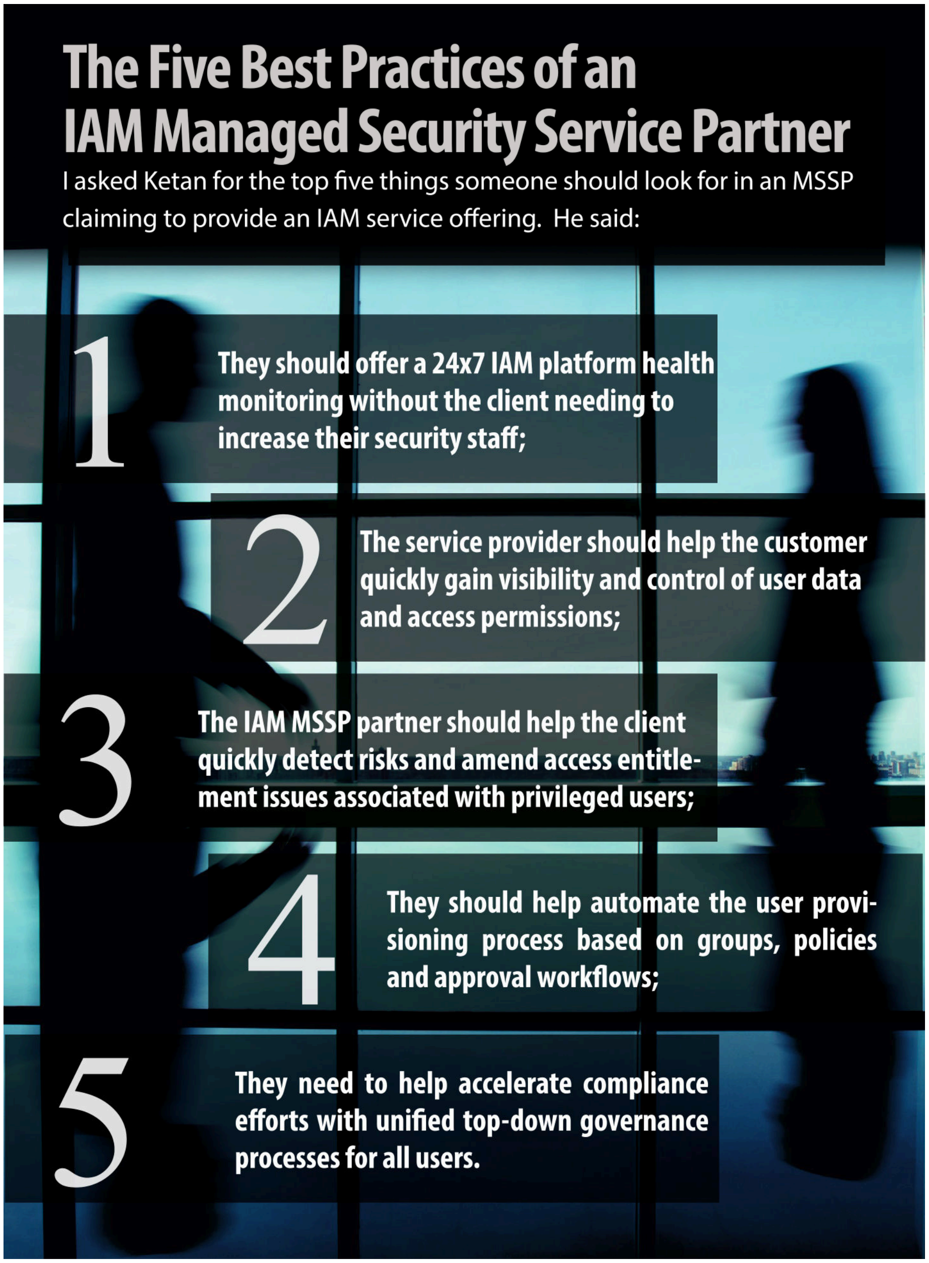
"Gary, your readers need to know what we've discovered at Herjavec Group and it's simply astonishing – most organizations think that security hygiene is based on firewalls, virtual private networks, patch management, vulnerability management and running the latest antivirus products – the reality is that Identity and Access Management is the epicenter of security."

"What is the commonality in most cases of cybercrime and data theft? We need to start putting **people** and their corporate-network centric **identities** at the center of the breach problem – this is all about best practices in IAM, which has been missing from the equation," Ketan told me in our interview.

This was very interesting to me so we dug deeper into his view and their findings. He told me that most organizations haven't created the best practices model for IAM. For example, onboarding users need to get the right access at the right time for the right role. As organizations evolve – shrink, grow, change, we see dynamics in user roles that should follow users. What happens when someone leaves the organization? How do you ensure access is taken away? There's a lot of interesting things we come across showing that the need is to focus on the root that the identity is the central point - then it's about the hygiene of the identity. According to Ketan, "the right person should have the right access at the right time…this is more than just working with IT - it's about getting a process in place and making sure human resources (HR) is also actively involved in IAM."

I also asked Ketan to give me the Herjavec Group definition of IAM because there's so much buzz about it and so many folks confusing other terms such as proxy access management, privileged access management, single sign on and access governance frameworks. He gave me the best answer and simply one word … it's all about **"IDENTITY"**. This is the core of IAM.

Anything an IDENTITY touches, whether it has privileged access to a server or with the shifting landscape in mobile and IoT – it's really about a user and all access by that IDENTITY i.e. that "carbon life form". Who you are as a USER and what you have access to – such as devices, network resources, databases, applications, servers and services.



The Five Best Practices of an IAM Managed Security Service Partner

I asked Ketan for the top five things someone should look for in an MSSP claiming to provide an IAM service offering. He said:

1 They should offer a 24x7 IAM platform health monitoring without the client needing to increase their security staff;

2 The service provider should help the customer quickly gain visibility and control of user data and access permissions;

3 The IAM MSSP partner should help the client quickly detect risks and amend access entitlement issues associated with privileged users;

4 They should help automate the user provisioning process based on groups, policies and approval workflows;

5 They need to help accelerate compliance efforts with unified top-down governance processes for all users.

What is the Best Way to Get Started with IAM Best Practices?

"We like to start out with an IAM assessment. Before deploying our full service offering in this area, it's best to help the clients understand their strengths and weaknesses at Identity and Access Management. In many cases, as part of the assessment our clients have complex regulatory compliance issues to deal with and how people are granted access.

As in most organizations, we find too many manual processes with a lot of hands on work, day to day crunching of info but without having a third party like Herjavec Group taking an independent view, most organizations don't notice where there are dropping the IAM ball - for example, we usually find that HR needs a better user onboarding and offboarding process where they and IT can work together hand in hand. We find this and many other issues to help ensure that best practices will be in place quickly for when someone changes a role or leaves the organization and these credentials won't be left in place as a window of vulnerability.

Depending upon the organization size, it takes typically 6-8 weeks for a solid IAM assessment. We outlined the existing use cases, challenges, processes, gaps and we came up with a best practices IAM plan on risk reduction, security posture improvements and regulatory compliance improvements. We easily find their pain points and phase in the implementation in digestible bite sizes in a strategic roadmap so clients can move towards a best practices in IAM without business disruption."

Ketan Kapadia
is Herjavec Group's Vice President of
Identity & Access Management.

"At Herjavec Group, when it comes to IAM deployment for our customers, we're vendor agnostic and help point out what processes, tools and techniques are best for them. We do a gap analysis from a vendor agnostic approach to accommodate customer specific use cases. Often, it's a multivendor playground with different solutions for different gaps we find," Ketan pointed out.

On being an IAM MSSP Innovator

Starting fresh from an MSSP perspective, I was wondering if HG would do something innovative in the IAM space and they are – the first to offer remote services as IAM managed services which is bleeding edge in the MSSP space. "In most cases, as a trusted advisor and MSS partner, we can handle access management remotely. We're overseeing the IAM platform 24x7, troubleshooting challenges and offering configuration support.," said Ketan.

"We leverage our Security Operations Centers (SOC) for analysis and triage and find that a unique differentiator we offer to clients who have both Security Information and Event Management (SIEM) and IAM Managed Service is that doing both improves visibility and triage significantly. We have the ability to look deeper into the IDENTITY of the user and contextually drive additional information from a SIEM event. For example, based on what we see with this person, they really shouldn't have this access – taking a proactive approach and granular monitoring. Often these issues are usually not visible for most organizations up front which leads to a reactive model rather than preventative model. We offer tremendous value by having the right visibility across SIEM and IAM....better data to drive to the right closure," he said.

Do the Boards and C Level Executives Understand the Need for IAM Yet?

"We've reached an inflection point, where the cybersecurity hygiene is becoming a Board level discussion and IAM is finally making it onto the radar at the Board and C level. It's a great time for us to provide this offering from a perspective of being an assessor, a trusted advisor and a partner of these companies. We don't tell them what to do, we help them discover what tools and technologies will fit their business processes to deploy IAM optimally for security and compliance."

My Conclusion: Now is the Best Time for an IAM Assessment by Herjavec Group

> *"We need to start putting people and their corporate-network centric identities at the center of the breach problem – this is all about best practices in IAM, which has been missing from the equation,"*
>
> **Ketan Kapadia**
> *Herjavec Group*

From my research and what we've learned from Herjavec Group, 'bad' IAM hygiene is a general problem across all markets making it easy for cybercriminals to steal the data from the inside-out, behind the corporate firewall. This is a glaring weak spot in most vertical market sectors which is why we read about breaches, data theft and lost personally identifiable information (PII) records, every day. These growing breaches might have been stopped more proactively, if best practice in Identity and Access Management had already been in place at these victim organizations. Therefore, having an IAM Assessment is a must for all organizations, no matter the size or the industry. The key is to have it done by a third party you can trust who has years of experience providing an independent view and expertise. By using the right tools, the right processes and governance, we can start to get one step ahead of the next breach. Now is the time to look into doing IAM the right way. If you are interested in an IAM assessment by one of the most trusted names in the MSSP space, please email iam@herjavecgroup.com and tell them you found out about this very compelling offering from Cyber Defense Magazine. anytime.

About the Author

Gary S. Miliefsky is the Publisher of Cyber Defense Magazine (CDM). Gary is a globally recognized cybersecurity expert, inventor and founder of numerous cybersecurity companies, is a frequent invited guest on national and international media commenting on mobile privacy, cyber security, cyber-crime and cyber terrorism, also covered in Forbes, Fortune and Inc Magazines. Miliefsky is a Founding Member of the US Department of Homeland Security (http://www.DHS.gov), the National Information Security Group (http://www.NAISG.org) and the OVAL advisory board of MITRE responsible for the CVE Program (http://CVE.mitre.org). Gary is a member of ISC2.org and is a CISSP®. He's frequently writing thought provoking articles at CDM and on LinkedIn as a Top 1% of all INFOSEC LinkedIn profiles and a Top 3% Globally on LinkedIn. Learn more about Gary on our website.

It may not be sexy, but cyber hygiene will be the most important conversation had in 2018.

HERJAVEC
GROUP

On a consumer level, poor cyber hygiene occurs with the use of simple, recycled passwords, which can be easily hacked, or by using default passwords that come with software applications.

At the enterprise level, we expect more – but don't always get it. Good hygiene includes password management, user access and control management and of course, device management.

Poor cyber hygiene can also cause enterprises to fall victim to common cybercrimes such as phishing or other social engineering tactics. For example, if a company uses legacy systems with few security patches, hackers can easily exploit a known vulnerability to gain access.

So how can enterprises improve their cyber hygiene?

"Make sure you're keeping up with patching, vulnerability management, managing rogue assets, controlling privileged accounts, and using multi-factor authentication. These are some key ways to maintain strong cyber hygiene," notes Ira Goldstein, VP of Technical Operations at Herjavec Group, "In fact, many large, complex enterprises are still having trouble with this issue."

It is also highly recommended to invest in proper security awareness training for employees. For example, all employees should be able to recognize an email scam; after all, 91% of cyber attacks are start through email.

Steve Morgan, Founder and Editor-in-Chief of Cybersecurity Ventures, says, "Security awareness training is the most underspent sector of the cybersecurity industry but it will be fundamental to cyber-defense strategies."

If there's one lesson to learn from the data breaches of 2017, it's that large enterprises should be buckling down on cyber hygiene. The reason we saw such damage from Wannacry, NotPetya and the Equifax breach (which resulted in the data compromise of 143 million Americans), was because of unpatched systems.

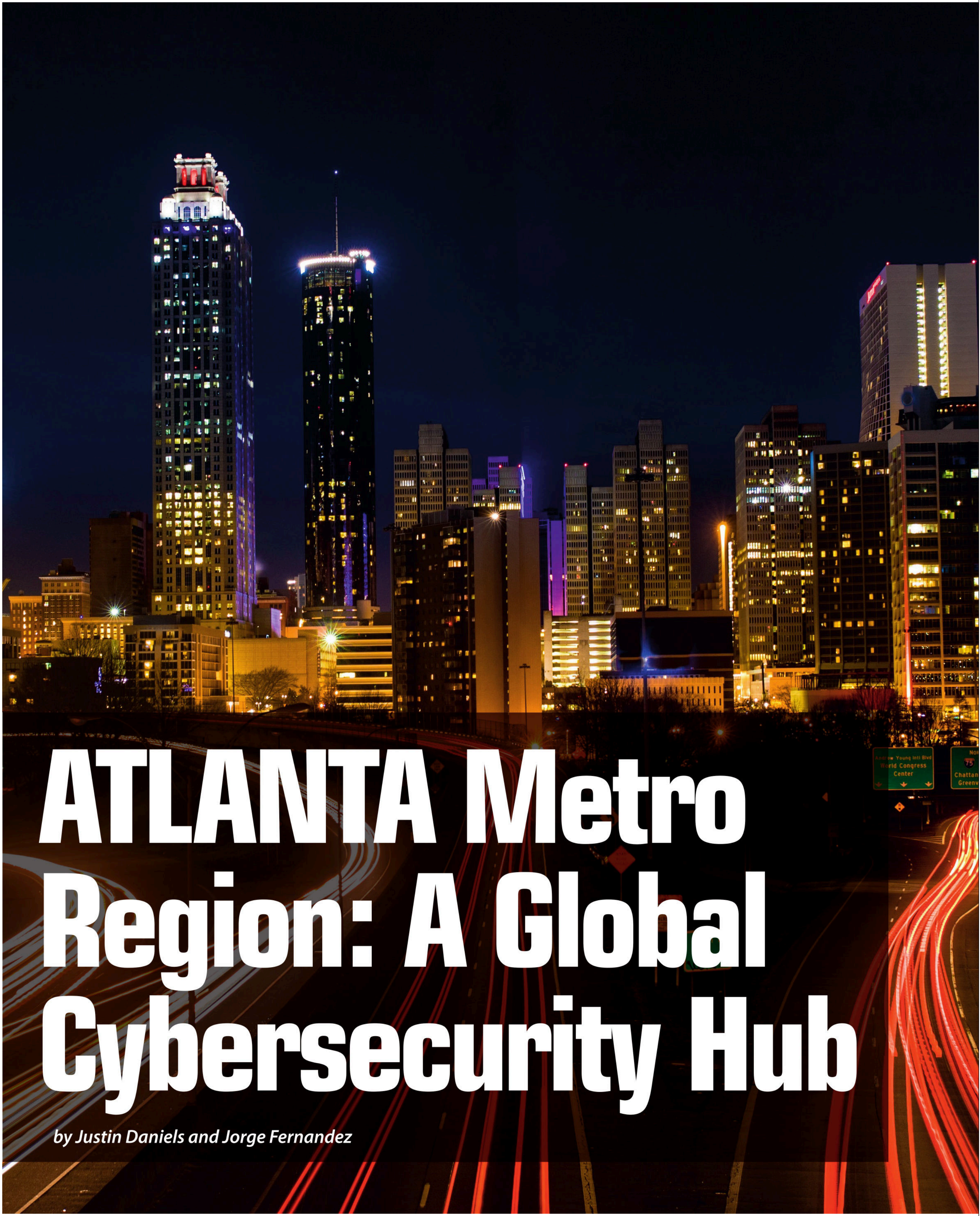
"There has to be governance around cyber hygiene," Goldstein states. "In the event that a cyber attack occurs due to a data breach, it will be unacceptable for C-level executives to blame the IT department. Everyone has to report on it and everyone is responsible for it."

☑ **ASK YOURSELF:**

□ Have we identified and patched all critical systems?

□ Do we have a framework in place to evaluate our cyber hygiene?

□ How will I prioritize the gaps in my cyber hygiene program in this year?



ATLANTA Metro Region: A Global Cybersecurity Hub

by Justin Daniels and Jorge Fernandez

Since the founding of Internet Security Systems 23 years ago, Atlanta continues to grow and develop as a world class corporate hub for cybersecurity companies. The robust business climate and unique regional cyber assets make the Atlanta metro region a dominant player in cybersecurity. Atlanta's business fundamentals make it the 33rd largest global economy with a $339 billion Gross Domestic Product. The key regional asset is Hartsfield Jackson International Airport. It is the largest airport in the world in passenger movement and a direct gateway to most major markets, foreign and domestic. Atlanta is also a digital logistical hub and benefits from the major port in Savannah just a few hours away. The region's existing business capabilities and potential identified Atlanta as a strong candidate under consideration as the location for Amazon's HQ2.

Atlanta also provides a fertile base upon which companies can scale and have access to a world class cyber trained workforce. At the same time, Atlanta has a great quality of life at significantly less cost than comparable cities. In addition, Atlanta is not only one of the top global hubs for cybersecurity, but also a significant innovation corporate center for sectors such as FinTech, advanced manufacturing, health IT, film, and IoT applications, all of which overlap with cybersecurity.

What Makes Atlanta the Premier Cybersecurity Hub

Cybersecurity is a key Georgia industry. Atlanta enjoys a critical mass of cyber companies and activities which engenders cyber companies with a sense of community and common purpose. Cybersecurity 500-ranked SecureWorks, Pindrop Security and Ionic Security all call Atlanta home. Atlanta is also home to the third largest concentration of Fortune 500 headquarters in the country. Iconic brands like Coca-Cola, Delta, UPS and Home Depot are headquartered here and are heavily engaged in the local community.

Our military is cyber-invested in Georgia, as the US Cyber Command is headquartered a short drive away in August.

When completed in 2020, Cyber Command will represent a $189 million investment. It will ultimately employ 1,200 personnel who will represent a formidable cyber trained knowledge base, many of whom who will be looking for cyber opportunities as they conclude their government service.

The State of Georgia has broken ground on the second phase of its Cyber Center for Innovation and Training. The Cyber Center, a State of Georgia investment of $95 million, will not only train all state employees on cybersecurity matters, but will also house an innovation center performing research and development services for the military, academic, and private sectors. That figure is only expected to grow as additional cyber resources are created to support the initial Cyber Center investment.

International and domestic cyber companies relocate to Atlanta because of the existing pool of skilled cyber trained employees and new cyber graduates from the local universities. These assets make the region score well in benchmarks related to innovation, education and relevant research. NCR moved its headquarters to Atlanta specifically because it wanted to tap into the existing talent base here to allow the company to maintain an innovate edge. Irish based Sysnet found it very appealing that it could recruit locally to quickly and significantly increase its personnel to service additional new business.

Educating the Next Generation of Cyber Workers

The Georgia Institute of Technology is one of the finest technical universities in the United States. It has 11 labs and centers dedicated to cybersecurity, with nearly 500 scientists, faculty and students involved with cybersecurity research. Through the efforts of Georgia Tech, Georgia State University, Kennesaw State University and Augusta University, more than 180 undergrads and 150 graduate degree-bearing cybersecurity workers entered the Atlanta cybersecurity talent pool over the past five years, and enrollment in their cybersecurity degree programs has been rising rapidly.

This talent pool is layered into a city which is growing its population at a pace greater than the nation's average. A pace which is forecasted to continue into the next decade. Layers that are also imbedded within a low cost of living and a business-friendly environment. All of this comes together as a great combination for sustainable cyber growth.

Join Us for the Second Annual Atlanta Cyber Week

In recognition of Atlanta's unique cyber ecosystem, a public private collaboration led by Atlanta Metro Chamber and the law firm Baker Donelson, launched the first Atlanta Cyber. During the week of October 2, 2017, Atlanta Cyber Week included 11 separate events hosted by a variety of cyber advocates such as Georgia Tech, National Technology Security Coalition, Georgia State University, PwC, JP Morgan Chase, Metro Atlanta Chamber of Commerce and Baker Donelson.

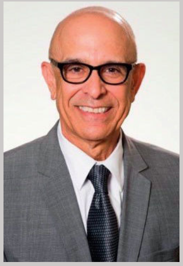
Over 1,000 attendees participated in Atlanta Cyber Week from five countries including Israel, U.K. Canada, Ireland and the U.S. Attendees were afforded a unique view on cybersecurity issues and opportunities, as well as exposure to Atlanta's collaborative cyber and business culture.

Sean Martin, cybersecurity reporter for ITSP Magazine noted in his article summarizing Atlanta Cyber Week:

"Another difference that is a bit more-subtle – but possibly more meaningful – is the culture of the city. While some cities may claim to be 'The Next Silicon' place, pretty much every Atlanta-based company and everyone from Atlanta that I spoke with throughout the week didn't focus on being 'the next' at the expense of the other companies in the area. Rather, instead of talking, they demonstrated with actions just how they will all succeed as a community by working together. This, to me, was way more powerful than any claim to be, let's say, the next "Silicon Peach."

Planning for Atlanta Cyber Week 2018 is well under way; it will be held October 8-12, 2018. This year, Cyber Week will be aimed at informing and educating attendees on the three pillars in assessing and responding to cyber challenges - (1) informing the c-suite about cyber risk; (2) identifying the latest innovative cyber technology and (3) cyber policy. We hope you will take the opportunity to learn more about what cyber opportunities the Atlanta metro region has to offer, and we hope to see you at Atlanta Cyber Week 2018.

About the Authors



Justin S. Daniels is a corporate lawyer and shareholder at Baker Donelson, and the founder of Atlanta Cyber Week.

Jorge L. Fernandez leads the Global Commerce arm of Metro Atlanta Chamber's economic development division.

For more information on Atlanta Cyber Week, please go to https://www.atlcyberweek.com/

Inky Phish Fence for
Office 365 | Exchange | G Suite

inky®
inky.com

STARTUP OF THE YEAR

Inky is the first solution to protect against Deep Sea phishing attacks, using artificial intelligence. Find out why it won Startup of the Year.

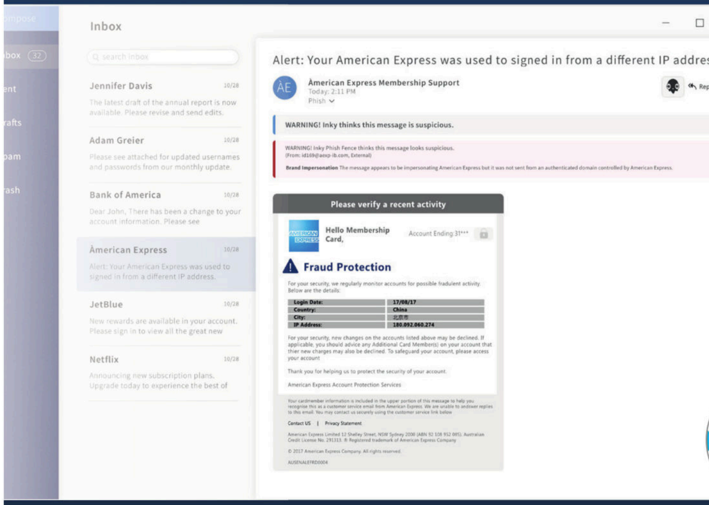
Inky wins 2017 startup company of the year
infosecurity®
NORTH AMERICA

State of the Art Phishing Protection

Inky Phish Fence provides better protection and more feedback to your users. It catches even the latest wave of deep sea phishing attacks that use clever tricks to hide from both trained users and conventional email filters. Protect yourself from the number one source of wire fraud, identity theft, and malware/ransomware delivery: get Inky today!

Explore A Deep Sea Phishing Example | Àmerican Express

How it works - a real world example dissected



Jennifer Davis 10/28
The latest draft of the annual report is now available. Please revise and send edits.

Adam Greier 10/28
Please see attached for updated usernames and passwords from our monthly update.

Bank of America 10/28
Dear John, There has been a change to your account information. Please see

Àmerican Express 10/28
Alert: Your American Express was used to signed in from a different IP address.

JetBlue 10/28
New rewards are available in your account. Please sign in to view all the great new

Netflix 10/28
Announcing new subscription plans. Upgrade today to experience the best of

Alert: Your American Express was used to signed in from a different IP address.

ÀE Àmerican Express Membership Support
Today: 2:11 PM
Phish

WARNING! Inky thinks this message is suspicious.

WARNING! Inky Phish Fence thinks this message looks suspicious.
(From: id169@aexp-ib.com, External)

Brand Impersonation The message appears to be impersonating American Express but it was not sent from an authenticated domain controlled by American Express.

Please verify a recent activity

Hello Membership Card, Account Ending:31***

Fraud Protection

For your security, we regularly monitor accounts for possible fradulent activity. Below are the details:

Login Date:	17/08/17
Country:	China
City:	北京市
IP Address:	180.092.060.274

For your security, new changes on the accounts listed above may be declined. If applicable, you should advice any Additional Card Member(s) on your account that thier new charges may also be declined. To safeguard your account, please access your account

Thank you for helping us to protect the security of your account.

American Express Account Protection Services

Your cardmember information is included in the upper portion of this message to help you recognise this as a customer service email from American Express. We are unable to andswer replies to this email. You may contact us securely using the customer service link below

Contact US | Privacy Statement

American Express Limited 12 Shelley Street, NSW Sydney 2000 (ABN 92 108 952 085). Australian Credit License No. 291313. ® Registered trademark of American Express Company

© 2017 American Express Company. All rights reserved.

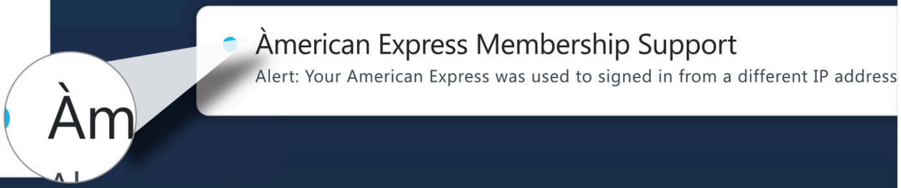
AUSENALEFRD0004

The email from Àmerican Express

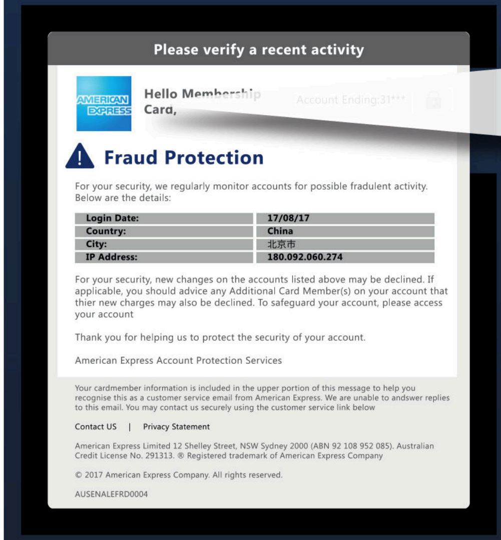
This message looks like a legitimate message from American Express, but it's actually a phishing scam. This example uses several clever tricks to get past mail protection software.

In practice this From: line looks good to most users.

However, that first A is actually Unicode latin capital À with grave.



Àmerican Express Membership Support
Alert: Your American Express was used to signed in from a different IP address


Please verify a recent activity

Hello Membership Card, Account Ending:31***

Fraud Protection

For your security, we regularly monitor accounts for possible fradulent activity. Below are the details:

Login Date:	17/08/17
Country:	China
City:	北京市
IP Address:	180.092.060.274

For your security, new changes on the accounts listed above may be declined. If applicable, you should advice any Additional Card Member(s) on your account that thier new charges may also be declined. To safeguard your account, please access your account

Thank you for helping us to protect the security of your account.

American Express Account Protection Services

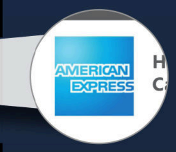
Your cardmember information is included in the upper portion of this message to help you recognise this as a customer service email from American Express. We are unable to andswer replies to this email. You may contact us securely using the customer service link below

Contact US | Privacy Statement

American Express Limited 12 Shelley Street, NSW Sydney 2000 (ABN 92 108 952 085). Australian Credit License No. 291313. ® Registered trademark of American Express Company

© 2017 American Express Company. All rights reserved.

AUSENALEFRD0004



Inky's AI recognizes brand imagery

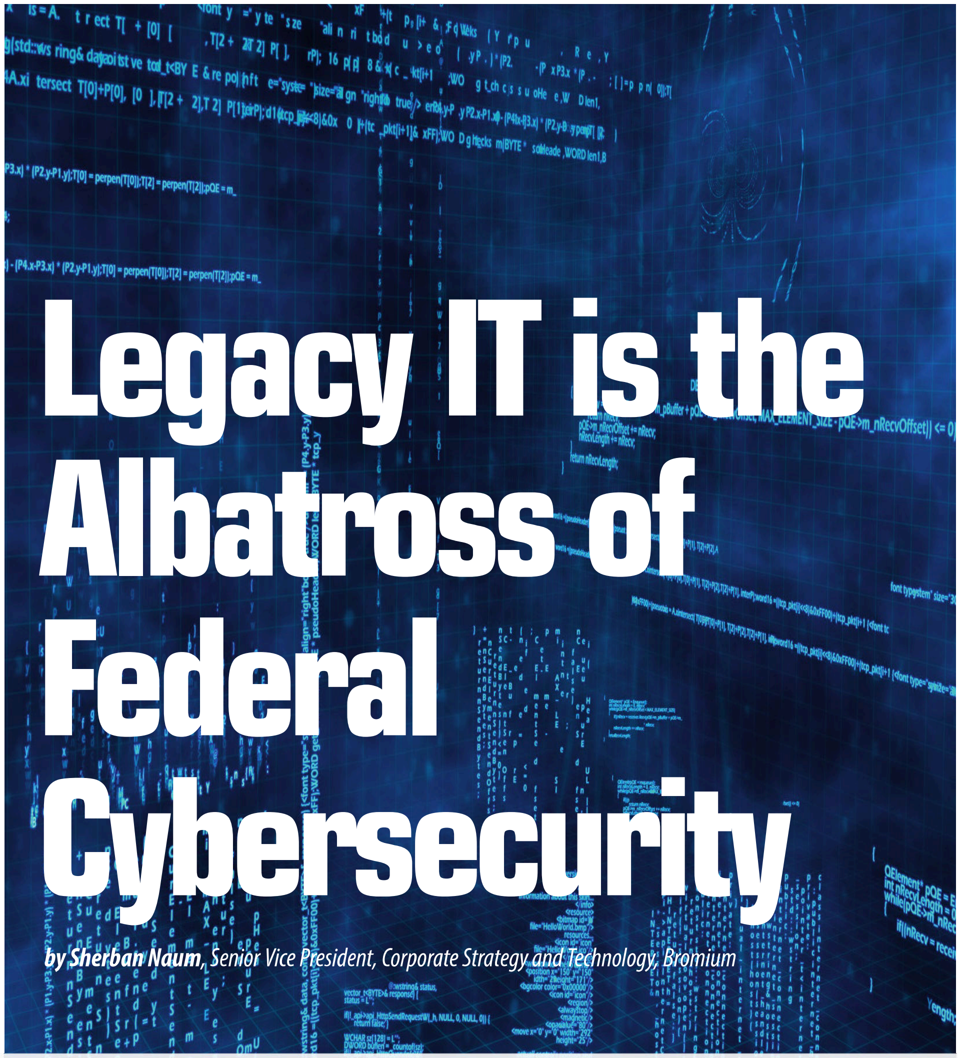
How Inky caught the attack.

Doman aexp-ib.com was registered the same day as the email was sent.

Recognized American Express brand imagery in the message

Fuzzy-matched "American Express" brand term in from text "Àmerican Express".

Not from a valid American Express mail server.



Legacy IT is the Albatross of Federal Cybersecurity

***by Sherban Naum**, Senior Vice President, Corporate Strategy and Technology, Bromium*

Patching isn't always the answer.

When IT systems get compromised, the common immediate response is to patch the vulnerability. This often works, but only after an attack has occurred and the problem has been identified. For example, prompt patching seems to have successfully stopped Meltdown and Spectre. However, the urgent nature and disruption caused by the micro-code updates for Spectre, demonstrate the heavy-lift created by patching.

In the public sector, detection and patching present real problems:

- **Effective detection requires a "patient zero" – which means someone must get owned first**
- **Legacy applications are tough to patch because vendors no longer provide support.**
- **Patches are unpredictable. Patch delivery can take weeks, if not months, after the vulnerability has been identified**
- **Patches are hard to roll out in the federal IT environment because of the testing and approval process.**

Government agencies need an alternative to patching-as-remediation.

The way forward: protect before you detect

The NSA and Homeland Security are recommending a different approach: application isolation and containment. Rather than playing catch-up with attackers, this approach neutralizes threats before they inflict damage.

With application isolation, end users perform tasks – anything that could be an ingress point for malware – in an isolated environment, even if the OS and apps are unpatched. If malware is present, it executes in the hardware-isolated environment, with no access to the protected host operating system, memory, credentials, or enterprise network. It's the classic "honey pot" scenario where malware believes it's fully running and executing, yet only damaging a disposable environment.

Cybercriminals have access to nation-state attack tools and even some source code, which they are using to deliver near real-time targeted attacks exploiting vulnerabilities unknown to the detection industry. Today's detection-based security methods are ineffective, and more agencies will be breached by these nation-state, polymorphic attacks missed by detection-based methods of security.

That's why the NSA and other experts recommend a security stack that includes application segmentation to isolate and contain threats. With virtualization-based protection, government agencies can drastically reduce the risk and impact of APTs and nation-state attacks.

About Bromium

Bromium isolates applications with virtualization-based security. We stop malware. We isolate threats, adapt to new attacks, and share threat intelligence with the SOC.

http://www.bromium.com

VECTRA®

Security that thinks®

COGNITO™

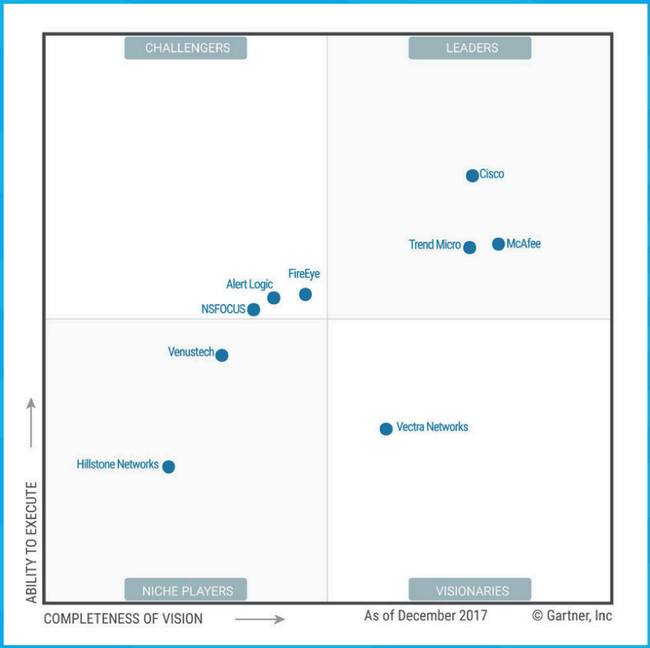
AI that eats cyberattackers for breakfast

Cognito is the award-winning threat detection and response platform from Vectra. Using artificial intelligence, Cognito automates the hunt for cyberattackers, shows where they're hiding and tells you what they're doing.

The highest-risk threats are instantly prioritized so security teams can respond faster to stop in-progress attacks and avert data loss – from cloud and data center workloads to user and IoT devices.

By automating the manual, time-consuming analysis of security events, Cognito condenses days or weeks of work into minutes and reduces the threat investigation workload by up to 29x.

Think of Cognito as a security analyst in software.



Vectra is the sole visionary in the 2018 Gartner Magic Quadrant for Intrusion Detection and Prevention Systems.

Source: Gartner (January 2018)

vectra.ai

A New Approach in the Fight Against Phishing.

by **Lou Ryan**, CEO EdgeWave

The advanced tactics of hackers and bad actors worldwide is getting more and more sophisticated. Nowhere is this truer than at the endpoint. After a decade of developing and deploying email security solutions with advanced self-learning engines and global databases of attack profiles, hackers are innovating on tactics such as next-gen phishing, spear phishing, ransomware and more to steal data and credentials across virtually every network.

Lou Ryan, CEO of leading web and email security firm EdgeWave, sees this evolution first hand. "It's not a matter of if, but when, the next attack gets past your current defenses. Targeted phishing attacks are still on the rise and show no signs of slowing."

The problem? It starts with your employees.

No email security system, no matter how advanced, can eliminate 100% of attacks. Which means that email-borne threats will get through your current defenses into employee inboxes. That leaves only one thing standing in their way: your end users. Most people on a network, though, are clicking time bombs. Incredibly, 9 out of 10 cyber-attacks today start with a phishing attempt. Employees simply don't know what to do when they see a suspicious email.

Even more alarming, in a recent study by Friedrich Alexander University, more than 50% of the employee participants admitted they were not always candid in how they reported email threats to IT. They clicked on many more possible threat emails than they passed on to IT. Which means we may still not know the full extent of how many incidents truly occur day to day.

Even when an end user does forward what they believe is a suspicious email to security or IT, it launches a chain reaction of effort. Administrators may spend hours investigating the legitimacy of the email. And if it is indeed malicious, it can then take hours, even days, rerunning anti-malware or potentially reimaging the system.

Can behavioral training make a difference?

One school of thought is to literally send employees back to school: i.e. Security Awareness training. It's a combination of programmed courses and simulated phishing scenarios designed to give end users a positive/negative reward system on identifying phishing emails. The theory is, if employees are consistently trained on how to recognize these email threats, then they can either delete them or send them to IT to analyze and resolve.

However, Security Awareness training can also be quite a burden for an organization. It can take a significant investment to roll out one of these integrated training programs. It's very much up to IT to run the program and keep the organization updated on the curriculum and current on testing and remediation. What's even more considerable is the time, and the consequential cost, of having everyone in the company do this training. It's an ongoing commitment that has to be reset whenever a firm brings in new hires. And imagine having every employee doing periodic training—that effort alone can cost companies thousands of man hours.

The long-term return on such a training investment? The verdict is still out. Of course, it's always beneficial to have training that helps bring awareness to employees. The heightened focus will likely deliver initial improvement with a percentage of end users. Yet most enterprises don't have learning management specialists on staff to curate and maximize ongoing programs like this. And, ultimately, training still doesn't solve the underlying security problem—how to remove the phishing attack in real-time from the network.

A new defense that helps both employees and IT.

EdgeWave has just launched a cloud service to enable employees to better defend themselves. Called ThreatTest—and powered by EdgeWave—this service installs a "threat test" button in MS Outlook for every employee. If the employee sees a strange or suspicious email, he or she can simply click the button. That email is quarantined away from the inbox, and automatically sent to EdgeWave's labs where it's run through artificial intelligence filters and expert human analysis.

In minutes the email is returned to the user as either validated, or removed if malicious. ThreatTest provides a low cost, immediate way for employees to question and resolve emails they deem suspicious. And it takes a huge burden off IT by cutting the significant time and cost of getting IT involved every time a threat is analyzed and eliminated.

Lou Ryan has already seen very positive responses from a large cross section of customers.

> *"ThreatTest is designed for any organization that wants to dramatically improve their endpoint security and activate employees as a united force to help stop phishing attacks. Even if you have unlimited time and budget, training may narrow—but still won't close—the gap. ThreatTest is a fast, easy way to give employees a remediation tool they can use today to stop email-borne threats."*

A core advantage of EdgeWave's ThreatTest is that it "closes the loop" and returns the email to the end user with a final resolution. Firms no longer have to put the onus on IT or security administrators to remediate each email in question. Which is especially valuable if you have thousands of employees, and they send waves of emails to IT for analysis. Instead of straining IT resources, ThreatTest does all the work. Management via the Administration Portal provides IT with easy deployment to users and central reporting enhances visibility into how phishing attacks are affecting the organization.

As email threats find more and more ways to get past current defenses and into employee inboxes, it seems logical to give every end user a way to quickly test and eliminate anything suspicious. Training can increase knowledge and awareness, yet having an automated process to solve the problem without weighing down IT or security resources is the best way an organization can truly scale their endpoint security along with their business.

To learn more about ThreatTest, powered by EdgeWave, go to www.edgewave.com/products/threattest/.

Innovations in MSSP: Predicting the Next Attack

by Raul Pavao

I've been following the Managed Security Service Provider (MSSP) market for some time. I'm always looking for innovators and those who understand how to harness 'big data' to their advantage. MSSPs have two advantages that most stand-alone organizations will never have:

1) They securely collect a lot of threat, attack, vulnerability and exploit data. The more clients, the more patterns become visible to the MSSP;

2) They become well-honed InfoSec teams willing to take on a very serious and real burden for their clients – usually across multiple vertical markets and regulatory compliance pressures;

Therefore, for those organizations who are under constant threat or just don't have the resources to find the very best of breed talent and build their own secure operations center (SOC), an innovative growing MSSP is the way to go. So, in my research, I found Proficio. They began their MSSP business in 2010 with a lot of experience from running silicon valey hardware and software companies.

In fact, their Chairman of the Board and President, Tim Mcelwee told me that he and John Humfreys started doing Business Process Outsourcing (BPO) way before it was an 'in-thing' or popular, hence the evolution into a great MSSP. In their journey to help well recognized players like InfoBlox and Proofpoint launch into Asia and the EU by outsourced sales, marketing and operations support, they found a high-tech channel and smart customers but not a lot of expertise in the delivery and integration of solutions for best practices in information security.

So, Tim had the epiphany to bring in the best leadership and expertise he could in the security information management (SIM) business, like Brad Taylor who knows how to go from startup to IPO and asked him to take the helm as CEO with a mission of revolutionizing the MSSP business. As a result, this visionary team has grown over the years with a strong client-base, a 98% retention rate and well over 200 clients.

Proficio has grown from a tiny humble one thousand square foot office and SOC to over 35,000 square feet of prime space in San Diego and Singapore. They have a growing team of threat hunters, SIM management experts and continue to focus on customer-driven growth with 12 data centers throughout Asia and North America. They've launched a GDPR compliance initiative for the EU and a managed detect and response (MDR) offering with 20% year over year growth.

What really caught my eye with Proficio is Tim's passion for innovation. His sister-company effort CyberSight (http://www.cybersight.com) offers an incredibly innovative and easy to use endpoint security solution that actually stops next generation ransomware in its tracks.

It's designed to complement existing antivirus solutions and is an integral extension to Proficio's MSSP offering, giving them a leg up on the competition by helping clients worry less about the latest ransomware threats.

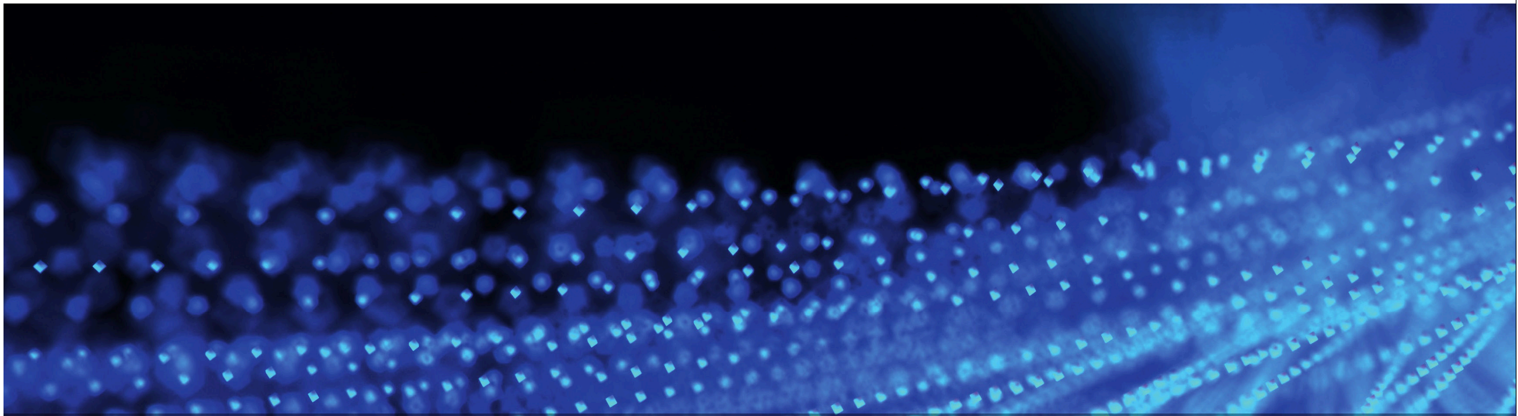
In addition, another innovator at Proficio is their upcoming "FICO-like" risk scoring system that I was given a sneak peek into – something designed for their customer CIO's and CSO's to simplify and help remove the noise and give them a real risk measurement they could take to the Board.

Imagine you have tons of data – hundreds of million events, and, following in IBM's footsteps on the thoughts of A.I., Machine Learning and access to this kind of big data, you could provide your clients with this scoring – showing them how exposed they really are for the next wave of attacks, the next breach. To me, this is a great step – to help customers be more aware and even, potentially, predict their exposure to the next attack. Suppressing the noise and wrapping this data with simplification, a scoring system and less alerts, we have an MSSP that really gets it.

As Tim said, "You can't slow down the attack, but you can predict what that attack might look like - from attack-vector to vulnerable device and credentialed user and share this in near real-time with our clients so they can begin to more proactively block tomorrow's threat, today." To me, this is a very exciting step towards breach prevention. If you are an organization from 500 employees up to 100,000, Proficio is ready to offer you a complete and compelling MSSP offering. Check them out at http://www.proficio.com.

About the Author

Raul Pavao, Vice President of Cyber Defense Magazine is also in charge of our upcoming launch of CyberDefense.TV. His background includes international end-to-end Business Development with more than 20 years of cross-functional expertise in innovative secure transactional solutions for Enterprises and Financial Institutions. In this extensive career, he has participated on relevant and pioneering initiatives in cybersecurity. He has led major Global initiatives on Mobile Financial Services (M-Banking, M-Payments and others), Omnichannel security, Multi-factor and Risk-Based authentication, focused on integrate high end security with the best user experience and partnering with renowned IT and Cybersecurity companies in U.S., Europe and Latin America.



Despite Recent Critical Press,

Secure Messaging Platforms Essential to an Enterprises' Defense-in-Depth Strategy

by Dr. Galina Datskovsky, CEO of Vaporstream

The media seems to have it out for secure messaging thanks to Uber vs. Waymo and other examples of misuse, but enterprise-grade secure messaging's compliance, privacy, security and incident response benefits cannot be ignored.

As an explosive legal case between Uber and Google's former self-driving car project, Waymo, began to make numerous media headlines in late 2017, an unsuspecting technology found itself in the crosshairs of the dispute. While one might suspect that it was autonomous vehicle technology or a top-secret robotics program at the center of debate, it was actually an ephemeral messaging services - specifically Wickr - that emerged as one of the most provocative arguments throughout the early days of litigation.

Upon the commencement of the trial in November 2017, Waymo presented its working theory, accusing current Uber executives - previous employees of Waymo - of using Wickr and other ephemeral messaging apps to communicate via disappearing text messages. The premise was that the messaging apps were used to secretly discuss trade secrets that were illegally taken from Waymo. Whether the theory presented by Google's former self-driving counsel is accurate or not, it was all but impossible to prove. The transactional and contextual history of any messages communicated via the secure messaging apps utilized by Uber are essentially untraceable and therefore impossible to present in court.

An unintended consequence of the plaintiff's argument, however, came from the negative media coverage that would pursue courtroom proceedings. Specifically, many media outlets began reporting on what they argued were major concerns about both the ethics and legality of ephemeral messaging apps in business environments. In fact, when this news came to light, many in the media even claimed that the outcome of the trial could set the legal precedent for business use of ephemeral messaging going forward. Such critical press undoubtedly led to the November mandate by Uber's CEO to ban secure messaging apps entirely.

To the surprise of the entire tech universe, Uber and Waymo recently settled out of court for $245 M. Yet the damage to the reputation and perception of secure messaging apps remains tarnished and misconceptions about the legality of ephemeral messaging, all due to one company's possible misuse of the technology, are circulating like never before.

As an example, an organization's proactive incident response personnel could utilize their secure messaging

The Use Cases for Secure, Ephemeral Messaging in the Workplace

The legality of secure messaging aside, it's important to first understand why so many businesses have started using ephemeral communications in the first place. Worldwide, the frequency and sophistication of cyberattacks are on the rise and as a result, compliance and incident response are now integral to any CISOs defense-in-depth strategy. Specifically, secure and ephemeral messaging platforms provide the following benefits to the enterprise:

- **Phishing Mitigation:** Secure messaging provides a unique, yet proven solution to mitigate risk by taking communications outside of where they are most vulnerable - email and SMS text. Although email is the most commonly used tool for digital business communication today, CISOs have worked diligently to educate employees of the vulnerabilities that email entails. This knowledge has caused many workers to reduce their reliance on email altogether, instead choosing to utilize SMS texting for its ease-of-use and simplicity. In fact, 80 percent of workers report using SMS texts as part of doing business; even if text messaging is not a sanctioned form of communication in the workplace, according to Seyfarth Shaw LLP. Unfortunately, however, SMS texts are not considered secure, do not meet regulation requirements for record retention and they are also at risk of SMS phishing (smishing) attacks. Secure messaging eliminates these threats inherent to SMS.

- **Messaging Encryption:** Secure messaging platforms use end-to-end encryption, meaning that only approved senders that have been granted access to an organization's platform can send messages, thereby eliminating the threat of outside senders entirely. Secure messaging also prevents man-in-the-middle attacks, which can occur when unencrypted SMS texts are sent on an open network.

- **Sender Controls:** Beyond encryption and exclusive to enterprise-grade secure messaging platforms, is that the sender maintains complete control of the conversation, the data and its use at all times. These advanced sender controls prevent unintentional sharing, data theft and propagation of information.

- **Governance & Compliance:** Unlike native SMS texting or email, secure messaging platforms do typically remove sensitive information from all devices based on a set interval of inactivity, which is what occurred in the Uber case. However, secure messaging platforms can also ensure that all messages are captured and archived to the organization's repository of record for compliance purposes and processes, while removing texts from sender and recipient devices.

- **Incident Response & Emergency Mass Communications:** Prior to, during or in response to emergency situations, such as during natural disasters, manmade threats or cyberattacks, swift and secure communication to company stakeholders, employees, emergency response teams and often times even the public is paramount. In these moments, secure messaging allows for rapid, secure notifications and response communications to meet corporate operating procedures and compliance mandates, without worry of third party surveillance or leaks.

platform to preemptively set up templates and pre-schedule a series of texts to notify first responders and emergency management offices as well as all field employees during a declared emergency. Such real-time communications are extremely useful when automating programs that call for routine communications that follow in a series, such as status and field updates as well as anticipated outage timelines. Replies to these automated communications can be routed to a specific mailbox or group for monitoring and response, or disallowed based on the type of communication and need, providing a central communication hub.

Secure Messaging is Legal, Despite What the Media Says

When secure messaging made headlines as part of the Uber/Waymo trial, many were quick to say that enterprises should be prohibited from using these private services for internal communications. Most of the arguments against secure messaging platforms proclaimed that executives shouldn't be discussing items that couldn't be presented publicly if needed at a later time, such as if ever called upon for litigation.

But according to a former U.S. Attorney in Virginia, there is nothing inherently unlawful about instructing employees to use disappearing applications, just as there is nothing wrong with communicating information over an unrecorded phone conversation. With that in mind, what needs to be considered when assessing the use of ephemeral messaging is actually the timing and the industry in which it is being used.

For organizations within highly regulated industries, ephemerality in and of itself can be extremely beneficial in maintaining compliance. For example, sending confidential healthcare information by disappearing text, which does not remain on smartphones after the issue(s) have been resolved helps keep the information confidential. Similarly, sharing sensitive financial information between wealth managers and their clients or diagnostic results between a plant administrator and a remote facility worker has tremendous value.

When the allegations against Uber's executives use of ephemeral messaging was revealed, a major concern amongst media and onlookers was that these solutions were unlawful because they didn't keep records of communications. In some ways, this concern is warranted, as most of the well-known and readily available consumer-grade messaging solutions on the market, as well as their more secure solutions for business users, do not meet record retention requirements.

However, what many may not be aware of is that there are select enterprise-grade secure communications platforms that have been built with security, privacy and compliance in mind from inception, allowing for encrypted copies of conversations to be archived securely to meet industry-specific record retention requirements, or in the case of anticipated litigation. For organizations that are required to keep a detailed history of communications, the ability to collect a single copy of record actually makes eDiscovery and compliance much easier by not requiring collection from multiple mobile points.

Despite the Uber/Waymo trial shining what could have been interpreted as an unpleasant light on the use of secure messaging in corporate environments, it did provide an opportunity to educate the public on the many use cases for secure messaging for business, and reinforce its legality. Although Uber permitted and encouraged the use of secure messaging for internal communications amongst staff, it failed to set an internal expectation of how the tool should be used, deploy a full-time compliance archive point or how communications would be stored in the event of litigation. On the opposite end of the spectrum, many organizations remain unaware of the benefits and possibilities of secure communications tools or have been influenced by recent media coverage. These companies should not refuse to adopt secure messaging solutions altogether, as this will instead push business users to find their own unsanctioned solutions or even worse, use vulnerable SMS texts. Instead, organizations should embrace the right secure messaging platform, which when used correctly, can be a key component of their defense-in-depth strategy.

Meet Vaporstream: The Right Choice for Secure, Ephemeral Communications

To keep confidential communications secure, while also proactively protecting against increasing cyber risks and ensuring legal compliance, it is up to organizations to provide employees with the right platform that meets the needs of the industry in which it operates.

Vaporstream is a secure, ephemeral and compliant communications platform that work teams can use on their smartphones, tablets or desktops. The solution provides sender controlled, encrypted and leak-proof messaging that helps ensure that only the intended receiver sees the message contents. For compliance purposes, organizations can retain a copy of messages to a secure, client-specified repository for safe keeping and control. Employees can also send attachments, collaborate with ease and seamlessly communicate with colleagues, third-parties' and other external contacts in a secure manner.

In an era of complex and aggressive security threats, complicated by rising demands for mobile agility and innovative client-engagement, Vaporstream's secure communications platform empowers enterprises to have asynchronous, secure and private mobile communications to conduct business – no matter where they are. Vaporstream's focus on security and privacy ensures that text messaging communications are kept confidential, secure and compliant, i.e. HIPAA, FINRA and others, while driving superior business outcomes.

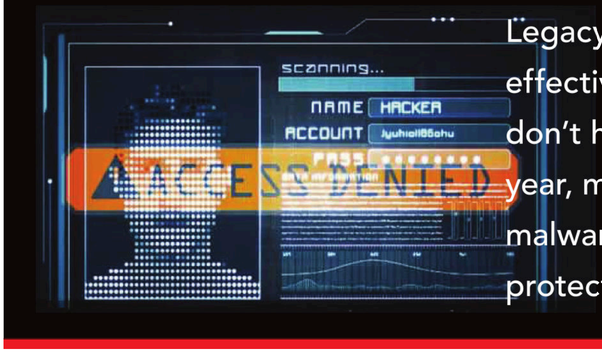
Vaporstream also eliminates concerns about information exposure, device loss or theft due to ever-increasing use of mobile devices and mobile communications. Third-party certified by NowSecure™ for information security, our patented technology and robust feature set for security, collaboration, automation and compliance provides an encrypted text messaging platform for teams to communicate with confidence and collaborate at the speeds demanded by today's business. Trusted by leading organizations across a variety of industries, Vaporstream helps ensure that critical communications flow seamlessly, securely and confidentially at the speed of business.

About the Author

Dr. Galina Datskovsky, CRM, FAI and serial entrepreneur is an internationally recognized privacy, compliance and security expert. Galina is the CEO of Vaporstream®, a leading provider of secure, ephemeral and compliant messaging.

FFRI Yarai

FFRI yarai's Precognitive Defense eliminates threats before they begin



Legacy anti-virus solutions require signatures to operate effectively. Targeted attacks using fileless malware, however, don't have signatures. As a result, you are not safe. Last year, more than 50% of malware attacks were fileless malware; the kind those traditional anti-virus solutions don't protect you against. Don't rely on luck again this year.

FFRI yarai

Leveraging five core protection engines to eliminate threats before detonation, FFRI's approach to layered security has become the trusted defensive stack for many global enterprises and international governments.

Application Protection

The patented ZDP engine protects against Zero-Day vulnerability attacks in real time.

Malware Prevention

Static Analysis and unique Sandbox engines monitor unusual programs at pre-execution.

Dynamic Protection

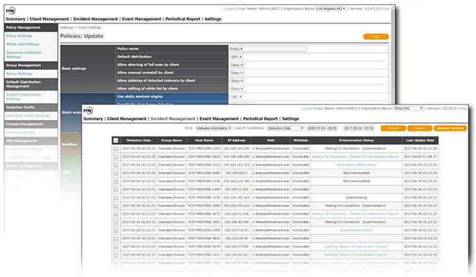
HIPS and Machine Learning engines capture advanced malware behavior in real time.

FFRI yarai is highly efficient and doesn't rely on cloud access, signatures or third-party feeds for detection and prevention.

Lightweight System Footprint, Simple Deployment, Intuitive Management

According to a 2017 survey by MIC Research Institute Ltd., FFRI's yarai platform was ranked #1 in protection from advanced targeted attacks.

With over a thousand enterprise customers, FFRI has created one of the top security technologies and a world-class security research team.


Summary | Client Management | Incident Management | Event Management | Periodical Report | Settings
Policy Management
Group Management
Default Distribution Management
Detection Notify
License Management
Policies: Update
Basic settings

Policy name: Policy A
Default distribution: OFF
Allow aborting of full scan by client: Deny
Allow manual uninstall by client: Deny
Allow deleting of detected malware by client: Deny
Allow editing of white list by client: Deny
Use static analysis engine: ON

Detection Date	Group Name	Host Name	IP Address	Path	Whitelist	Extermination Status	Last Update Date
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

FFRI's research and development efforts have led to the detection and prevention of the most sophisticated malware attacks, helping countless customers remain safe, secure and breach-free.

FFRI has recently been named a **Top 50 Cyber Security Leader of 2017** by Cyber Defense Magazine, which recognizes companies that demonstrate innovation and leadership in cyber security solutions and services.

FFRI yarai received the recognition based on its Precognitive Defense which eliminates threats before they begin.

FFRI North America, Inc. | 65 Enterprise 3rd Floor | Aliso Viejo, CA 92656 | email: sales@ffri-inc.com

Attention CISOs:

Welcome to the Era of Advanced Phishing Threat Protection

by Eyal Benishti

Today's frequent and sophisticated Business Email Compromise, Advanced Persistent Threats, and Ransomware Attacks negate effectiveness of point solutions such as secure email gateways and phishing awareness training tools.

Despite the rise in popularity of secure messaging platforms and workflow management tools like Slack, email far and away remains the predominant method for personal and business communications. In fact, worldwide more than 269 billion emails are sent every single day.

Thus, it should come as no surprise that email remains the primary attack vector for cyber criminals, with more than 90 percent of all cyberattacks beginning with a malicious email sent to an unsuspecting recipient. Astoundingly, Symantec found that one out of every 131 of said emails contains malware, a frightening statistic that threatens organizational risk at epic levels.

Where the Email Phishing Epidemic Stands

The full figures from 2017 are just beginning to trickle in, but here's what we do know:

- According to SC Magazine UK, 96 percent of business were hit with BEC attacks in the second half of 2017.

- During the first six months of 2017, the Anti-Phishing Working Group (APWG) identified more than 590,000 unique email phishing attacks and hundreds of thousands of illegitimate phishing websites.

- According to the Symantec 2017 Internet Security Threat Report, more than 400 businesses are targeted with business email compromise (BEC) scams every day, and ransomware increased by 35 percent.

- Malware injected through phishing scams grew by more than 1000 percent.

- 1.4 million new phishing websites were created every month.

Such statistics should come as no surprise when considering 9 out of 10 attacks begin with some method of email phishing. And while spear-phishing attacks intended to compel people to download a malicious attachment or click on a compromised link remain prevalent, new BEC attacks are extremely difficult to identify because they do not include any links or code. It's social engineering at its finest. Combine the rise of email spoofing, BEC and ransomware with the general availability of phishing-as-a-service kits, and enterprises find themselves on red alert 24/7/365.

In recent years, companies of all sizes have supplemented their security stacks with two defense methods to combat email phishing attacks: phishing awareness and training tools and modules, and secure email gateways (SEGs). Many organizations, including U.S. government agencies, are also choosing to adopt the DMARC authentication protocol.

Yet despite such investments, the email phishing epidemic has gotten exponentially worse, and not any better. Employees continue to succumb to complex social engineering messages, and fraudulent codeless messages can easily bypass SEGs, while DMARC has already been exposed by Mailsploit.

Such discouraging events beg the question - will SEGs and security awareness training tools ever be enough to fight the phish?

The Myths of Phishing Awareness Training Exposed

For years we've heard cybersecurity "experts" pontificate about the necessity of phishing awareness training. They proclaim that all organizations - regardless of size, location or revenue - should invest time, money and resources into phishing prevention education for all employees. Sure, modest training can provide some benefit, but any argument that such training modules can change employees' behavior and transform them into an impenetrable first line of defense is misguided at best, and a flat out lie at worst.

There are additional myths and lies about the value and ROI of phishing awareness training tools that vendors don't want you to know, such as the amount of time, content and modules needed to educate, among others. But one thing is clear, with the damage that phishing continues to cause, awareness and training is falling short of its intended mission. After all, it only takes one small mistake on the behalf of an employee to circumvent even the most complex and advanced security systems.

Myths aside, one of the primary inefficiencies of phishing awareness and training tools is that such are merely a point solution in which success is predicated on changing human behavior. Putting the daunting task of changing how humans act aside, point solutions, of which SEGs and security training are the epitome of, have come under increasing scrutiny by CISOs for their inability to serve as a comprehensive phishing risk mitigation solution mainly because they lack the ability to automatically initiate remediation and orchestration in real-time.

Such reality is expediting consolidation of the awareness and training market. Since the calendar flipped to 2018, Barracuda Networks has announced its acquisition of PhishLine to add what it said were new capabilities to deliver integrated, adaptive security awareness training. Additionally, Proofpoint recently announced its forthcoming acquisition of Wombat Security to "provide the industry's first-ever integration of market-leading protection and awareness offerings." Security vendors such as Trend Micro and Sophos have consolidated offerings with computer-based training (CBT) modules to help educate staff on the latest security issues and vulnerabilities. Rumors of other phishing awareness and training companies looking to exit are gaining steam, and it won't be long until more follow suit, or such point solutions risk becoming obsolete.

Limitations & Vulnerabilities of Secure Email Gateways

In the midst of phishing attacks becoming exponentially more sophisticated and targeted, the majority of SEGs continue to only offer signature-based and behavioral signature solutions that scan links and attachments, determine domain reputation and verify sender-receiver relationship, among other futile safeguards.

According to Gartner's May 2017 Market Guide for Secure Email Gateways report, "a SEG is typically categorized as 'preventive' since it is put in place to block malicious messages before they can impact the enterprise." This same report also argues that advanced threats easily bypass signature-based prevention mechanisms that SEGs have traditionally used.

Overall, SEGs fail to address new threat models because of insufficient advanced threat defense capabilities, such as automation and forensics. For example, an impersonated email message can easily evade legacy gateway detection, arriving into an employee's inbox, where it can lay idle for days, weeks or months. With minimal to no post email delivery detection and response capabilities, a SEG will not recognize this type of email as malicious because the attack lacks links and attachments to analyze. Other limitations and vulnerabilities of SEGs include:

- **The misguided reliance on content filtering (URLs/attachments), and signatures despite hyper-targeted messages increasingly bypassing traditional email security controls.**

- **Sender-recipient reputation-based context prevention mechanisms are too reliant on static VIP lists and similar algorithms such as fuzzy hash.**

- **Relatively basic post email delivery capabilities easily defeat signature-based email security solutions by using polymorphism techniques. This includes changing email artifacts like the sender's IP, subject lines and elements of the email body.**

- **Not all inbound emails can be sandboxed or sanitized using Content Disarm & Reconstruction (CDR) technology.**

Many organizations, especially the enterprise, are beginning to come to terms with the fact that their employees are now targeted and falling victim to all types email fraud - from phishing and social engineering to BEC and spoofing - every day. As such, mitigating phishing risk requires stakeholders to rethink their approaches to security to one that prioritizes advanced phishing threat protection driven by the combination of human intelligence with machine learning.

The IRONSCALES Platform: The World's Most Advanced Phishing Threat Protection

Knowing that the use of signature and rules-based solutions continue as the status quo, attackers often find their hacking tools and techniques relatively unchallenged. These defenses are limited to following rules that hackers can easily subvert through spear-phishing and social engineering.

Although there is almost universal agreement by malware researchers to ditch signatures, many SEGs are lagging in doing so. To ensure the vulnerabilities of said rules, attackers now frequently test their malicious attachments and links against common cybersecurity solutions, only launching attacks after verifying that the attack is fully undetected.

The IRONSCALES platform is designed for pre-and-post email delivery, always assuming that emails will pass through the prevention layer. The platform consists of four modules that work in tandem to automatically prevent, detect and remediate email phishing at all phases of an attack's lifecycle.

The platform utilizes mailbox-level anomaly detection to analyze employees' mailbox behavior and protect against hyper-targeted phishing attacks both before and after they bypass all gateway level solutions and land in an inbox.

Security teams must empower their organizations with the tools and

The four layers of the IRONSCALES platform include:

Layer 1:

Simulation & Awareness Training - IronSchool, IRONSCALES' customized micro-learning method helps employees to think and act as virtual SOC response team members, becoming proactive against malware attacks. Our gamified, interactive micro-learning method is customized to each employee based on an initial assessment of users phishing recognition and classification skills. Then, all employees are given tailored training and simulations with mock phishing attacks to increase awareness and responsiveness to social engineering techniques. Our CIO/CISO dashboard performs ongoing real-time analysis of each campaign and training results, generating KPIs for routine and on-demand reviews. Enterprise-wide and employee-specific reports provide insights into the effectiveness of every campaign, so security teams can see in real-time which employees are improving and which are most vulnerable to phishing scams.

Layer 2:

Advanced Phishing Threat Detection - Known as IronSights, IRONSCALES' advanced mailbox-level anomaly detection module automatically identifies spoofing and impersonation attempts in real-time. Powered by machine learning technology, IronSights detects anomalies and communication habits at the mailbox-level based on sophisticated user behavioral analysis and deep email scans that check the credibility of the email sender's reputation. Our machine learning algorithms cross-reference suspicious attempts by hackers or those that attempt to hide their identities by using common impersonation and spoofing tactics. Our algorithms continuously improve the detection of irregular communication patterns based on learned experiences that negate false positives and bolster proactive defenses. When email spoofing or impersonation is identified, Advanced InMail visual phishing alerts help users report the threat in real time.

Layer 3:

Automatic Phishing Incident Response - IronTraps is a non-signature, machine learning based module that automatically detects and remediates known and zero-day phishing attacks that exploit email as the attack vector. Using a proprietary detection algorithm to discover trending and unknown phishing emails, IronTraps provides protection and incident response across clients, servers and mobile. To assess threats, IronTraps conducts continuous automated email clustering to find similarities in phishing emails, creating a repository of phishing patterns.
For known and reported attacks, IronTraps provides fully automated proprietary and 3rd party forensics and analysis with URL/link scanning, attachment scanning, real-time affected mailbox reports and spam analysis using best of breed multi av and sandbox engines. When a new attack is detected, IronTraps orchestrates an automatic response across multiple security controls, eliminating the threat completely from network to endpoint with little to no involvement from the security team.

Layer 4:

Phishing Intelligence Sharing - IRONSCALES' Federation module offers human verified, real-time actionable collaboration, integrated with automated incident response, as a means to better prepare and respond to new attacks before they target other employees' or other companies' inboxes. Federation is the first and only threat intelligence technology to provide a comprehensive real-time automated intelligence sharing ecosystem that can be integrated into automated incident response and prevention layers. The features and capabilities of this product tackle organizations' newest information security needs by proactively providing human and machine verified intelligence and crowd sourced intelligence with other organizations as a means to thwart zero day threats.

> *Overall, SEGs fail to address new threat models because of insufficient advanced threat defense capabilities, such as automation and forensics.*

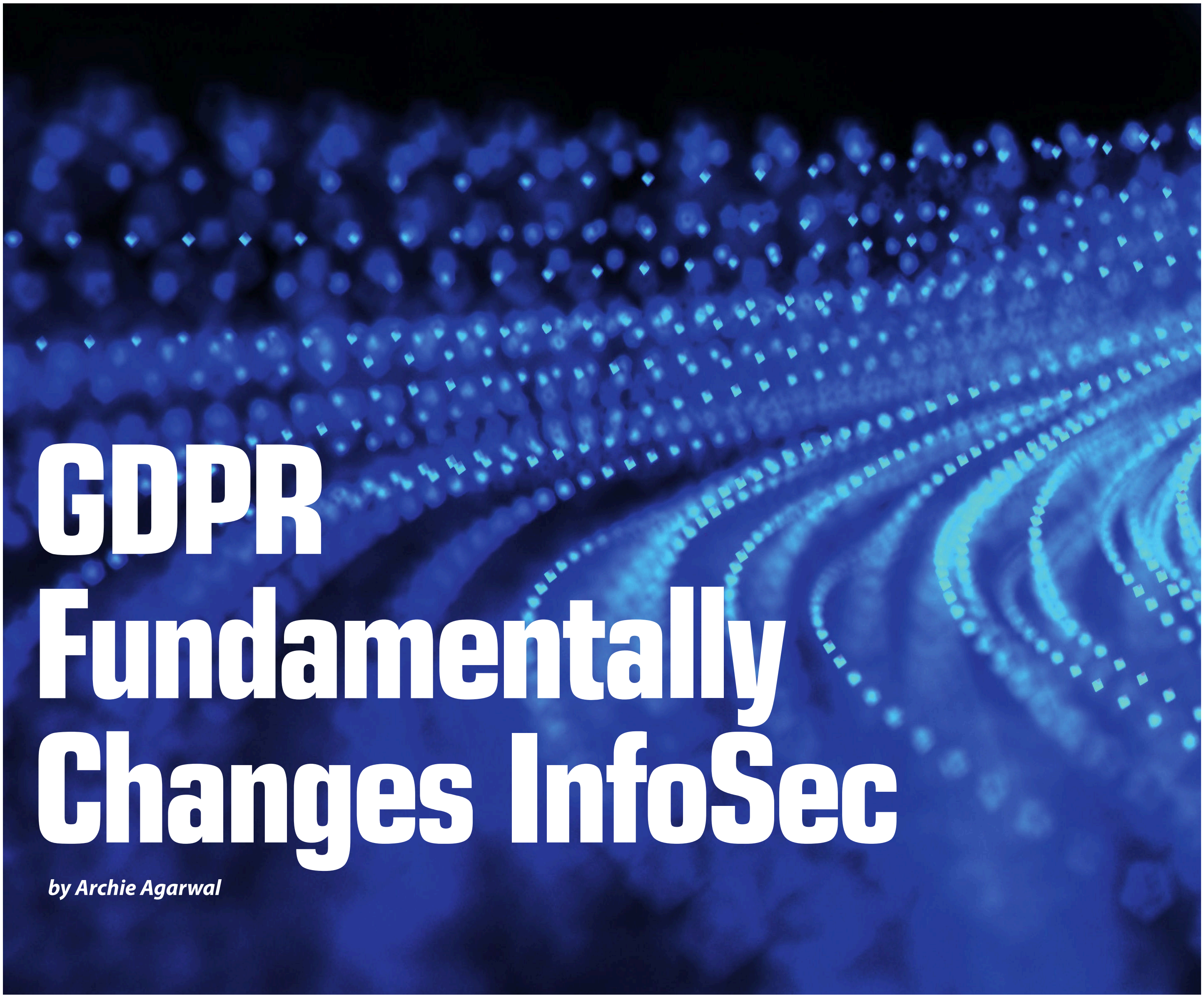
techniques to fight the phish at every phase of the attack lifecycle, while always assuming that attacks will subvert the prevention phase.

This can only be accomplished through a multi-dimensional phishing mitigation approach that includes safeguards for both pre-and-post email delivery, and ditches rules and learning modules for powerful technology that combines human intelligence with machine learning.

Welcome to the era of advanced phishing threat protection; the best opportunity to fight off the phish that the world has ever seen.

About the Author

Eyal Benishti is a veteran malware researcher and founder and CEO of IRONSCALES, a leading provider of anti-email phishing technologies.



GDPR Fundamentally Changes InfoSec

by Archie Agarwal

European Union Regulation may impose Substantial Increase of Risk to US Companies.

The European Union's upgrade of the current Data Protection Direction, known by most as the General Data Protection Regulation or GDPR, is one of the most sweeping overhauls of data protection the world has ever seen. Not only does GDPR come with real teeth – including fines starting at €10 million which may go as high as €20 million or 4% of the organization's global gross revenues, whichever is greater – but it fundamentally redefines the focus and purpose of information security.

Since the beginning of shared computing, InfoSec has been about securing the data and other digital assets stored, transferred, and otherwise processed via IT systems. The primary focus of InfoSec has been to prevent the unauthorized release, dissemination, or use of an organization's data assets. In this regard, InfoSec shared common ground with other security functions within an organization: protecting the company from loss.

For companies engaging in online business with EU residents – regardless of where that company resides – the GDPR changes all that. Come May 25 of this year, organizations will be held accountable for also mitigating the risks to the personal rights and freedoms of data subjects.

The scope of GDPR's reach may be surprising. Consider, for example, an American company that sells goods online. Sally, a new customer and US citizen, downloads the company's mobile app onto her cell phone. Sally takes a European tour during which she makes purchases using the American company's mobile app.

To boost sales or provide a better customer experience the company may want to use Sally's data, "to take decisions concerning her or him or for analyzing or predicting her or his personal preferences, behaviors and attitudes." If the company does so while Sally is in the EU, however, they could be found in non-compliance with Article 3(2) and subjected to substantial fines.

Per article 79, protected individuals have the right to an "effective judicial remedy" where they consider an organization's non-compliance has infringed upon their rights and freedoms. Per the GDPR definitions, an "infringement" may include material or non-material damage.

Though the new regulation has yet to be tested in the courts, legal analysts anticipate the courts will maintain, or even extend, the broad view of infringement and personal damage developed under the old Data Protection Act. Under the Act, an organization could be found liable even in the case of non-pecuniary "damage" to personal dignity, integrity, or autonomy – including a claimant's anxiety and distress over what might result if their personal information is mishandled. Actual financial loss is not necessary – the European courts have already found that "emotional distress" is an infringement on individual rights and freedoms.

Can organizations protect themselves by beefing up their information security level? While that is a good start, it does not satisfy the Regulation's intention of protecting individual privacy. As the example above with Sally illustrates, companies using collected personal information for legitimate business reasons can be found to be violating the regulation's standard of protecting personal rights and freedoms.

Furthermore, according to Article 82(3), organizations will be required to prove that they were not responsible – in any way – for an event which gives rise to damages. Organizations may thus be considered de facto liable for a claim of "infringement on personal rights and freedoms" as broadly defined by the courts. Anyone throughout an organization who in any way processes personal data (as defined by articles 4(1) and 4(2)) will become an information security stakeholder. Securing against potential data breaches will no longer be enough.

Can organizations protect themselves by beefing up their information security level?

Per Article 24(1), organizations processing the personal information of EU residents need to demonstrate that they have assessed the risk of varying likelihood and severity of infringing upon data subjects' rights and freedoms. Article 25(1) further requires organizations to implement the appropriate "technical and organizational measures" to mitigate those risks.

The challenge organizations are facing is that assessing and mitigating risks to "individual rights and freedoms" goes well beyond considering the IT system attack surface or the likelihood of a data breach. Organizations need to develop a process by which they can define and understand the GDPR-relevant risks before the regulation is enforceable. However, that process also identifies the relevant risks, cost-effectively, on an on-going basis. To this end, automated enterprise threat modeling provides a meaningful solution for organizations dealing with the personal data of individuals protected by GDPR.

Long after the annual training programs have concluded and the compliance audits are set aside, evaluating and mitigating risks to data holders' rights and freedoms will be a daily operating concern. Getting a handle on information security for GDPR compliance, evaluating the relevant risks, and – very importantly – developing cost-effective mitigation strategies to reduce the GDPR-related risks – is why organizations and InfoSec consulting firms need automated enterprise threat modeling. Enterprise threat modeling starts with identifying the relevant business and technological risks in applications. It builds on this start to identify the relevant risks in deployment environments, devices, and systems.

Moreover, enterprise threat modeling automatically collates the individual threat model portfolio to provide security leaders and executives the security, data, risk, and regulatory "big-picture," including risks to personal rights and freedoms, across the full cyber ecosystem with the click of a button.

About the Author

Archie Agarwal, CISSP, Founder and CEO, ThreatModeler Software, Inc. Anurag "Archie" Agarwal, is the Founder & CEO of ThreatModeler Software, Chief Technical Architect of ThreatModeler™, and the principle author of the VAST (Visual, Agile, and Simple Threat modeling) methodology. Archie has more than 20 years of real-world experience in threat and risk analysis and has been instrumental in the successful implementation of secure software development processes at a number of Fortune 1000 companies, thereby minimizing their exposure to cyber threats and improving their ability to mitigate risks. Prior to founding ThreatModeler in 2010, he was the Director of Education Services at WhiteHat Security.

Defending Mission Critical Assets

(when you have no defenders)

by Derek Harp, founder, The Cyber List

If you have anything to do with cybersecurity then you know that there's a large and growing shortage of trained and experienced professionals available. For years, advances in technology and interconnectivity have been driving demand for defenders up faster than people with the needed skills have been entering the workforce, and all indications are that this trend is going to continue for the foreseeable future - leaving most of us on the front lines without troops to back us up. This problem is especially concerning for the small-to-medium business enterprise. It's almost a given that bad actors will come after your company - no matter the size, location or annual revenue - in some fashion sooner or later, and you don't want to be standing alone when they get there.

Obtaining Cybersecurity Help: Most Companies Don't Know Where to Begin

Anyone looking into workforce conditions will see that demand is driving up salaries for qualified cybersecurity professionals at a rate of 8-10% annually, yet companies often spend three to six months trying to fill open positions. For many businesses outside the Fortune 1000, the cost of acquiring your own cybersecurity defenders is excessive both in terms of financial outlay and time; with the open question of how much risk you're accepting by remaining under-protected in the interim. Training internal resources might cost less, but doing so takes longer and, unless you pay the premium that these skills command, you're likely to lose your defenders to someone who will.

What you want and what most companies urgently need are trusted third parties: a team of skilled cybersecurity practitioners that can assess your current security posture and help you develop and actually implement a meaningful security strategy. On the positive side, more cybersecurity providers are coming into the market every day; however, such commoditization is making finding the provider that best fits your company's unique needs a challenge all on its own. Every vendor has brochures, marketware, websites and tradeshow appearances designed to convince you that they're the answer you're looking for, but most of them are actually not. Whether for reasons of location, technological specializations, business model familiarity, resource availability or any of the dozens of other factors that

go into the selection process, only a few actually match up well with what you're in need of right now.

Even if your interest in reading all of those brochures and websites and talking with all of the sales reps might be higher than average, most people are looking for solutions over unnecessary conversations. They're looking for help as quickly as possible, not educating themselves on the state of cybersecurity offerings in the marketplace. In many situations time pressures inhibit searching, reading and comparative evaluations. Certainly no one whose company has just been hit by ransomware or who has found an Advanced Persistent Threat dwelling in their network can afford the time it takes to do research on service providers – they need to find a good cybersecurity team with the right skills that's available to help in their location immediately, and won't take advantage of your urgency on payment terms.

The truth is that the providers don't want to waste your time or theirs either. Believe it or not, even with demand significantly outpacing supply, some cybersecurity practitioners still spend time 'on the bench' awaiting their next work assignment because of delays in matching them up with the right projects. That isn't in anyone's best interest. Regardless of their specific focus, all vendors share the same core business model: providing goods and/or services to address customer goals. The more they are able to focus their resources on that the better. Time and effort spent in 'recruiting' new customers through marketing, websites, tradeshows, etc., is an accepted necessity, but everyone benefits from a mechanism that matches up customer needs to goods and service providers as efficiently as possible.

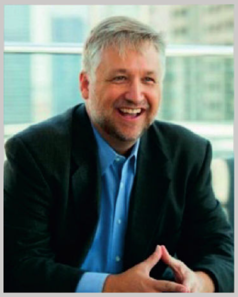
Some on the customer side may suggest that outsourcing the cybersecurity role to a managed security service provider (MSSP) is the answer to their concerns, and for some it may be a good choice. But for most of us, our security needs don't line up with engaging an MSSP, and it can be a cost-prohibitive option. We need a firm that can help us formulate and execute on a reasonable security plan tailored to our business profile.

Introducing the Cyber List

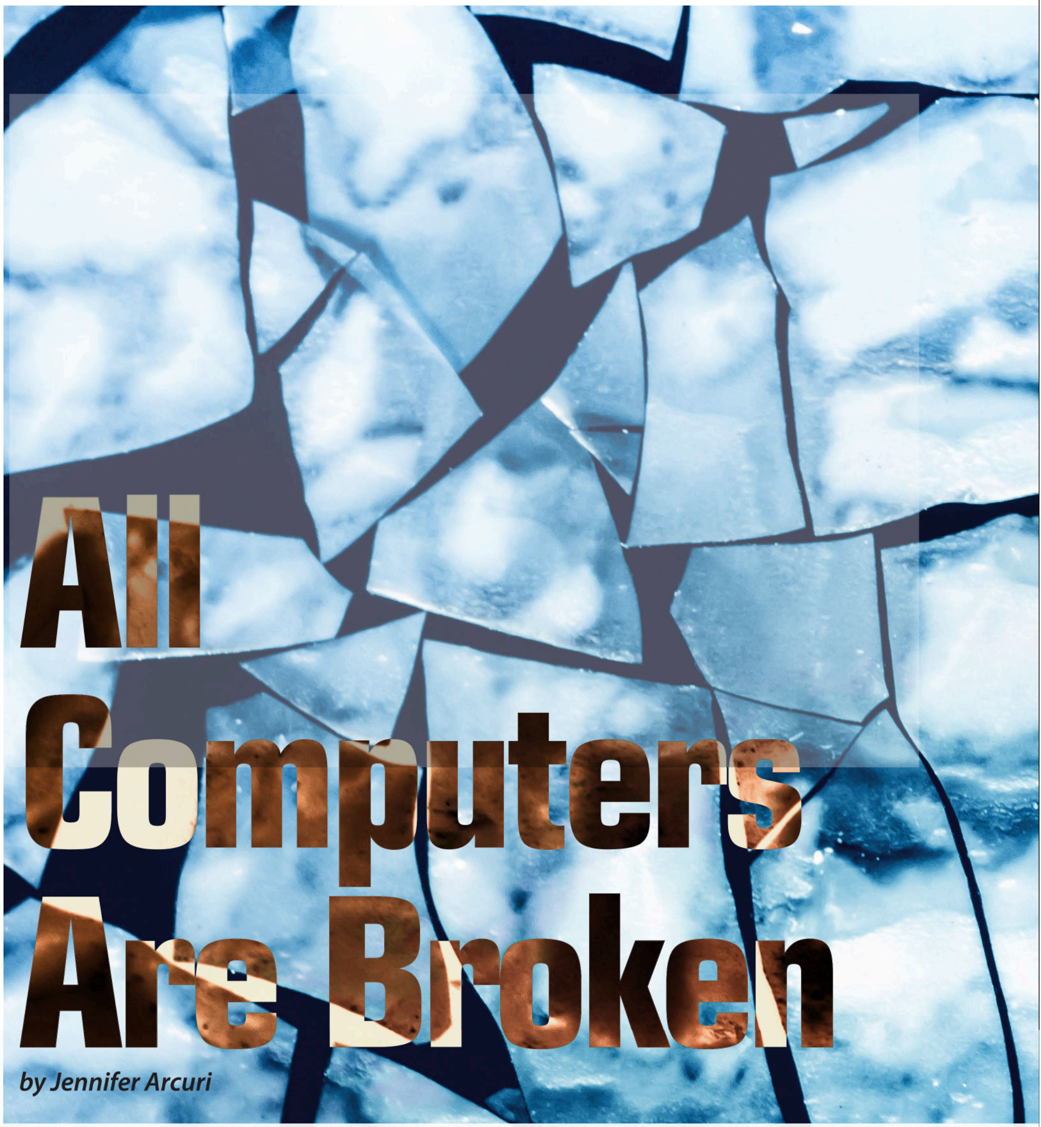
Whichever side of this problem you're on, connect with The Cyber List™ today. If you're a solution provider, let customers find you at the moment they are ready to engage and you're able to provide exactly what they are looking for. If you're looking for the right solution for your business, then become a member of The Cyber List community and start your qualified search right away. When you submit a request for proposal our system confidentially matches your profile with geographically available providers already familiar with companies in situations like yours. Member providers with available resources respond immediately with proposals to address your situation so you know how quickly they can get started and how much it should cost. You choose what you want to follow-up on.

Rather than starting from a lengthy web research project or just going with the same vendor you've already worked with by default, we arm you with the actionable information you need to make a decision and get your issues resolved. So, sign up with The Cyber List at https://www.thecyberlist.com now to start finding your vendors, and your clients, the easy way.

About the Author



Derek Harp has served as a founder, CEO, or advisor of early-stage companies for the last 20 years with a frequent focus on cyber security. Most recently, Derek founded TheCyberList.com as an organized answer to the growing number of personal requests for help he routinely receives. Previously he founded Control System Cyber Security Association International (CS2AI), a nonprofit organization dedicated to supporting local practitioner peer groups around the globe. He is currently a co-founder and board member of NexDefense, Inc., an Atlanta software company focused on the specific security needs of industrial control systems (ICS) asset owners. Derek's experience also includes co-founding and helping to grow the ICS business at the SANS Institute, GICSP Certification Steering committee chair and CEO and co-founder of LogiKeep, Inc.



All Computers Are Broken

by Jennifer Arcuri

Between the dependency on critical infrastructure, the rise of connected devices, and all the talk of increased cyber attacks, everyone has an interest in cyber security. It's a rare day where there isn't some big "hack" that's cost companies millions in losses, someone's identity has been stolen, or some indecent exposure has taken place online. This isn't about weak passwords, out of date software, another intrusion detection system, anti virus, or firewall. Automate and introduce all the managed services you want, but at the end of the day, we absolutely need more cyber skills and training.

The most obvious reason? — All computers are broken. Inherently computers are susceptible to an increasing number of threats, advances in attacking has made cybercrime easier to perform and harder to defend against.

Every system can be hacked. There is not a company, network or software which cannot be compromised in some way. It's time for us to embrace the problem solving abilities of hacking and accept it as part of the solution. Knowing how your adversary works and attacks allows for better targeting of resources, models like the cyber kill chain have helped paved the way for companies to better understand their risks. Yesterday it was mobile devices and apps, today its cryptojacking threats and ransomware. To keep ahead of the threats we need to understand the adversary and the tools they use.

We have heard it all from government, big corporates, and small business --- everyone has something to say about how to stay secure. And yet, cyber threats continue to escalate. There seems to be more and more breaches on a daily basis.

Why do we continue to listen to the same rhetoric and fear mongering?

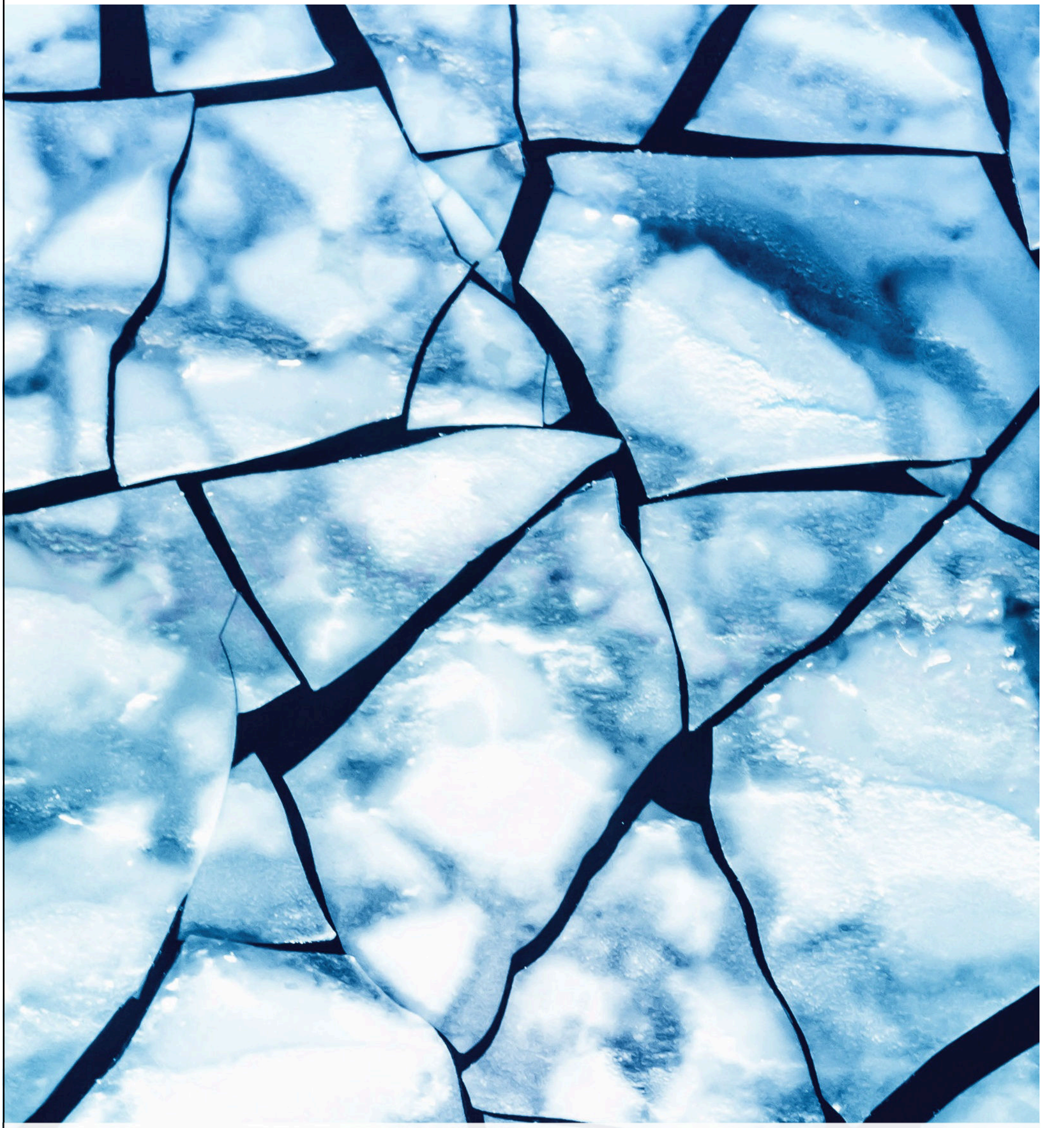
Isn't it time we heard from the hackers?

Our team has consistently breached security of devices, from the latest "ransomware proof" computers to "security appliances" meant to prevent advanced attacks. Exploit developers and purveyors of the art of hacking, our team embodies the hacker spirit to show you what your adversary already knows.

One of the biggest reasons companies are failing at security is because they don't have the right skills on the team. Even if they hire an outside consultant, there is still no guarantee that the missing "patches" pointed out are now secure and that the company is indeed, protected from further attack. The cyber consultancy model is flawed. Companies can't afford to keep up with the "ask" for security budget if there is no one on the team who can think as an attacker would. The result is a shift in industry.

Hackers are now essential.

Companies invest in hackers on their team rather then to "wait" to be made a target. These cyber skills are invaluable to the business because it better



prepares companies to handle more of their own internal breaches with a better incident response management. Having an on-site resource who can make sense of cyber security requirements and knowledge of the tools used can be invaluable to a company as an asset.

Hacker House™ has developed a Hands on Hacking course to give companies those real world simulations of what happens with their systems are attacked. It is designed to teach skills used by ethical hackers to conduct a variety of assessment activities. Hands on Hacking™ allows companies to quickly train and scale their security teams. Rather then pay for expensive theory based content and out of date information- companies are looking for real hackers to train their teams to respond to attacks. "Consulting" is not enough; companies want the "real deal;" hacking required.

The Hands on Hacking course is made up of modules where students are presented a topic and are taught how to launch an attack upon completion of each lesson. The course can be taken in a class-room environment, live online or our on-demand portal. Once the course is completed, students retain access to all lab work: a virtual hacking lab set up for a live 365 environment to hone their skills and better prepare defences for attacks.

Hacker House teaches the core concepts used in many cyber security related job roles from intelligence analysts to penetration testing. More and more companies are turning to the Hacker House Hands on Hacking™ course to deliver up to date content, with real world threats, to train teams in classroom, or remote from their laptops. For our remote and global network, we have introduced the live stream and on demand versions which will be available with all the trainings. Now you can hack the planet, wherever you are in the world!

> *Every system can be hacked. There is not a company, network or software which cannot be compromised in some way.*

Whatever your job in technology, isn't it time you learned how to protect yourself against modern threats?

Join us for an intensive in-person 4 day workshop or contact us for details of our upcoming live offerings. For a complete list of all the IN CLASSSROOM and LIVE STREAMED 2018 trainings please visit https://hacker.house/training

About the Author

Jennifer Arcuri is an advisor to Hackers and Founders in Silicon Valley, alongside Founders for Schools across the UK. In 2015 she also launched the Cyber Security group, Cyber TLA, as part of Tech London Advocates Group, and is a certified ethical hacker herself.

Cybersecurity Best Practices for Human Resources (HR)

by Yan Ross, J.D.

Ten Most Important Actions HR Can Take in Response to Cyber Threats

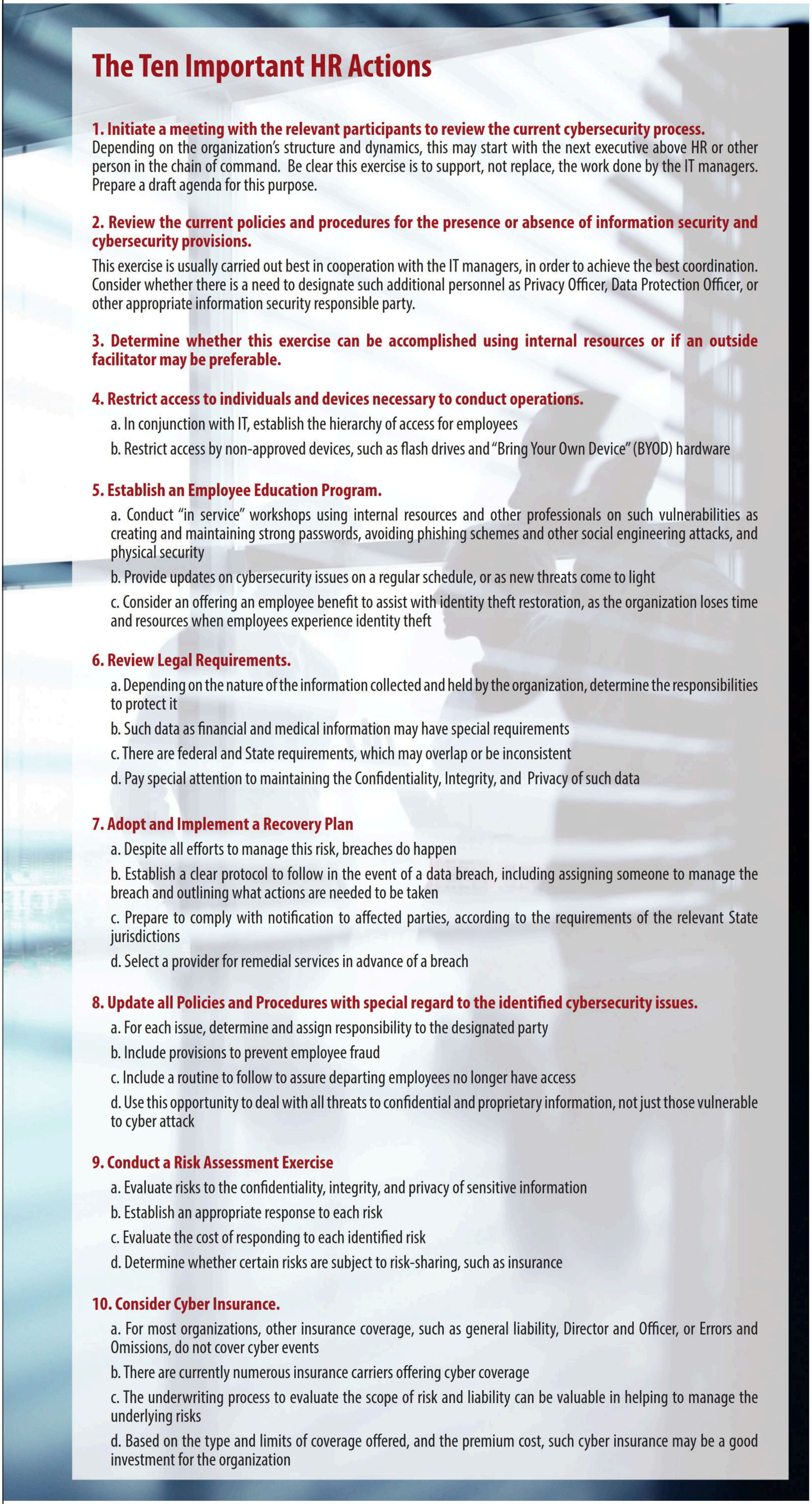
In today's world of growing identity theft and cyber attacks, the Human Resources (HR) office of nearly every organization needs to be an integral participant in developing and implementing ways to avoid the adverse effects of these criminal activities.

This article is focused on small businesses and non-profit organizations, since there is evidence that larger companies already have both the budget and awareness to respond to cyber threats. Based on current reports, it appears that many HR professionals are easily lulled into a false sense of security, arising out of several common misconceptions.

"If you can keep calm in the midst of a catastrophe, you have probably found someone to blame it on." Adopting and implementing policies and procedures is an excellent place to start. These rules of operation provide the basic instructions and guidelines on running an effective and efficient organization. Also, they are periodically reviewed and updated, affording an excellent opportunity to include healthy cyber practices, sometimes referred to as good "cyber hygiene."

Who are the organizational parties for HR to include in this exercise?

- Starting at the top, the C-level executives
- Information Technology (either internal or outside contractors)
- Accounting and Finance
- Compliance and Audit Officers (including outside accountants)
- All employees with access to the IT systems



The Ten Important HR Actions

1. Initiate a meeting with the relevant participants to review the current cybersecurity process.
Depending on the organization's structure and dynamics, this may start with the next executive above HR or other person in the chain of command. Be clear this exercise is to support, not replace, the work done by the IT managers. Prepare a draft agenda for this purpose.

2. Review the current policies and procedures for the presence or absence of information security and cybersecurity provisions.

This exercise is usually carried out best in cooperation with the IT managers, in order to achieve the best coordination. Consider whether there is a need to designate such additional personnel as Privacy Officer, Data Protection Officer, or other appropriate information security responsible party.

3. Determine whether this exercise can be accomplished using internal resources or if an outside facilitator may be preferable.

4. Restrict access to individuals and devices necessary to conduct operations.

a. In conjunction with IT, establish the hierarchy of access for employees

b. Restrict access by non-approved devices, such as flash drives and "Bring Your Own Device" (BYOD) hardware

5. Establish an Employee Education Program.

a. Conduct "in service" workshops using internal resources and other professionals on such vulnerabilities as creating and maintaining strong passwords, avoiding phishing schemes and other social engineering attacks, and physical security

b. Provide updates on cybersecurity issues on a regular schedule, or as new threats come to light

c. Consider an offering an employee benefit to assist with identity theft restoration, as the organization loses time and resources when employees experience identity theft

6. Review Legal Requirements.

a. Depending on the nature of the information collected and held by the organization, determine the responsibilities to protect it

b. Such data as financial and medical information may have special requirements

c. There are federal and State requirements, which may overlap or be inconsistent

d. Pay special attention to maintaining the Confidentiality, Integrity, and Privacy of such data

7. Adopt and Implement a Recovery Plan

a. Despite all efforts to manage this risk, breaches do happen

b. Establish a clear protocol to follow in the event of a data breach, including assigning someone to manage the breach and outlining what actions are needed to be taken

c. Prepare to comply with notification to affected parties, according to the requirements of the relevant State jurisdictions

d. Select a provider for remedial services in advance of a breach

8. Update all Policies and Procedures with special regard to the identified cybersecurity issues.

a. For each issue, determine and assign responsibility to the designated party

b. Include provisions to prevent employee fraud

c. Include a routine to follow to assure departing employees no longer have access

d. Use this opportunity to deal with all threats to confidential and proprietary information, not just those vulnerable to cyber attack

9. Conduct a Risk Assessment Exercise

a. Evaluate risks to the confidentiality, integrity, and privacy of sensitive information

b. Establish an appropriate response to each risk

c. Evaluate the cost of responding to each identified risk

d. Determine whether certain risks are subject to risk-sharing, such as insurance

10. Consider Cyber Insurance.

a. For most organizations, other insurance coverage, such as general liability, Director and Officer, or Errors and Omissions, do not cover cyber events

b. There are currently numerous insurance carriers offering cyber coverage

c. The underwriting process to evaluate the scope of risk and liability can be valuable in helping to manage the underlying risks

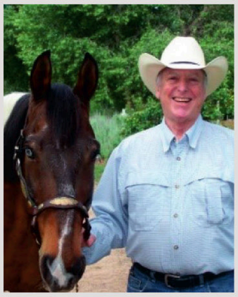
d. Based on the type and limits of coverage offered, and the premium cost, such cyber insurance may be a good investment for the organization

When should these actions be taken?

- At the earliest practicable time
- When new employees come to work, as part of the onboarding process
  - *This includes contractors with access to the system*
- When employees leave, as part of the exit process
  - *"Clean out your desk and return your keys" is not enough*
  - *This also includes contractors with access to the system*
- Periodically as cyber threats are identified, at least once a year
- As other organizational participants may require or changes are adopted in the organizational policies and procedures

Implementing these ten actions will provide the foundation for HR to participate in a substantial step forward in responding to the threat of cyber-attacks and managing the risk of damage to the organization caused by this growing challenge.

About the Author



Yan Ross is ICFE's Director of Special Projects, and the author of the Certified Identity Theft Risk Management Specialist ® XV CITRMS® course. As an accredited educator for over 20 years, he has addressed Identity. Theft Risk Assessment and management for consumers, organizations holding personally identifiable information, and professionals who work with individuals and organizations who are at risk of falling victim to identity thieves.

Stopping the Next WannaCry:

Engineering Security in Software by Design

by Tal Widerman

Most everyone I talk to has seen the news and heard about the WannaCry ransom worm. The first piece of ransomware melded with a worm, designed not only to lock up a computer but to leverage a major software vulnerability in windows – the SMB v1 protocol. It hit the United Kingdom's National Health Service, www.NHS.uk first, demanding $300 in bitcoins for each system it infected - in the NHS this amounted to about $500,000 USD in ransomware demand due to malware propagation. It then quickly spread across the globe, to more than 74 countries and hitting additional targets such as the Russian Interior Ministry and US-based FedEx.

"What made WannaCry such big news is not the financial impact but the fact that it locked up a hospital to the point where operations were delayed and lives were in jeopardy."

How WannaCry was created is very interesting. Here's what seems to have happened: The Shadow Brokers leaked a bunch of NSA hacking tools. One is called EternalBlue, a perfect exploit for creating a Windows worm - software that attacks a Microsoft windows SMB v1 vulnerability and then installs on the next vulnerable windows system and on and on...WannaCry is ransomware, this is software that encrypts a computer, in this case your windows hard drive(s), and asks for a payment ($300) to be made in bitcoins.

But what's even more interesting to me, is to look at the root cause – analyze why it was so successful and if future WannaCry-like malware could do the same kind of damage. The answer is a weak software deployment – either SMB v1 or SMB v2 are the problem. In fact, if you read any book on how to run Metasploit – to penetration test your network, it gets into details about the Server Message Block (SMB) protocol and recommends scanning the intranet first for weak SMB deployments to test exploitation on, first.

Even Microsoft has taken note and has created the SMB 1 Product Clearinghouse – it's their page of 'shame' to try to convince vendors to upgrade their SMB protocol code integration at least up to version 3.0 which includes encryption and is not vulnerable to similar ransomworms like WannaCry. The page is found here: http://www.bit.ly/SMBrisks/ and there is even more at this link https://aka.ms/StopUsingSMB1 dedicated to this issue.

It all gets down to better software by design with security modeled into the design, not an after fact. Just look at MITRE's Common Weakness Enumeration called CWE™ to see the community-developed list of common software security weaknesses at http://cwe.mitre.org . It serves as a common language, a measuring stick for software security tools, and as a baseline for weakness identification, mitigation, and prevention efforts. What you'll learn from the CWE program and what I propose is that we get past the past, ie, we need to build software without vulnerabilities – we need to start with strong authentication and strong encryption.

So, when it comes to products that need to integrate some form of file management in Windows platforms or integrate with those platforms, upgrading to SMB version 3 is the way to go, removing one less major vulnerability in your product. For example, many java developers who have integrated with the well-developed open-source JCIFS library to help them deploy SMB v1 on Non-windows platforms are now realizing that they also opened up their non-windows platforms to the same risks exploited by WannaCry. They are also looking for a way to move past their SMB v1 implementation and get to the more safe and secure SMB v3.

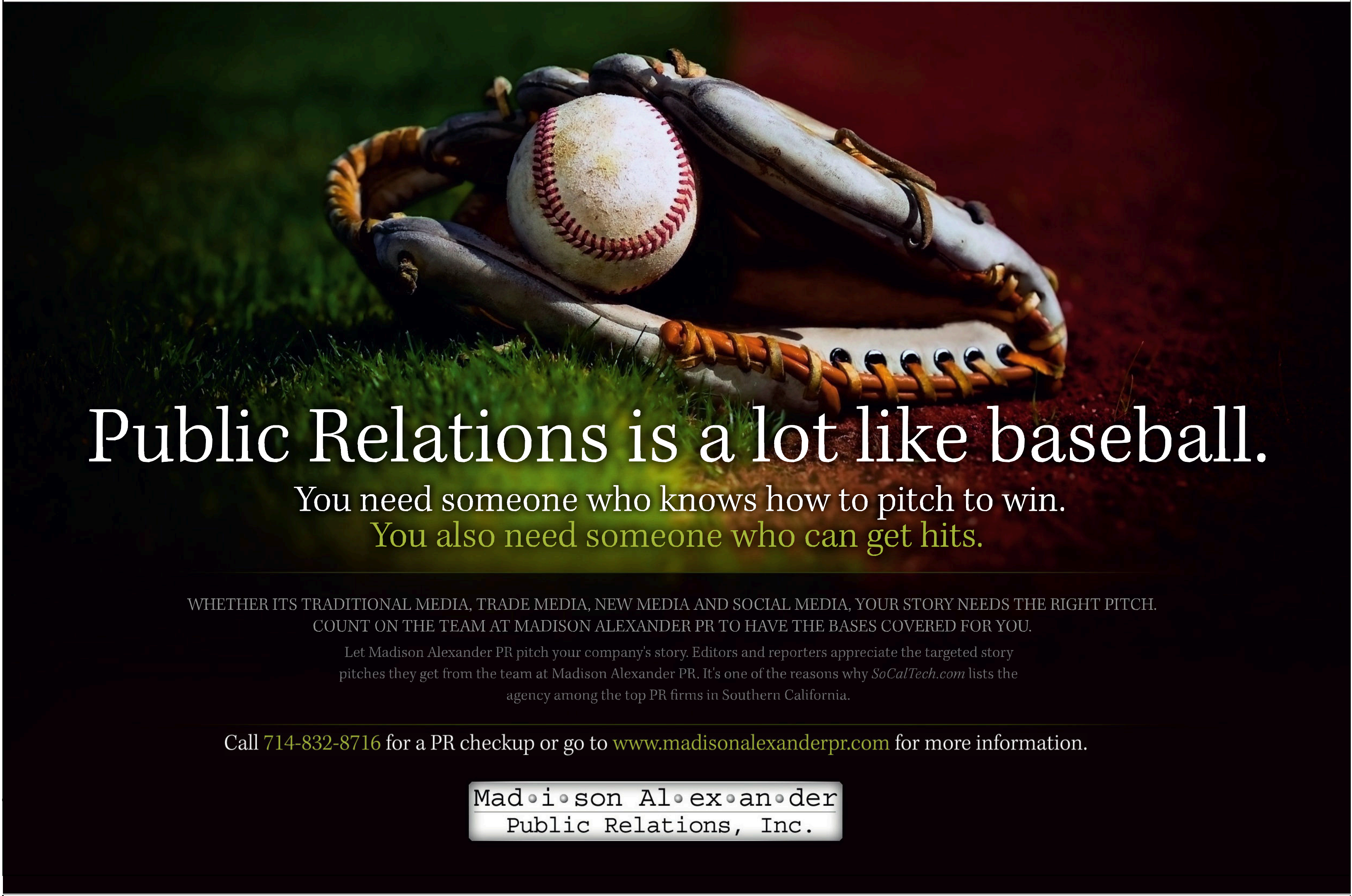
At Visuality Systems, we've worked with SIEM developers who need to rapidly scan the corporate network to retrieve event logs from all the Microsoft Windows Servers and Clients on the Network. They've learned how important doing this using SMB v3 and ensuring clients are not running any system with an SMB v1 or v2 on their network is so important.

The same holds true for software backup programmers, data management programmers and the Internet of Things developers. All of these groups are finally starting to see that security by design, inherent in the software development process is so important. So, let's work together to make security an inherent part of software design and this should reduce the risk that the next WannaCry will be able to exploit our solutions.

About the Author

Tal Widerman is the director of Marketing at Visuality Systems located at 3 Hatamar St. Hi Tech Star Building, Yokneam Illit. Israel. 20692002. For years Tal has been active in the file sharing technology marketplace, managing licensing and partnerships of Visuality's software and security libraries.

He loves to study cyber security trends and was one of the first to take notice of how WannaCry exploited an easily fixed vulnerability.


Public Relations is a lot like baseball.
You need someone who knows how to pitch to win.
You also need someone who can get hits.

Breach Prevention Starts with Time-based Security

by Gary S. Miliefsky

Here we are in 2018 wondering where all the time went? So much to do so little time. Time is of the essence. Time is the fire in which we burn. Ok, I'm sure you would agree that while time is a man-made concept, usually, it is completely out of our control. We can, for now at least, joke about time travel and time machines but understanding the importance of time, in specific regards to network security and breaches could change the dynamic dramatically. We could start winning again and stopping the breaches before they happen.

Time-based Security: The Futurist 1999 Discovery

Discovered and written about in 1999 by Winn Schwartau in his book called "Time-based Security", Winn must have been a time traveler because he wrote this book 20 years ahead of his time. No one really understood it back then. However, without even truly understanding the concept, more and more vendors are on the scene creating innovative ways to manipulate the time equation in regards to breaches. For example, deception-based technology vendors are trying to actually slow down breaches by creating dynamic honeypot-like environments for the cyber criminals to ensnare them long enough to stop their breach from being successful. They actually slow down the breach – they can affect the time it takes for a breach to occur, so they have manipulated 'breach time.'

On the other side of the equation, many vendors have bragging rights now about their artificial intelligence (a.i.) and machine learning systems coupled with crowdsourcing and cloud 'big data' so that they can analyze malware and cyber attacks in near real-time and even predict when and where the next threat will strike. Hence they have sped up or reduced the time required to detect a threat, once again affecting 'breach time' but in this case making it so successful breaches have to go even faster. Both approaches can be leveraged together to dramatically improve network security.

The Time-based Security Equation

So what is Time-based Security (TBS) and is there a formula we can use to quantifiably test and measure the effectiveness of these and other INFOSEC countermeasures? The answer is yes – TBS gives us a measurable foundation for stopping breaches – and here is the formula:
Protection(time) must be greater than Detection(time) + Response(time) or formulaically

$$Pt > Dt + Rt$$

Putting TBS to Work or Cybersecurity

Now let's think about our own cyber security posture from the cloud data to the firewall and throughout the intranet of our organization. Assuming we have the best training, techniques and tools in place – strong encryption, good key

A Real-world Example: Time Needed to Rob a Bank

Let's look at a real-world example of TBS – Bank Robbers. They drive up to the bank. They enter the bank and hold a gun to the teller, informing the teller to 'open the vault' and help them fill up their bags. Let's say the teller pressed the 'red button' silent alarm to call the local police. The police are on their way and will arrive in 11-12 minutes. Meanwhile the bank robbers fill their satchels in 9 minutes, hop in their getaway car and are gone on the 10th minute. A minute or two later, the police arrive, and of course it's a minute or two too late.

So the Protection time for this bank needed to be 12 minutes or more, to give the police time to arrive and catch the robbers. If the safe/vault required two employees to bring two sets of keys or two passcodes and maybe one of them was upstairs and recently had a hip replacement, maybe it would take that second teller an extra few minutes to get the the vault to turn their key and enter their secret code. That would have increased the protection time by a few minutes.

Look at it this way, the Detection time (when the teller pressed the alarm) was less than 1 minute but the Response time, when the police finally arrived was 11 or 12 minutes, so in this case Pt < Dt + Rt and the robbers get away. What if you took my advice, added the second set of keys, a second passcode i.e. two factor authentication? What if you actually moved the bank branch closer to the local police department. A building near the police goes up for sale, you buy it and move the branch. Now your Response time has been moved from 12 minutes to 2 minutes. This makes it really hard for the bank robbers to get in and out with the 'loot' and in fact, they would rather go elsewhere where the risks of successful exploitation are much lower.

management, authentication, up to date firewall, patched and secured endpoints, a great Security Information Event Management (SIEM) system and the best threat feeds on the planet, can we begin to measure our Dt and Rt? The answer is yes. We can review our logs, leverage our SIEM or a great MSSP partner and take notes as follows:

- **Time to detect an event**
- **Time to respond to an event**
- **How much damage can be done in Dt + Rt**

So to begin understanding how to use TBS to beat the next attacker and defend against a breach, we need to look at one more variable in the TBS equation and that's called Exposure(time) or Et. This is so important – Exposure time is the window of vulnerability or the crack in our armor which would allow an intruder to steal our crown jewels, in this case the important customer or confidential records and data sets we wish to protect.

In the case of the bank being robbed, our Et was 12 minutes (ie how long before the police actually arrived on the scene from the moment the robbers entered the bank branch) or Dt+Rt (time the teller took to press the red button plus the time it took for the police to arrive).

TBS Mission: Minimize our Exposure Time

We need to minimize Exposure time or at least make it smaller than the time it takes for the cybercriminals to complete the exploitation and steal our confidential data. There are two ways to minimize our Exposure time – one is to make Breaches go slower, for example using virtual machines and honeypots in deception-based security models, bandwidth limiting, data padding and stronger encryption throughout our organization.

For example, if our Dt = 12 minutes but we can get the cybercriminals to spend more than 12 minutes in our honeypot at the perimeter using deception-based security technologies, while they are busy attempting to steal fake but 'juicy' looking data, they are detected and stopped before they can breach the intranet and get at the real data. They can't exfiltrate real data if we Detected them fast enough.

Another way to slow down the breach is called 'data padding'. Imagine you could pad all the critical files on your network so their size exceeds the Exposure time (Et). An example would look something like this. Let's say your Et is 10 minutes and your network bandwidth (Bw) is 6 Gigabytes (Gb) per hour. So Et =10 min, Bw = 6Gb / hr, now we know what we need to do to pad our files. File size = (1/6 hr) / (6 Gb / hr) = 1GB, therefore, all critical files should be padded to be larger than 1Gb. When hackers try to steal critical data, it will take them too long to get it, because the time to steal one file is larger than our Exposure time, our Et. Make sense?

Now let us look at the flip side, which I alluded to earlier, we could go faster – we could speed up our Detection time and/or our Response time. To do this, we need real-time analytics coupled with human intelligence, artificial intelligence and machine learning. We need this information tied into our SIEM and our EDR (endpoint detect and response) as well as our firewall, ids/ips and switches. This would allow us to detect malicious traffic or an infected system and more rapidly isolate or quarantine it so that no data theft can occur.

We must know all of our threats as quickly as possible. We must know all of our serious or critical vulnerabilities as quickly as possible and understand the correlation between an exploiter or threat and the vulnerability they are attempting to exploit. Finally, we must track, control, manage and value all of our network assets, especially those that host or manage critical and confidential data.

We can also reduce Detection time (Dt) by defending against exploitable holes. If we are not using a CVE (common vulnerability and exposure) auditing system from any of the well-known vendors or even the OpenVAS free and open-source solution, we're at risk of too many open windows and doors. We need to patch, harden and reconfigure our systems to affect Dt, while we need next generation endpoint security solutions that can reduce our Response time (Rt) through detection, orchestration, automation and isolation. Some of the best methods for isolation include agent-based and agentless quarantine technology such as 802.1x as well as various methods of network access control (NAC).

In summary, the smaller we can make the Detection time plus the Response time, ie, Dt+Rt should be as close to zero as possible, the higher probability we cannot easily be breached and if we are breached, the data cannot be exfiltrated fast enough to cause harm or require regulatory compliance reporting. It's time we start asking our INFOSEC trusted MSSP partners and vendors – what are you doing in regards to Time-based Security? Can you slow down the breach? Do you offer any deception-based solutions? What can you do to speed up the Detection time and Response time? What threat intel and other tools do you offer? How fast is your EDR solution? Are we doing continuous/real-time backups known as Continuous Data Protection (CDP)? Have we tested and measured our Exposure time? By starting to focus on simple, measurements such as Protection time (Pt), Exposure time (Et), Detection time (Dt) and Response time (Rt), we can finally begin to understand our true breach prevention posture.

About the Author

Gary S. Miliefsky is the Publisher of Cyber Defense Magazine (CDM). Gary is a globally recognized cybersecurity expert, inventor and founder of numerous cybersecurity companies, is a frequent invited guest on national and international media commenting on mobile privacy, cyber security, cyber-crime and cyber terrorism, also covered in Forbes, Fortune and Inc Magazines. Miliefsky is a Founding Member of the US Department of Homeland Security (http://www.DHS.gov), the National Information Security Group (http://www.NAISG.org) and the OVAL advisory board of MITRE responsible for the CVE Program (http://CVE.mitre.org). Gary is a member of ISC2.org and is a CISSP®. He's frequently writing thought provoking articles at CDM and on LinkedIn as a Top 1% of all INFOSEC LinkedIn profiles and a Top 3% Globally on LinkedIn. Learn more about Gary on our website.

2018 CYBER SECURITY PREDICTIONS

by Pierluigi Paganini

1. Ransomware

One of the most dangerous cyber threats

The number of malware continues to increase, every week security experts discover new strains of ransomware involved in attacks in the wild.

Ransomware such as WannaCry, NotPetya and Bad Rabbit could have a dramatic impact on almost any industry. Financial data published by major multinational firms such as the transportation giant Maersk and FedEx confirmed huge losses caused by the threat.

Last year the transportation giant Maersk announced that it would incur hundreds of millions in U.S. dollar losses due to the NotPetya ransomware massive attack, FedEx confirmed the cost caused by the massive NotPetya ransomware are $300m in lost business and response costs.

In 2018, ransomware will continue to be one of the most dangerous threats for organizations and end-users. Vxers will be more focused on mobile devices implementing new evasion techniques making these threats difficult to detect. In the next months new ransom-as-a-service platforms will appear in the criminal underground allowing wannabe crooks to arrange their ransomware campaigns.

2. Cybercriminals focus on crypto currencies

The spike in the value of some crypto currencies observed in the last part of the year will attract crooks that will intensify their fraudulent activities against virtual currency industry.

We will expect to see an increasing number of malware developed to steal funds from victims' computers or to deploy hidden mining tools on machines.

A growing number of websites and servers will be compromised to deploy cryptocurrency miner scripts, security experts will uncover massive mining campaign that involve hundred of thousands of systems.

We will see that mass Internet scanning campaigns for wallet accidentally exposed online will increase, we will also see several phishing campaigns focused on cryptocurrency firms and targeting ICO (Initial Coin Offering) events.

3. Nation State Actors hacking

. . . a serious problem for governments and businesses

All governments continue improve their cyber capabilities for both defense and offense purposes.

The number of hacking campaigns conducted by Nation-state actors will increase, the level of sophistication of many attackers is expected to increase making it harder to attribute these cyber attacks to specific entities.

State sponsored APT groups from China, North Korea and Russia will continue to target Western entities for cyber espionage purposes and sabotage.

We will expect an intensification of hacking activities conducted by Iran-Linked group, such as OilRig, mostly focused on Middle East targets, while at the same time, Russian APT groups will extend their activities to Asia.

The risk of escalation and retaliation in cyberspace, the increasing number of cyber attacks and cyber threats even more sophisticated could have a destabilizing effect on international peace and security. The risk of conflict between Nation state caused cyber-attacks will encourage all States to engage in law-abiding, norm-respecting and confidence-building behavior in their use of ICT.

4. GDPR

Several companies will not be in compliance with the new EU regulation by the deadline.

Once the GDPR legislation becomes enforceable it will provide data owners transparency into how their information is collected and used.

Companies that do not comply will face fines of up to 20 million Euros or 4 percent of global turnover, a disaster for companies that are not ready by the GDPR deadline.

As businesses enter 2018 and realize the effort necessary to become GDPR compliant by May 25, 2018, will cause chaos and turmoil if pressured by regulators. The regulation is far from being adopted by many states, Italy is one of them. Many organizations will continue to have a wary approach and the effects could be severe.
The regulation will have a huge impact on security teams for any companies that operates in a multi-national contest.

5. IoT devices

A dangerous weapon in the wrong hands

Unsecured IoT devices are a privileged target of hackers and cyber criminals. The availability of source code for IoT malware (i.e. Mirai) will cause the rapid diffusion of new powerful 'thingbots'. Many of them will be offered for rent in the criminal underground allowing to power massive DDoS attacks.

The good news is that IoT vendors will dedicate more effort to secure their devices and harden them against exploitation.

6. Mobile malware

on the rise

Mobile threat landscape will see the raise of malware, especially ransomware and financial malware. These malicious codes are designed to target mobile devices causing the infection of millions of devices worldwide. In many cases the malware was spread through compromised apps published on the official Google Play Store.

7. Cloud security

A major concern for businesses

A growing number of companies will rely on cloud storage, unfortunately in many of cases totally ignoring cyber security principle. The lack of security will attract the interest of cyber criminals and state-sponsored hackers, the number of security breaches involving cloud infrastructures will rapidly increase.

In response, enterprises should adopt security guidelines and strategies to mitigate the risk of exposure to cyber threats.

8. CyberBullying

… it's an emergency

When dealing with the social impact of cyber security we cannot avoid mentioning cyberbullying that refers to practice of using technology to harass, or bully, someone else. This type of crime is very common and often underestimated, teenagers will continue to be the most exposed and the number of victims will dramatically increase.

It is a global widespread emergency that must be rapidly addressed by Government with specific law framework and social initiatives.

9. Cyber-Insurance

proposal will explode

The current scenario is creating the optimal conditions for a rapid growth of the demand for cyber insurance. Cyber-insurance will grow at a steady pace, organizations are aware of the potential risks and will evaluate also the possibility to mitigate and transfer them with a cyber insurance.

Due to growing awareness of cyber-attacks across the recent months, businesses' will start to consider security as a key commercial risk rather than an 'IT issue.'

Once the GDPR legislation becomes enforceable, organizations will gain a visibility of their cyber-risks and will evaluate with interest solutions to transfer the risk such as a cyber-insurance.

The Europe and Asia will have a greater penetration of cyber insurance liability policies respect the US, where the market is more mature.

Financial institutions and information technology firms will continue to be primary adopters of cyber insurance policies, policies, with respect to the United States, where the market is more mature.

2018 InfoSec AWARDS

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

CDM INFOSEC AWARDS 2018

Welcome to the InfoSec Awards for 2018. It's been nearly six months in the making - our annual review of the hottest, most innovative, best, market leaders, next-generation and cutting edge INFOSEC companies offering incredible products and services. This year we decided to also include and give credit to a small list of public relations firms that do a great job to help get the word out about these innovators and we've included a small list of very important people to keep an eye on - because they are making a difference. We scoured the globe and found nearly 3,000 companies who create and offer the most respected InfoSec products and services. Some of them you have never even heard of until today. Some are startups and some are early stage. Some are bigger known players. But what they all have in common is a drive for innovation. They truly want to help you get ahead of the next breach. They are on a mission to help you comply with regulations, stop the cybercriminals, hackers, hacktivists, cyber terrorists and threats against critical infrastructure. They offer solutions for businesses and government agencies of all sizes, big and small. We took this list and narrowed it down to nearly 500 market leaders as finalists and of those our judges selected less than 200 winners. The judging was challenging and difficult and to those who didn't win this year, there will always be future opportunities to continue to improve and innovate and let us know. The outcome is here, for your review. Please join us in congratulating the winners - stop by their booth at RSAC 2018 and let them know you found them in Cyber Defense Magazine.

Gary Miliefsky
Publisher

CATEGORIES

Advanced Persistent Threat (APT) | Anti-Malware

HOT COMPANY Advanced Persistent Threat CYBER DEFENSE MAGAZINE 2018

AWN CyberSOC
Arctic Wolf

ARCTIC WOLF

CUTTING EDGE Advanced Persistent Threat CYBER DEFENSE MAGAZINE 2018

Hornetsecurity Advanced Threat Protection (ATP)
Hornetsecurity

HORNETSECURITY®

BEST PRODUCT Advanced Persistent Threat CYBER DEFENSE MAGAZINE 2018

ThreatQ
ThreatQuotient

THREATQUOTIENT

NEXT GEN Advanced Persistent Threat CYBER DEFENSE MAGAZINE 2018

Fidelis Elevate
Fidelis CyberSecurity

Fidelis™ Cybersecurity

CATEGORIES

Advanced Persistent Threat (APT) | Anti-Malware

MOST INNOVATIVE
Advanced Persistent Threat
CYBER DEFENSE MAGAZINE
2018

Cognito

Vectra

VECTRA®

NEXT GEN
Anti-Malware
CYBER DEFENSE MAGAZINE
2018

Ericom Shield

Ericom Software

ERICOM
Be Connected, Be Secure

HOT COMPANY
Anti-Malware
CYBER DEFENSE MAGAZINE
2018

FFRI yarai

FFRI

FFRI

LEADER
Anti-Malware
CYBER DEFENSE MAGAZINE
2018

PC Matic Pro 1.1.5.0

PC Pitstop Inc.

PC Pitstop

CATEGORIES

Anti-Malware | Anti-Phishing

BEST PRODUCT
Anti-Malware
CYBER DEFENSE MAGAZINE
2018

CylancePROTECT®

Cylance Inc.

CYLANCE

CUTTING EDGE
Anti-phishing
CYBER DEFENSE MAGAZINE
2018

Bromium Secure Platform 4.0

Bromium

Br Bromium®

LEADER
Anti-phishing
CYBER DEFENSE MAGAZINE
2018

ThreatTest v1

Edgewave

EdgeWave™

LEADER
Anti-phishing Research
CYBER DEFENSE MAGAZINE
2018

Phishme

Cofense

COFENSE

CATEGORIES

Anti-Phishing | Antivirus Gateway

HOT COMPANY
Anti-phishing Training
CYBER DEFENSE MAGAZINE
2018

Phishme

COFENSE

COFENSE

BEST PRODUCT
Anti-phishing Protection
CYBER DEFENSE MAGAZINE
2018

Phishme

COFENSE

COFENSE

MOST INNOVATIVE
Anti-phishing
CYBER DEFENSE MAGAZINE
2018

IRONSCALES

IronScales

IRONSCALES
World's 1st *Automated Phishing* Prevention, Detection & Response Platform

HOT COMPANY
Anti-Virus Gateway
CYBER DEFENSE MAGAZINE
2018

Bluedon Anti-Virus Gateway v 1.1

Bluedon Information Security Technologies Co, Ltd.

BD ® 蓝盾 BLUEDON

CATEGORIES

Application Security

BEST PRODUCT
Application Security
CYBER DEFENSE MAGAZINE
2018

Bromium Secure Platform 4.0

Bromium

Br Bromium®

CUTTING EDGE
Application Security
CYBER DEFENSE MAGAZINE
2018

IAST CxIAST

Checkmarx

CHECKMARX

LEADER
Application Security
CYBER DEFENSE MAGAZINE
2018

Citrix NetScaler ADC

Citrix Systems Inc.

CITRIX®

NEXT GEN
Application Security
CYBER DEFENSE MAGAZINE
2018

CYBRIC's Continuous Application Security Platform

Cybric

CYBRIC

CATEGORIES

Application Security | Artificial Intelligence and Machine Learning

HOT COMPANY
Application Security
CYBER DEFENSE MAGAZINE
2018

ShiftLeft
ShiftLeft

ShiftLeft

EDITOR'S CHOICE
Application Security
CYBER DEFENSE MAGAZINE
2018

Twistlock 2.2
Twistlock

Twistlock™

MOST INNOVATIVE
Application Security
CYBER DEFENSE MAGAZINE
2018

Mobile Operative Risk Evaluator
XTN Lab

XTN
Cognitive Security

LEADER
Artificial Intelligence and Machine Learning
CYBER DEFENSE MAGAZINE
2018

Enterprise Immune System 3
Darktrace

DARKTRACE

CDM INFOSEC AWARDS 2018

CATEGORIES

Artificial Intelligence and Machine Learning

CUTTING EDGE
Artificial Intelligence and Machine Learning
CYBER DEFENSE MAGAZINE
2018

Endpoint Security AI

Deep Instinct

deepinstinct

EDITOR'S CHOICE
Artificial Intelligence and Machine Learning
CYBER DEFENSE MAGAZINE
2018

Security Platform 2.2.5

Empow

empow
You have it in you.

BEST PRODUCT
Artificial Intelligence and Machine Learning
CYBER DEFENSE MAGAZINE
2018

ERPScan Smart CyberSecurity Platform for SAP

ERPScan

ERPScan

MOST INNOVATIVE
Artificial Intelligence and Machine Learning
CYBER DEFENSE MAGAZINE
2018

JASK ASOC Platform

JASK

JASK

CATEGORIES

Artificial Intelligence and Machine Learning | Authentication | Biometrics

NEXT GEN
Artificial Intelligence and Machine Learning
CYBER DEFENSE MAGAZINE
2018

Open Threat Management Platform 3.3
Seceon

seceon

HOT COMPANY
Artificial Intelligence and Machine Learning
CYBER DEFENSE MAGAZINE
2018

Cognito
Vectra

VECTRA®

HOT COMPANY
Authentication Multifactor
CYBER DEFENSE MAGAZINE
2018

LaunchKey
Iovation

iovation®

BEST PRODUCT
Biometrics
CYBER DEFENSE MAGAZINE
2018

Netverify 2.5.0
Jumio

JUMIO®

CATEGORIES

Breach & Attack Simulation | Central Log Management | CEO of the Year

CUTTING EDGE
Breach & Attack Simulation
CYBER DEFENSE MAGAZINE
2018

AttackIQ FireDrill

Attack IQ

EDITOR'S CHOICE
Breach & Attack Simulation
CYBER DEFENSE MAGAZINE
2018

Breach & Attack Simulation Platform

Cymulate

HOT COMPANY
Central Log Management
CYBER DEFENSE MAGAZINE
2018

Fluency

Fluency

MOST INNOVATIVE
CEO of the Year
CYBER DEFENSE MAGAZINE
2018

Shridhar Mittel

Zimperium

CATEGORIES

CEO of the Year | CISO of the Year | Cloud Security

EDITOR'S CHOICE
CEO of the Year
CYBER DEFENSE MAGAZINE
2018

Brad Taylor
Proficio

PROFICIO™

LEADER
CISO of the Year
CYBER DEFENSE MAGAZINE
2018

Phil Richards
Ivanti

ivanti

BEST PRODUCT
Cloud Security
CYBER DEFENSE MAGAZINE
2018

Unified Security Management (USM) Anywhere
AlienVault

ALIEN VAULT

MOST INNOVATIVE
Cloud Security
CYBER DEFENSE MAGAZINE
2018

Bitglass Zero-day CASB Core
BitGlass

bitglass
Next-Gen CASB

CATEGORIES

Cloud Security

EDITOR'S CHOICE
Cloud Security
CYBER DEFENSE MAGAZINE
2018

Citrix Cloud

Citrix Systems, Inc.

CiTRIX®

MOST INNOVATIVE
Cloud Security
CYBER DEFENSE MAGAZINE
2018

Dome9 Arc Platform

Dome9 Security

Dome9 SECURITY

BEST PRODUCT
Cloud Security
CYBER DEFENSE MAGAZINE
2018

Centra Security Platform 2.5

GuardiCore

GuardiCore
Securing the Software Defined Data Center

HOT COMPANY
Cloud Security
CYBER DEFENSE MAGAZINE
2018

CloudAdvisor and CloudSPF

HyTrust

HYTRUST

CATEGORIES

Cloud Security

CUTTING EDGE
Cloud Security
CYBER DEFENSE MAGAZINE
2018

BreakingPoint Cloud

Ixia Solutions Group, A Keysight Business

ixia
A Keysight Business

PUBLISHER'S CHOICE
Cloud Security
CYBER DEFENSE MAGAZINE
2018

Cloud SecOps Program

Threat Stack

threat stack

NEXT GEN
Cloud Security
CYBER DEFENSE MAGAZINE
2018

SecureDoc CloudVM 8.2

WinMagic

WINMAGIC®

LEADER
Cloud Security
CYBER DEFENSE MAGAZINE
2018

Illumio Adaptive Segmentation Platform

Illumio

illumio

CDM
INFOSEC
AWARDS
2018

CATEGORIES

Content Management and Filtering | CTO | Cyber Risk Management

HOT COMPANY
Content Management and Filtering
CYBER DEFENSE MAGAZINE
2018

iPrism Web Security v.102

Edgewave

EdgeWave™

EDITOR'S CHOICE
CTO of the Year
CYBER DEFENSE MAGAZINE
2018

Corey Nachreiner

WatchGuard Technologies

WatchGuard™

EDITOR'S CHOICE
Cyber Risk Management
CYBER DEFENSE MAGAZINE
2018

Kenna Security Platform

Kenna

kenna
Know Your Risk

HOT COMPANY
CyberSecurity
CYBER DEFENSE MAGAZINE
2018

ANS Ecosystem 7th Generation

Blue Ridge Networks

BLUERIDGE® NETWORKS

CATEGORIES

CyberSecurity | CyberSecurity Discovery | Data Center Security

LEADER
CyberSecurity
CYBER DEFENSE MAGAZINE
2018

Cognito
Vectra

VECTRA

CUTTING EDGE
CyberSecurity Discovery
CYBER DEFENSE MAGAZINE
2018

Cyberbit EDR
Cyberbit

CYBERBIT
PROTECTING A NEW DIMENSION

MOST INNOVATIVE
CyberSecurity Discovery
CYBER DEFENSE MAGAZINE
2018

HID Global
HID Global

HID®

HOT COMPANY
Data Center Security
CYBER DEFENSE MAGAZINE
2018

Illumio Adaptive Segmentation Platform
Illumio

illumio

CATEGORIES

Data Center Security | Data Loss Prevention

NEXT GEN
Data Center Security
CYBER DEFENSE MAGAZINE
2018

BrickStor
RackTop Systems

RACKTOP®

EDITOR'S CHOICE
Data Center Security
CYBER DEFENSE MAGAZINE
2018

Cognito
Vectra

VECTRA®

EDITOR'S CHOICE
Data Loss Prevention
CYBER DEFENSE MAGAZINE
2018

Digital Guardian Data Protection Platform 7.4
Digital Guardian

DIGITALGUARDIAN®

CUTTING EDGE
Data Loss Prevention
CYBER DEFENSE MAGAZINE
2018

DLP that Works Platform 15.4
GTB Technologies

GTB Technologies
Data Protection that Works™

CATEGORIES

Database Security | DDoS Protection | Deception Based Security

MOST INNOVATIVE
Database Security
CYBER DEFENSE MAGAZINE
2018

DB Networks

DB Networks

DB NETWORKS.

MOST INNOVATIVE
DDoS Protection
CYBER DEFENSE MAGAZINE
2018

Thunder TPS

A10 Networks Inc.

A10 Networks

MOST INNOVATIVE
Deception Based Security
CYBER DEFENSE MAGAZINE
2018

ThreatDefend™ Deception and Response Platform

Attivo Networks

Attivo NETWORKS

LEADER
Deception Based Security
CYBER DEFENSE MAGAZINE
2018

Fidelis Elevate

Fidelis CyberSecurity

Fidelis™ Cybersecurity

CDM INFOSEC AWARDS 2018

CATEGORIES

Deception Based Security | Deep Sea Phishing | Digital Footprint Security

BEST PRODUCT
Deception Based Security
CYBER DEFENSE MAGAZINE
2018

Nfusion 2
Ntrepid Corporation

NTREPID

HOT COMPANY
Deception Based Security
CYBER DEFENSE MAGAZINE
2018

DeceptionGrid 6.1
TrapX

TRAPX
SECURITY

EDITOR'S CHOICE
Deep Sea Phishing
CYBER DEFENSE MAGAZINE
2018

Inky Phish Fence
Inky

inky.com

NEXT GEN
Digital Footprint Security
CYBER DEFENSE MAGAZINE
2018

Nfusion 2
Ntrepid Corporation

NTREPID

CATEGORIES

Digital Rights Management | Email Security and Management

CUTTING EDGE
Digital Footprint Security
CYBER DEFENSE MAGAZINE
2018

Enterprise Digital Footprint

RiskIQ

RISKIQ

LEADER
Digital Rights Management
CYBER DEFENSE MAGAZINE
2018

Seclore

Seclore

SECLORE
Securing Information Wherever It Goes

HOT COMPANY
Email Security and Management
CYBER DEFENSE MAGAZINE
2018

Bromium Secure Platform 4.0

Bromium

Br Bromium®

CUTTING EDGE
Email Security and Management
CYBER DEFENSE MAGAZINE
2018

GreatHorn Inbound Email Security

GreatHorn

GreatHorn

CDM INFOSEC AWARDS 2018

CATEGORIES

Email Security and Management | Encryption

MOST INNOVATIVE
Email Security and Management
CYBER DEFENSE MAGAZINE
2018

Valimail Enforce

Valimail

VALIMAIL™

EDITOR'S CHOICE
Email Security and Management
CYBER DEFENSE MAGAZINE
2018

Advanced Content Disarm and Reconstruction solutions 7.2

Votiro

VOTIRO
SECURED.

BEST PRODUCT
Encryption
CYBER DEFENSE MAGAZINE
2018

Apricorn

Apricorn

APRICORN

MOST INNOVATIVE
Encryption
CYBER DEFENSE MAGAZINE
2018

Self-Defending Key Management Service ™ (SDKMS)

Fortanix

Fortanix

CATEGORIES

Encryption | Endpoint Security

LEADER
Encryption
CYBER DEFENSE MAGAZINE
2018

CryptoComply

SafeLogic

SafeLogic

CUTTING EDGE
Encryption
CYBER DEFENSE MAGAZINE
2018

ParaDoxBox Enterprise 1.2.5.0

Secure Channels

SECURE CHANNELS

CUTTING EDGE
Endpoint Security
CYBER DEFENSE MAGAZINE
2018

360Skylar v 6.3

360 Skylar

360
ENTERPRISE SECURITY GROUP

MOST INNOVATIVE
Endpoint Security
CYBER DEFENSE MAGAZINE
2018

Tachyon 3.1

1E

1E

CDM
INFOSEC
AWARDS
2018

CATEGORIES

Endpoint Security

CUTTING EDGE
Endpoint Security
CYBER DEFENSE MAGAZINE
2018

Absolute Platform, featuring Reach 7
Absolute

ABSOLUTE®

EDITOR'S CHOICE
Endpoint Security
CYBER DEFENSE MAGAZINE
2018

Bromium Secure Platform 4.0
Bromium

Br Bromium®

CUTTING EDGE
Endpoint Security
CYBER DEFENSE MAGAZINE
2018

Code 42
Code 42

CODE42

BEST PRODUCT
Endpoint Security
CYBER DEFENSE MAGAZINE
2018

Comodo Advanced Endpoint Protection (AEP)
Comodo

COMODO
Advanced Endpoint Protection

CDM
INFOSEC
AWARDS
2018

CATEGORIES

Endpoint Security

HOT COMPANY
Endpoint Security
CYBER DEFENSE MAGAZINE
2018

CounterTack Predictive EDR

CounterTack

CounterTack

NEXT GEN
Endpoint Security
CYBER DEFENSE MAGAZINE
2018

Endpoint Protection Platform with AI

DriveLock SE

DriveLock
Control, Secure & Protect.

LEADER
Endpoint Security
CYBER DEFENSE MAGAZINE
2018

ESET

ESET

eset®

EDITOR'S CHOICE
Endpoint Security
CYBER DEFENSE MAGAZINE
2018

Kaspersky Endpoint Security for Business 11

Karspersky

KASPERSKY lab

CATEGORIES

Endpoint Security | Enterprise Mobile Threat Defense | Enterprise Security

NEXT GEN
Endpoint Security
CYBER DEFENSE MAGAZINE
2018

SentinelOne
Endpoint Protection Platform 2.5
Sentinel One Inc.

SentinelOne®

PUBLISHER'S CHOICE
Endpoint Security
CYBER DEFENSE MAGAZINE
2018

TriagingX
TriagingX

TriagingX

HOT COMPANY
Enterprise Mobile Threat Defense
CYBER DEFENSE MAGAZINE
2018

Zimperium Mobile Threat Defense
Zimperium

ZIMPERIUM®
MOBILE THREAT DEFENSE

CUTTING EDGE
Enterprise Security
CYBER DEFENSE MAGAZINE
2018

Lastline Breach Defender v1
Lastline

lastline™

CATEGORIES

Enterprise Security | ERP Security

EDITOR'S CHOICE
Enterprise Security
CYBER DEFENSE MAGAZINE
2018

ThreatQ
ThreatQuotient

BEST PRODUCT
Enterprise Security
CYBER DEFENSE MAGAZINE
2018

Cognito
Vectra

LEADER
Enterprise Security
CYBER DEFENSE MAGAZINE
2018

Advanced Content Disarm and Reconstruction solutions 7.2
Votiro

MOST INNOVATIVE
ERP Security
CYBER DEFENSE MAGAZINE
2018

Onapsis Security Platform v1.9.16
Onapsis

CDM INFOSEC AWARDS 2018

CATEGORIES

Firewall | Fraud Prevention

BEST PRODUCT
Firewall
CYBER DEFENSE MAGAZINE
2018

Untangle NG Firewall

Untangle

untangle™

MOST INNOVATIVE
Firewall
CYBER DEFENSE MAGAZINE
2018

WatchGuard Firebox M470

WatchGuard

WatchGuard™

HOT COMPANY
Fraud Prevention
CYBER DEFENSE MAGAZINE
2018

Netverify 2,5.0

Jumio

JUMIO®

BEST PRODUCT
Fraud Prevention
CYBER DEFENSE MAGAZINE
2018

ThreatMetrix ID

ThreatMetrix

ThreatMetrix®

CATEGORIES

Hybrid Cloud Security | ICS/SCADA Security

MOST INNOVATIVE
Hybrid Cloud Security
CYBER DEFENSE MAGAZINE
2018

Cavirin Hybrid Cloud Security

Cavirin

cavirin

HOT COMPANY
ICS/SCADA Security
CYBER DEFENSE MAGAZINE
2018

Claroty Platform

Claroty

CLAROTY

NEXT GEN
ICS/SCADA Security
CYBER DEFENSE MAGAZINE
2018

CyberX Platform

CyberX

CyberX

MOST INNOVATIVE
ICS/SCADA Security
CYBER DEFENSE MAGAZINE
2018

Industrial Immune System

Darktrace Industrial

DARKTRACE
INDUSTRIAL

CATEGORIES

ICS/SCADA Security | Identity & Access Management

CUTTING EDGE
ICS/SCADA Security
CYBER DEFENSE MAGAZINE
2018

SCADAguardian 17.5

Nozomi Networks

NOZOMI NETWORKS

EDITOR'S CHOICE
Identity & Access Management
CYBER DEFENSE MAGAZINE
2018

Auth0

Auth0

Auth0

BEST PRODUCT
Identity & Access Management
CYBER DEFENSE MAGAZINE
2018

Centrify Zero Trust Security

Centrify

Centrify®

LEADER
Identity & Access Management
CYBER DEFENSE MAGAZINE
2018

IAM Services

Herjavec Group

HERJAVEC GROUP

CATEGORIES

Identity & Access Management | Incident Response

MOST INNOVATIVE
Identity & Access Management
CYBER DEFENSE MAGAZINE
2018

Ivanti Identity Director, powered by RES 10.2
Ivanti

ivanti

MOST INNOVATIVE
Identity & Access Management
CYBER DEFENSE MAGAZINE
2018

SailPoint's Open Identity Pla-tform
SailPoint

SailPoint

HOT COMPANY
Identity & Access Management
CYBER DEFENSE MAGAZINE
2018

Semperis' Directory Services Protection Platform
Semperis

Semperis
Enterprise Identity Protection

NEXT GEN
Incident Response
CYBER DEFENSE MAGAZINE
2018

Demisto
Demisto

DEMISTO

CDM INFOSEC AWARDS 2018

CATEGORIES

Incident Response | Infosec Research | Infosec Startup of the Year

CUTTING EDGE
Incident Response
CYBER DEFENSE MAGAZINE
2018

Siemplify
Siemplify

SIEMPLIFY

LEADER
Infosec Research
CYBER DEFENSE MAGAZINE
2018

ESET
ESET

eset®

NEXT GEN
Infosec Startup of the Year
CYBER DEFENSE MAGAZINE
2018

Corelight Sensor
Corelight

corelight

EDITOR'S CHOICE
Infosec Startup of the Year
CYBER DEFENSE MAGAZINE
2018

Polarity
Polarity

POLARITY

CATEGORIES

Insider Threat Detection

CUTTING EDGE
Infosec Startup of the Year
CYBER DEFENSE MAGAZINE
2018

XM
XM

XM • DEFENSE BY OFFENSE®

BEST PRODUCT
Insider Threat Detection
CYBER DEFENSE MAGAZINE
2018

ThreatDefend™
Deception and Response Platform
Attivo Networks

Attivo NETWORKS

HOT COMPANY
Insider Threat Detection
CYBER DEFENSE MAGAZINE
2018

Code 42
Code 42

CODE42

CUTTING EDGE
Insider Threat Detection
CYBER DEFENSE MAGAZINE
2018

Dtex Advanced User Behavior Intelligence Platform
Dtex System

systems Dtex

CATEGORIES

Intrusion Prevention Systems (IPS) | Managed Security Service Provider (MSSP)

LEADER
Insider Threat Detection
CYBER DEFENSE MAGAZINE
2018

ObserveIT

ObserveIT

observe it

EDITOR'S CHOICE
Intrusion Prevention Systems (IPS)
CYBER DEFENSE MAGAZINE
2018

Hillstone S-Series Network Intrusion Prevention System (NIPS) V2.1

Hillstone Networks

Hillstone™ NETWORKS

MOST INNOVATIVE
Managed Security Service Provider (MSSP)
CYBER DEFENSE MAGAZINE
2018

Unified Enterprise Security

Masergy Communications

MASERGY

HOT COMPANY
Managed Security Service Provider (MSSP)
CYBER DEFENSE MAGAZINE
2018

Managed CyberSecurity Services

Proficio

PROFICIO™

CATEGORIES

Memory Augmentation | Messaging Security | Messaging Security

LEADER
Managed Security Service Provider (MSSP)
CYBER DEFENSE MAGAZINE
2018

MSSP
Herjavec Group

HERJAVEC GROUP

BEST PRODUCT
Memory Augmentatio
CYBER DEFENSE MAGAZINE
2018

Polarity
Polarity

POLARITY

HOT COMPANY
Messaging Security
CYBER DEFENSE MAGAZINE
2018

ePrism Email Security 11.1
EdgeWave

EdgeWave™

CUTTING EDGE
Messaging Security
CYBER DEFENSE MAGAZINE
2018

Vaporstream 3.5.1.1
Vaporstream

Vaporstream

CDM INFOSEC AWARDS 2018

CATEGORIES

Microsegmentation | Multi-factor Authentication

MOST INNOVATIVE
Microsegmentation
CYBER DEFENSE MAGAZINE
2018

GuardiCore Centra Security Platform 2.5

GuardiCore

GuardiCore
Securing the Software Defined Data Center

BEST PRODUCT
Microsegmentation
CYBER DEFENSE MAGAZINE
2018

Illumio Adaptive Segmentation Platform

Illumio

illumio

MOST INNOVATIVE
Multi-factor Authentication
CYBER DEFENSE MAGAZINE
2018

Attribute Exchange Network

ID DataWeb

iddataweb

BEST PRODUCT
Multi-factor Authentication
CYBER DEFENSE MAGAZINE
2018

Authenticator App 1.1.2

Veridium

VERIDIUM
HANDS ON SECURITY

CATEGORIES

Network Access Control | Network Security and Management

BEST PRODUCT
Network Access Control
CYBER DEFENSE MAGAZINE
2018

Portnox CLEAR Winter
Portnox

portnox™

HOT COMPANY
Network Security and Management
CYBER DEFENSE MAGAZINE
2018

IntellaTap-VM
APCON

APCON
Solutions for Networks

EDITOR'S CHOICE
Network Security and Management
CYBER DEFENSE MAGAZINE
2018

Service SmartWall vNTD
Corero

corero

CUTTING EDGE
Network Security and Management
CYBER DEFENSE MAGAZINE
2018

Network Modeling and Cyber Risk Scoring Platform
RedSeal

REDSEAL

CATEGORIES

Network Security and Management | Network Traffic Analysis | Next Generation Endpoint Protection | Patch and Configuration Management

MOST INNOVATIVE
Network Security and Management
CYBER DEFENSE MAGAZINE
2018

Tufin Orchestration Suite 17-2

Tufin

tufin

LEADER
Network Traffic Analysis
CYBER DEFENSE MAGAZINE
2018

Corelight Sensor

Corelight

corelight

EDITOR'S CHOICE
Endpoint Protection
CYBER DEFENSE MAGAZINE
2018

FFRI

FFRI

FFRI

BEST PRODUCT
Patch and Configuration Management
CYBER DEFENSE MAGAZINE
2018

Apache Spot

Cloudera

cloudera

CATEGORIES

Patch and Configuration Management | PR firm for InfoSec

EDITOR'S CHOICE
Network Access Control
CYBER DEFENSE MAGAZINE
2018

Ivanti Patch Management

Ivanti

ivanti

HOT COMPANY
PR firm for InfoSec
CYBER DEFENSE MAGAZINE
2018

Finn Partners

Finn Partners

FINNPARTNERS

EDITOR'S CHOICE
PR firm for InfoSec
CYBER DEFENSE MAGAZINE
2018

Madison Alexander PR

Madison Alexander PR, Inc

Mad•i•son Al•ex•an•der
Public Relations, Inc.

MOST INNOVATIVE
PR firm for InfoSec
CYBER DEFENSE MAGAZINE
2018

ARPR

ARPR

arpr
PRopelling What's Possible

CDM INFOSEC AWARDS 2018

CATEGORIES

Privacy Expert of the Year | Privacy Management Software | Privileged Account Security | Public Cloud Security

EDITOR'S CHOICE
Privacy Expert of the Year
CYBER DEFENSE MAGAZINE
2018

Kabir Barday

One Trust

OneTrust

HOT COMPANY
Privacy Management Software
CYBER DEFENSE MAGAZINE
2018

Privacy Management Software

One Trust

OneTrust

NEXT GEN
Privileged Account Security
CYBER DEFENSE MAGAZINE
2018

Privileged Account Security Solution

CyberArk

CYBERARK®

NEXT GEN
Public Cloud Security
CYBER DEFENSE MAGAZINE
2018

Polygraph

Lacework

LACEWORK™

CATEGORIES

Risk Management

CUTTING EDGE
Risk Management
CYBER DEFENSE MAGAZINE
2018

Digital Shadows SearchLight™
Digital Shadows

digital shadows_

BEST PRODUCT
Risk Management
CYBER DEFENSE MAGAZINE
2018

Kenna Security Platform
Kenna

kenna
Know Your Risk

NEXT GEN
Risk Management
CYBER DEFENSE MAGAZINE
2018

AtomicEye RQ
Nehemiah Security

NEHEMIAH
SECURITY

LEADER
Risk Management
CYBER DEFENSE MAGAZINE
2018

RiskSense Platform
RiskSense

RiSKSENSE™

CDM
INFOSEC
AWARDS
2018

CATEGORIES

Risk Management | SaaS/Cloud Security | Security Automation & Orchestration

HOT COMPANY
Risk Management
CYBER DEFENSE MAGAZINE
2018

Security Services Practice

The Chertoff Group

THE CHERTOFF GROUP

MOST INNOVATIVE
SaaS/Cloud Security
CYBER DEFENSE MAGAZINE
2018

Cyren Cloud Security 4.0

Cyren

CYREN

NEXT GEN
SaaS/Cloud Security
CYBER DEFENSE MAGAZINE
2018

Hillstone CloudView V2.1

Hillstone Networks

Hillstone™
NETWORKS

EDITOR'S CHOICE
Security Automation & Orchestration
CYBER DEFENSE MAGAZINE
2018

DFLabs IncMan

DFLabs

DFLABS
CYBER INCIDENTS UNDER CONTROL

CATEGORIES

Security Company of the Year

CUTTING EDGE Security Company of the Year
CYBER DEFENSE MAGAZINE
2018

Cybereason
Cybereason

cybereason

HOT COMPANY Security Company of the Year
CYBER DEFENSE MAGAZINE
2018

Herjavec Group
Herjavec Group

HERJAVEC GROUP

MOST INNOVATIVE Security Company of the Year
CYBER DEFENSE MAGAZINE
2018

Illumio
Illumio

illumio

PUBLISHER'S CHOICE Security Company of the Year
CYBER DEFENSE MAGAZINE
2018

Proficio
Proficio

PROFICIO™

CDM
INFOSEC
AWARDS
2018

CATEGORIES

Security Company of the Year

CUTTING EDGE
Security Company
of the Year
CYBER DEFENSE MAGAZINE
2018

Seceon
Seceon

seceon

EDITOR'S CHOICE
Security Company
of the Year
CYBER DEFENSE MAGAZINE
2018

SonicWall
SonicWall

SONICWALL™

NEXT GEN
Security Company
of the Year
CYBER DEFENSE MAGAZINE
2018

Cognito
Vectra

VECTRA®

LEADER
Security Company
of the Year
CYBER DEFENSE MAGAZINE
2018

WatchGuard
WatchGuard Technologies

WatchGuard™

CATEGORIES

Security Investigation Platform | Security Software | Security Training

NEXT GEN
Security Investigation Platform
CYBER DEFENSE MAGAZINE
2018

Awake Security Investigation Platform 1.0

Awake Security

AWAKE

MOST INNOVATIVE
Security Software
CYBER DEFENSE MAGAZINE
2018

BUFFERZONE 5.6

Bufferzone Security

BUFFERZONE

EDITOR'S CHOICE
Security Training
CYBER DEFENSE MAGAZINE
2018

Hands on Hacking

Hacker House

HACKER
HOUSE

MOST INNOVATIVE
Security Training
CYBER DEFENSE MAGAZINE
2018

Security Awareness Training 4.9

Inspired eLearning

inspired eLearning
education for your enterprise

CATEGORIES

Security Training | Security-as-a-Service | SIEM

BEST PRODUCT
Security Training
CYBER DEFENSE MAGAZINE
2018

Security Education Platform
Wombat Security Technologies

wombat® security technologies

HOT COMPANY
Security-as-a-Service
CYBER DEFENSE MAGAZINE
2018

OPAQ 360 Platform
OPAQ

OPĀQ℠ Networks

HOT COMPANY
SIEM
CYBER DEFENSE MAGAZINE
2018

Security Platform 2.2
Empow

e empow
You have it in you.

EDITOR'S CHOICE
SIEM
CYBER DEFENSE MAGAZINE
2018

Exabeam Security Intelligence Platform (SIP)
Exabeam

exabeam

CATEGORIES

SIEM | Social Media, Web Filtering, and Content Security | SSL Visibility | Storage and Archiving

BEST PRODUCT
SIEM
CYBER DEFENSE MAGAZINE
2018

Threat Lifecycle Management (TLM) Platform

LogRhythm

CUTTING EDGE
Social Media, Web Filtering, and Content
CYBER DEFENSE MAGAZINE
2018

The ZeroFOX Platform

ZeroFOX

ZEROFOX

BEST PRODUCT
SSL Visibility
CYBER DEFENSE MAGAZINE
2018

Thunder SSLi

A10 Networks

A10 Networks

MOST INNOVATIVE
Storage and Archiving
CYBER DEFENSE MAGAZINE
2018

BrickStor

RackTop Systems

RACKTOP

CDM INFOSEC AWARDS 2018

CATEGORIES

Threat Intelligence

LEADER
Threat Intelligence
CYBER DEFENSE MAGAZINE
2018

Unified Security Management (USM) Anywhere

AlienVault

ALIEN VAULT

BEST PRODUCT
Threat Intelligence
CYBER DEFENSE MAGAZINE
2018

Anomali Enterprise 3.0

Anomali

ANOMALI™

HOT COMPANY
Threat Intelligence
CYBER DEFENSE MAGAZINE
2018

Alpine Patrol Cyber Intelligence Access Orchestration

NetQuest CorporationW

NetQuest

MOST INNOVATIVE
Threat Intelligence
CYBER DEFENSE MAGAZINE
2018

ThreatBook

ThreatBook

ThreatBook

CATEGORIES

Threat Intelligence | Threat Modeling

EDITOR'S CHOICE
Threat Intelligence
CYBER DEFENSE MAGAZINE
2018

TC Complete
ThreatConnect

THREATCONNECT™

NEXT GEN
Threat Intelligence
CYBER DEFENSE MAGAZINE
2018

ThreatQ
ThreatQuotient

THREATQUOTIENT

CUTTING EDGE
Threat Intelligence
CYBER DEFENSE MAGAZINE
2018

Untangle, Inc
Untangle, Inc.

untangle™

MOST INNOVATIVE
Threat Modeling
CYBER DEFENSE MAGAZINE
2018

ThreatModeler
ThreatModeler Software

ThreatModeler™

CATEGORIES

Unified Threat Management (UTM) | User Behavior Analytics

HOT COMPANY
Unified Threat Management (UTM)
CYBER DEFENSE MAGAZINE
2018

Untangle NG Firewall

Untangle, Inc.

untangle™

MOST INNOVATIVE
Unified Threat Management (UTM)
CYBER DEFENSE MAGAZINE
2018

WatchGuard Firebox T35

WatchGuard Technologies

WatchGuard™

BEST PRODUCT
User Behavior Analytics
CYBER DEFENSE MAGAZINE
2018

Risk Fabric 6.0.7

Bay Dynamics

Bay Dynamics®

LEADER
User Behavior Analytics
CYBER DEFENSE MAGAZINE
2018

Exabeam Advanced Analytics

Exabeam

exabeam

CATEGORIES

User Behavior Analytics | Vendor Risk Management | Vulnerability Management

MOST INNOVATIVE
User Behavior Analytics
CYBER DEFENSE MAGAZINE
2018

Gurucul Risk Analytics
Gurucul

GURUCUL
PREDICTIVE SECURITY ANALYTICS

EDITOR'S CHOICE
Vendor Risk Management Platform (VRMP)
CYBER DEFENSE MAGAZINE
2018

iTrust
iTrust

iTrust®

LEADER
Vulnerability Management
CYBER DEFENSE MAGAZINE
2018

Endpoint Security for Endpoint Manager 2017.3
Ivanti

ivanti

CUTTING EDGE
Vulnerability Management
CYBER DEFENSE MAGAZINE
2018

Kenna Security Platform
Kenna Security

kenna
Know Your Risk

CDM INFOSEC AWARDS 2018

CATEGORIES

Vulnerability Management

MOST INNOVATIVE
Vulnerability Management
CYBER DEFENSE MAGAZINE
2018

Unified VRM 4.6

NopSec

NEXT GEN
Vulnerability Management
CYBER DEFENSE MAGAZINE
2018

Code Dx 2.6

Code Dx

CUTTING EDGE
Vulnerability Management
CYBER DEFENSE MAGAZINE
2018

Kenna Security Platform

Kenna Security

BEST PRODUCT
Vulnerability Management
CYBER DEFENSE MAGAZINE
2018

Skybox Vulnerability Control

Skybox Security

CATEGORIES

Web application Security | Wireless, Mobile, or Portable Device Security

LEADER
Web application Security
CYBER DEFENSE MAGAZINE
2018

Contrast Protect and Assess
Version 3.4.5
Contrast Security

MOST INNOVATIVE
Wireless, Mobile or Portable Device Security
CYBER DEFENSE MAGAZINE
2018

GoSilent
Silent Circle

LEADER
PR firm for InfoSec
CYBER DEFENSE MAGAZINE
2018

News & Experts
News & Experts

HOT COMPANY
Risk Management
CYBER DEFENSE MAGAZINE
2018

Balbix
Balbix

How do you stop an enterprise phishing attack in 19 minutes? Human intelligence, of course.

by John "Lex" Robinson

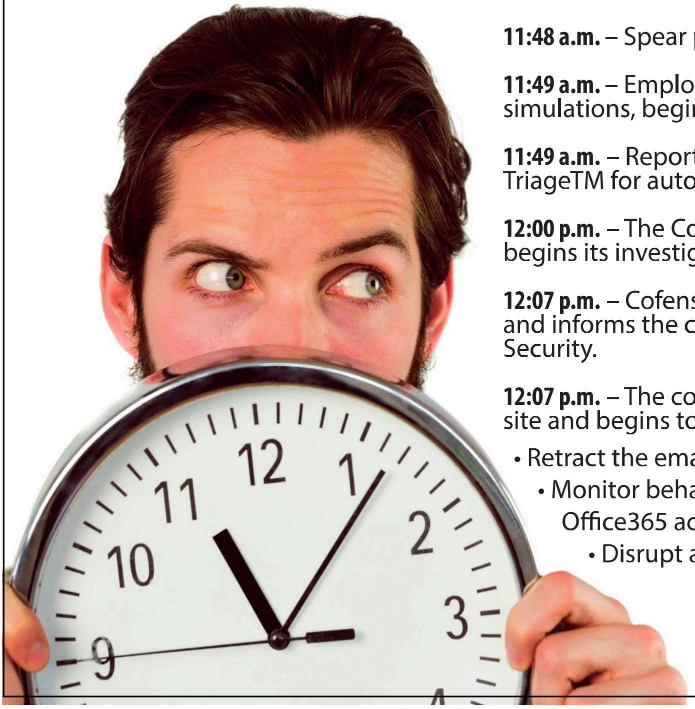
What do you do when a phishing attacker sends your users an email that mimics your CEO so well that lots of people click? You trust in having a collective phishing defense, assuming you have one in place. That's what one Cofense™ (formerly PhishMe) client did—and they stopped the attack in under 20 minutes.

The attacker did his homework.

The client, a healthcare technology provider, faced an especially well-crafted attack. "The email looked and sounded exactly as though our CEO had sent it," said the VP of Information Security.

The fake email asked employees to click a link to show they understood an important corporate policy, taking them to a counterfeit O365 page asking for login credentials. The idea was to steal credentials, gain file system access and reroute automatic payroll deposits. The bad news: the email looked so credible that many recipients clicked. The good news: a hawk-eyed employee reported it and incident responders sprang into action.

Their response was a blend of man and machine—user-supplied intelligence fed to an incident response platform, Cofense Triage™. Before Cofense, the team had a backlog of thousands of employee-reported emails. The platform automates their analysis, allowing the Cofense Phishing Defense Center, a global team of security consultants, to work with the client for fast incident response. Here's how fast the company and Cofense disrupted the attack:



11:48 a.m. – Spear phishing campaign launched.

11:49 a.m. – Employees, trained through phishing simulations, begin reporting the email.

11:49 a.m. – Reported emails went to Cofense TriageTM for automatic analysis.

12:00 p.m. – The Cofense Phishing Defense Center begins its investigation on behalf of the client.

12:07 p.m. – Cofense completes the investigation and informs the company's VP of Information Security.

12:07 p.m. – The company blocks the phishing site and begins to:

- Retract the email from inboxes
- Monitor behavior coming from affected Office365 accounts
- Disrupt any lateral movement

"We removed the email quickly," said the VP, "though in the space of a few minutes a lot of people clicked. Once we contained the threat, we started on repair and recovery work, seeing who clicked and mitigating problems linked to their accounts. All of this was the result of a single well-crafted phishing email. If we hadn't been prepared, the damage would have been worse. We were able to retract the email in under 20 minutes."

The team has recently complemented Cofense Triage with capabilities to help automate the retraction of malicious emails.

The stakes will always be high.

Attackers looking to make a quick buck will continue targeting healthcare organizations for their valuable data. It's one reason why a collective defense strategy is a must.

By enlisting the entire organization in awareness, reporting and response, the client continues to reduce the risk of phishing and a host of other threats that bypass traditional technology layers, demonstrating the power of a collective defense in safeguarding the entire organization against today's top threats.

John "Lex" Robinson
Anti-phishing strategist, Cofense

Lex has over 30 years of experience in information technology with a strong focus on strategic planning and program delivery. He is responsible for Cofense Professional Services (formerly PhishMe Professional Services) delivery strategy and provides hands-on program consulting, as well as customized results analysis and recommendations for clients seeking to reduce their organizations' susceptibility to phishing attacks.

Prior to Cofense, Lex's professional career has included consulting and management of product and service delivery teams for small businesses, glo Wbal Fortune 20 organizations and Government Agencies.

Lex is a Certified Counter Intelligence Threat Analyst (CCTA), holds an Electronic Engineering Degree, has numerous technical and behavioral science certificates, as well as continuing professional development credits in IT Security and Ethical Hacking.

Additionally, Lex is a frequent speaker on personal responsibility and ethics in information security and has published multiple books and papers on topics from security awareness to social engineering.

GO ANYWHERE®
Managed File Transfer