STRATEGY / INSIGHT / TECHNOLOGY

info security

Malicious Mail Mayhem

Q4, 2018 / Volume 15 / Issue 4

AUTOMATION'S DARK SIDE
How attackers use machine learning

CYBER INSURANCE
The next step in cybersecurity preparedness

FAITH IN ZERO TRUST
The resurrection of the zero trust network concept




White HAT BALL 2019

Friday 25 January 2019
Lancaster London, Hyde Park

Gold table of 10 - £2,100
Platinum table of 10 - £3,100

The White Hat Ball is a sell-out, glamorous and fun-filled event hosting 650 guests from the Cyber Security and Information Risk industry. It offers the chance to have an incredible evening with industry colleagues, being entertained from start to finish, all in the name of a fantastic cause, Childline.

Tables are available for purchase now and we're hoping for another sell-out year so if you're interested, please complete our booking form.

We also have plenty of opportunities to showcase your brand and support of Childline through **event sponsorship**, ranging from sponsoring the champagne reception, cupcakes, technology and more.

JOIN THE SPONSORS | RESERVE A TABLE

0203 772 9059 **charlotte.bignell@nspcc.org.uk**

Support the White Hat Ball
Make a Difference

www.whitehatevents.org

In aid of
childline

Watch Ball highlights from 2018

#WHB19

CONTENTS

The Contributors...

Michael Hill

Acting Editor
With his degree in English Literature & Creative Writing and his love of the written word, Michael is dedicated to keeping *Infosecurity* readers up-to-date with all the latest from the infosec industry.
@MichaelInfosec

Dan Raywood

Contributing Editor
Dan has written about IT security since 2008. He has spoken at 44CON, SteelCon and Infosecurity Europe, as well as writing for a number of vendor blogs and speaking on webcasts.
@danraywood

James Ingram

Digital Sales Manager
James sells print advertising for *Infosecurity* and is also responsible for selling across all the online marketing and advertising options, including webinars and white papers.
@infosecJames

Rebecca Harper

Portfolio Digital Marketing Manager
Rebecca is a skilled content and digital strategy marketer with a proven track record of delivering innovative campaigns in the tech and information services industries. **@BeccaInfosecMag**

Infosecurity Magazine

Infosecurity Magazine

@Infosecurity Mag

infosecurity

Acting Editor **Michael Hill**
michael.hill@reedexpo.co.uk
+44 (0)20 84395643

Contributing Editor **Dan Raywood**
dan.raywood@reedexpo.co.uk
+44 (0)20 84395648

Online UK News Editor **Phil Muncaster**
phil@pmmediauk.com

Online US News Editor **Kacy Zurkus**
kacy.zurkus@kszfreelance.com

Proofreader
Phee Waterfield
pheewaterfield@gmail.com

Print and Online Advertising
James Ingram
james.ingram@reedexpo.co.uk
+44 (0)20 89107029

Portfolio Digital Marketing Manager
Rebecca Harper
Rebecca.harper@reedexpo.co.uk
+44 (0)20 89107861

Senior Digital Marketing Executive
Ankita Bulsara
ankita.bulsara@reedexpo.co.uk
+44 (0)20 8910 7751

INFOSECURITY GROUP

Director **Nicole Mills**
Nicole.Mills@reedexpo.co.uk
+44 (0)20 84395683

Head of Marketing **Ralu Ionescu**
+44 (0)20 89107712

Head of Sales **Paul Stone**
+44 (0)208 9107817

Production Manager **Andy Milsom**

ISSN 1754-4548

Locklizard

Protect your Documents against Leakage & Theft

Protect from piracy

- Stop copying & prevent unauthorized distribution
- Stop printing / control prints
- Stop screen grabbing
- Expire & revoke access
- Audit document use

Share securely

Control access to and use of information inside and outside your organization.

Securely, and cost effectifely, distribute and manage your digital content.

Control BYOD use and lock PDF documents to specific locations.

Dynamic control

Change access, print, location restriction and expiry controls even after distribution.

Apply dynamic watermarks displaying individual user information.

Revoke documents no matter where they reside.

Total protection

Using AES 256 bit encryption, public key technology, device locking, IP & country restrictions and DRM controls, you can be assured that documents are safe, both at rest and in transit.

We don't use insecure plugins, JavaScript or passwords.

From the Editor...

I Open at the Close

There does seem to be something slightly poetic in the fact that this issue of *Infosecurity*, our last of 2018, is also my very first as acting editor of this publication

With Eleanor's latest addition to the family, Ralph Thomas Dallaway, arriving safe and well in September, she is now on maternity leave spending time with her new mini infosec superstar, and thus the responsibility of steering the editorial ship falls to me.

It's a wonderful feeling to have the opportunity to sit, albeit temporarily, in the editor's chair. I'm genuinely so excited for what the next several months will bring and I can't wait to meet the challenge head-on, but before I look forward, I'm going to start with a glance back at a year that was certainly a busy one for the industry.

The social engineering threat known as business email compromise came to the fore in a big way in 2018 (see more on that on page 12), cyber insurance as a means of indemnity skyrocketed (see page 46) and the GDPR finally came into force after what seemed like an eternity of build-up (check out our review of the first six months of the new regs on page 44).

What's more, unsurprisingly but not unimportantly, we saw a number of high-profile breaches and privacy issues come to light this year with the likes of Dixons Carphone, British Airways and even The Pentagon all making the news. However, it was a certain social media giant that stole many of the headlines.

In March, it was revealed that Facebook had exposed data on up to 87 million of its users to Cambridge Analytica (a political consulting firm) via a quiz called 'thisisyourdigitallife'. The incident left CEO Mark Zuckerberg facing a lot of heat as Facebook's privacy policies were brought under immense scrutiny. Facebook was forced to launch a range of new privacy and transparency features to win back user trust.

Then, in September, news broke that Facebook issued a password reset for some 90 million users after a flaw was found in its code that affected the 'View As' feature – which lets users see how their own profile page looks to other people. Apparently, the vulnerability could have allowed attackers to steal Facebook access tokens and use them to take over people's accounts.

Facebook was quick to patch the exploit and the storm seemed to settle pretty fast, but it will be very interesting to see what 2019 has in store for social media platforms with regards to security, privacy and transparency.

The industry event calendar was just as hectic this year: April saw more than 40,000 visitors flock to San Francisco's Moscone Centre for RSA Conference,

1: There weren't many 'likes' for Facebook's privacy policies this year

2: Dr Black has made such a difference to so many people in tech over the last 20+ years

Infosecurity Europe had its biggest and busiest show to date in June and Black Hat USA was its usual, sparkling self under the hot Vegas sunshine. *Infosecurity* had a presence at them all. Bringing you all the latest news and content from events such as these is one of the things we are most passionate about – it really never gets old!

I also can't miss the opportunity to mention our brand new Online Summit which, after several months of work and preparation, went superbly on September 11 & 12. It was a fantastic two days of quality content and conversation, and huge credit should go to the whole *Infosecurity* team for putting that event together so well. You attended in your droves and your feedback was amazing, but if you weren't able to make it on either of the days (or if you just want to take it all in again) you can still watch all of the sessions on-demand via our website.

Finally, and on a personal note, I have to say that, almost three years after first starting my adventure as an information security journalist with very little knowledge of this sector, I have always experienced nothing but warmth, welcome and freely-given advice from countless talented and knowledgeable people in this industry. Without that help and guidance, I simply would not be where I am today. The latest industry rock star I was lucky enough to meet was the incredible Dr Sue Black. You can read all about her amazing story on page 18.

So, I sincerely hope you've enjoyed our content, both digital and in print, over the last year. We've got some fantastic new ideas in the pipeline and I can't wait to bring them to you next year, but until then, enjoy the issue, have a wonderful end to 2018 and we'll see you all in 2019!

Michael Hill,
Acting Editor

MAGECART ATTACKS: THE CARD SKIMMING EPIDEMIC

Kacy Zurkus looks at the common tactics contributing to recent Magecart attack success and explores how to defend against them

The hacker groups using Magecart attacks have been indiscriminate in their widespread offensive strategies, successfully victimizing organizations from British Airways to Ticketmaster, Feedify and Newegg with skimming attacks.

Earlier this year, RiskIQ identified bad actors attacking the supply chains of e-commerce sites around the globe. Going after the supply chain was not only efficient but quite effective for the threat actors, enabling them to successfully access thousands of victims at a time.

One of the hacking groups was also responsible for inserting malicious JavaScript into the code of Shopper Approved, a customer rating plugin. In the British Airways attack, the attackers veered from the previous pattern of infecting a third-party software provider and instead targeted the carrier itself.

Again, attackers successfully compromised Newegg in a stealthy attack in which they were able to avoid detection by registering – and then certifying with Comodo – a domain similar to the primary newegg.com domain on which a back-end server storing skimmed card information was hosted.

Having tracked the activity of malicious actors using Magecart attacks for a few years now, RiskIQ has surmized that the attackers appear not to be a singular group, but a collection of several different groups.

Diverse Groups, Targeted Attacks

As diverse as the hacking groups are, they are all highly targeted in their attacks. A stylistic element that links the various groups together, despite the multiple methods of operation (MO) used by different actors, is that they are all quite consistent in grabbing content from payment pages, according to Yonathan Klijnsma, head researcher at RiskIQ.

"The way they do this varies from group to group. Some groups grab any form [of information], others explicitly look for payment information and validate this first," says Klijnsma. This key MO is potentially one reason why Magecart attacks remain successful.

The skimming attacks start with a very generic step: breaching the organization they targeted. Whether it's by using default credentials or credentials from public and non-public data breaches, attackers gain access relatively easily. Some might exploit outdated server software, while others exploit outdated CMS installations like older installs of Magento.

"Once inside they will, depending on what the payment process is, inject themselves on the right pages or simply inject their skimmer code on any page. Many skimmer implementations manually check if a visitor is on the checkout page and if payment information is available," Klijnsma explains.

Another reason why Magecart attacks are so successful is that attackers are often easily able to identify a vulnerability in web applications, which are, unfortunately, rife given how little attention web app developers give to security and privacy, argues Chris Olson, CEO of The Media Trust. Even when developers make updates and patches available, website operators often delay, if not forego them altogether. Too often operators fail to scan their sites in real time, making a bad situation even worse given that bad actors often modify their tactics, as has been the case in many of the Magecart attacks.

"Relying on scanning experts with the most extensive malware data is key because attacks are often modified in order to escape detection by weak scanners," Olson says. "Modification tactics range from obfuscating code, which enables malware to elude conventional anti-malware tools, to arresting an attack when the presence of a known expert's technology is detected.

"Having this scanning done by experts would enable them to closely monitor all the known and unknown third parties that execute code in their digital

ecosystem, and identify any unauthorized activities that heighten the risk of a data breach and regulatory infringement."

Continued Success

In analyzing the myriad attacks, a few fundamental issues have come to light, revealing factors that contribute to the continued success of the Magecart attacks. One factor is that companies, industries and standards continue to ignore the significant risks that third-party code suppliers pose, according to Olson.

"Security and risk professionals would rather perform checks on whether they've been hit than take the more proactive approach of preventing these attacks from happening again. The only way to do this is to continuously scan their sites and mobile apps in order to identify any unauthorized code and, when needed, terminate them."

What poses another problem is that website owners only know a fraction of all the third-party code that executes within their ecosystem but outside the purview of their IT security team. "They have no incentive to know these direct and indirect third parties because the information security standards around applications and the handling of credit card payments fail to recognize the risks third parties pose. PCI, NIST and ISO standards, for instance, do not require knowing third-party code," Olson says.

Moreover, most organizations lack visibility into their internet-facing attack surface, leaving them unable to determine whether they've been breached. According to Klijnsma: "Many organizations simply lack visibility into the client-side of their sites, so they're unaware of their vulnerabilities and if they've been breached. It's a fertile ground for Magecart attacks in the e-commerce space, especially amongst the huge number of small and mid-sized online stores."

Preventing the Attacks

The good news is that attacks can potentially be prevented through good security practices, but also by performing additional integrity checking. One option, Klijnsma explains, is to monitor your server for any kind of file modifications. One approach RiskIQ takes here is that it monitors all resources, be it locally hosted or remote, and whenever there is a change it notifies customers about this change, which can then be marked as benign or not.

"For consumers, get your bank to issue new cards but also look into setting up additional verification steps on your payment account," Klijnsma advises. "Keep in mind that banks don't always have those added steps enabled by default, but you can add a second step to your payment process where you have to provide additional proof for the payment. When using additional verification steps, even when your card is skimmed, payments cannot go through as the attackers cannot perform the second step of verifications in two-factor authorization (2FA) such as one-time passwords (OTP)."

When security practices and the standards that govern them fail to account for internal vulnerabilities introduced by third parties, bad actors are able to bypass security measures through trusted connections, which is why Olson says companies should take a proactive approach to digital security by knowing all their direct and indirect third-party code suppliers and monitoring all their activities by continuously scanning digital assets in real time.

"They should work with all their third parties on terminating code that violates their digital policies. Also, they should test their web apps to ensure they are not vulnerable to attacks involving cross-site scripting or SQL injections.

"Developers should restrict user input by restricting text to a certain number and range of characters. They should write code that checks to ensure that data without the proper format is never inserted directly into the HTML content that comprises the web application," Olson concludes END

infosecurity®
GROUP
EUROPE • NORTH AMERICA • GLOBAL MAGAZINE

infosecurity®
EUROPE
04-06 JUNE 2019 OLYMPIA LONDON

infosecurity®
NORTH AMERICA
14-15 NOVEMBER 2018 NEW YORK USA

info security
STRATEGY | INSIGHT | TECHNOLOGY

THANK YOU TO OUR GOLD PARTNERS who partner with Infosecurity Europe, Infosecurity North America and Infosecurity Magazine

algosec
APRICORN
BLACKDUCK by SYNOPSYS
egress
ipswitch
LastPass
ManageEngine
mimecast
SailPoint
STORMSHIELD
TITANIA
tripwire
WhiteSource

Q&A

JENNY RADCLIFFE

Jenny Radcliffe – aka 'The People Hacker' – is a force to be reckoned with. She can diffuse a crisis situation, talk her way into a secure building and spot a psychopath at a hundred paces. She has been called a mind reader, a 'human lie detector' and likened to a Jedi Knight. In reality, she's an expert in social engineering, using her skills to help clients protect themselves from malicious social engineering attacks

By Michael Hill

What was your route into social engineering and pen testing?

I'd always been interested in wandering around places and looking at what happens in buildings after-hours, behind the scenes or once they became empty. I started to look around such places as a child, as many of us do, and I never really stopped. By the time I was getting paid to test security systems in what we now refer to as penetration tests or social engineering, I'd already spent most of my life doing it!

Who do you admire most in the industry?

I admire people who have done the work and have the experience in the industry so that when they stand up to talk to people they really are an authority on what they say. I admire those who quietly help people in different ways without using it as a vehicle for their own ego and profit, and also those who are only just starting out but are willing to put in the work in order to get really good at what they do. They'll be protecting us all in the future.

What's the most interesting thing about social engineering threats?

That nothing changes! Scams and cons evolve and technology has enabled social engineering to be much quicker, broader and more dangerous than before, but ultimately people are still fooled by the same few psychological tools they always were. Understand the tools and you are less likely to be conned by a social engineer: it's simple to say but incredibly difficult to remember for a target, especially in the midst of the con.

Tell our readers an interesting fact about yourself

My first pet was a dog called Gripper, which was a joke because he was so fluffy. My mother's maiden name was Dublin, so we were known as the 'Irish family', but we aren't even Irish and I have no idea where the name originated from!

If you could change one thing about the infosec industry, what would it be?

Plagiarism, snake oil merchants and false prophets plague an otherwise incredible industry. If I could change only one aspect of infosec it would be to get rid of those things. Truth and integrity are integral to security and it matters here more than most industries; that we all have the highest standards, not just for the people we are trying to help but to raise our expectations of what is possible both for the industry and for ourselves.

BIO

@Jenny_Radcliffe

Jenny Radcliffe is a speaker, consultant and trainer in the skills of people hacking. She advises businesses on how social engineering can be both a huge threat and a valuable tool to organizations of all sizes.

YOU'VE GOT M@IL: THE RISE OF BUSINESS EMAIL COMPROMISE

Danny Bradbury assesses how BEC attacks have become a top social engineering threat to organizations of all sizes

Sophisticated zero-day attacks may be a cyber-criminal's first weapon of choice in the movies, but in real life, an email or a phone call can often be enough to get the information you need. Social engineering, the art of manipulating people to achieve your goals, has long been a mainstay in the hacker's arsenal. Now, cyber-criminals are applying the concept to surgically extract money from companies as part of a technique called business email compromise (BEC).

In a BEC attack, a criminal sends an email impersonating a senior company executive. The mail, sent to someone with access to a company's financial accounts, demands that they solve an urgent business problem by sending a third party payment. When the panicked employee sends the payment, supposedly to a supplier or service company, it actually goes straight into the attacker's account.

"One of the primary reasons BEC attacks have become such a growing problem is because the skill level needed to execute them is low and the return for successful attacks is significant," says Crane Hassold, senior director of threat research at Agari, which sells AI-based email protection solutions.

Just how successful are these attacks? The FBI counted global losses exceeding $12.5bn between October 2013 and May 2018, from nearly 80,000 reported cases worldwide.

Why Now?

BECs may have grown over the last few years, but the first email was sent in 1971 and most people were using emails to do business by the early 2000s. So why has it become a phenomenon now?

"Social media has played a big part," says Dr Jessica Barker, co-founder of UK security consulting firm Cygenta. Sites like LinkedIn, Twitter and Facebook have enabled attackers to research their targets and understand their relationships and the way that they communicate, she adds.

The rise in cryptocurrency has also made money laundering and fast international transfer far easier, according to Justin Forbes, penetration testing lead in the CERT division of Carnegie Mellon University's Software Engineering Institute. "Wire transfer is still what I'm seeing as the primary vector to get money out," he says. "Cryptocurrency has enabled the ability to move things a lot faster afterwards."

There are several levels of BEC attack. The least sophisticated is a simple email impersonation attack, in which criminals send emails impersonating a C-suite executive from the wrong address. In many cases, these addresses can use a common consumer domain such as Gmail, but they can be highly effective, because the attacker can pretend that they are an executive sending from a personal email address, says Lance Spitzner, director of the Securing the Human awareness training operation at SANS.

> ***"One of the primary reasons BEC attacks have become such a growing problem is because the skill level needed to execute them is low and the return for successful attacks is significant"***

"There's a tremendous sense of urgency, and the bad guys are trying to pressure or intimidate you, and rush you into making some kind of mistake," he says.

"They will usually keep the email message short and to the point, to avoid making any mistakes and to heighten the sense that the executive is rushed for time," he adds. If someone queries the request, "the person will email back and say 'I'm sorry, but I'm getting on the train – you have to process this right now.'"

Hot States & Impulsive Acts

Using psychological tricks to manipulate someone's behavior is a key technique in social engineering. Barker draws on a behavioral economics theory when describing two sides to the brain; the cognitive side that thinks things through carefully before acting, and the impulsive side which is driven by feelings and mood. The social engineer uses a series of techniques to trigger that latter behavioral mechanism.

"If you flatter someone, if you tempt someone, if you make someone curious or angry, if someone is tired or stressed, they're more likely to be in that hot state where they act rather than think," she explains.

The likelihood of a successful attack increases when combining that hot state with a convincing story. Forbes identifies a more sophisticated attack which compromises the victim's business email account.

Attackers often use credential stuffing techniques here, trawling publicly available dumps of compromised emails and passwords. When they find a match with a business email address, they will try logging into the executive's email account using the dumped password. If the executive reused their passwords, they may score a hit. "Then they'll compromise that user's email account and send a request to transfer money to a bank account that they control," he says. As the request arrives from the executive's legitimate email address, it won't trigger any phishing alerts.

Then, there are malware infections that also happen to include a BEC attack as part of their payload. These infections, delivered via conventional methods such as

spear phishing and infected attachments, can launch a range of attacks including remote access tools and keyboard loggers. Forbes has also seen them include a particularly sneaky attack that uses malware to set automatic rules in a victim's email account.

"If they know they're commonly sending a specific routing number and bank ID, they'll set a rule to auto-replace that," he says. When the user enters the details of a legitimate payment transfer, it will switch them to the attacker's account details, effectively rerouting payments at the source.

The Power of Voice

Not all attacks start with email: Barker points to voice phishing (vishing) as a case in point. She explains this attack, which predates email, uses voice persuasion and can be especially powerful in building relationships to manipulate victims.

"Especially in the last year we've seen a growth in voice phishing attacks to warm up a target to then launch a BEC," she explains. The attacker will call posing as a supplier explaining that an urgent payment hasn't gone through, and ask if they can send the payment request via email for a quick resolution.

"That's very clever because the target feels like they've spoken to the real person and they've built up a rapport," she says. "They've been asked to do this favor, so when the email comes in they won't look at it as carefully and they'll maybe bypass whatever processes they're meant to go through."

What kinds of companies fall victim to these attacks? Barker notices a lot of clients in the financial sector, and news articles bear this out. In a 2013 attack, hedge fund Fortelus Capital Management lost £740,000 to voice phishers who didn't use email at all. Instead, they called an employee on a Friday afternoon pretending to be security staff from Coutts, the company's bank. They warned of a security compromise and asked the employee to use the two-factor authentication hardware that Coutts had given him to generate codes that would let them access the company's account. When he obliged, they quickly transferred the money, and he lost his job.

> ***"There's a tremendous sense of urgency, and the bad guys are trying to pressure or intimidate you, and rush you into making some kind of mistake"***

SANS' Spitzner says that another increasing target are real estate customers. Criminals will compromise a realtor's email and use it to tell house buyers to transfer funds to a fraudulent account.

"Real estate transactions are the perfect place to do electronic transaction fraud because people are prepared to transfer very large sums of money. Real estate transactions are complicated, you only do it once or twice in your life. It's the perfect time to interject yourself in that communication," he says.

The most difficult part of the whole process for criminals may be handling the money once it leaves a company. "Most of the costs of running money laundering goes on mules: the people who are setting up accounts, going to ATMs and removing money," says Barker's partner, a longtime ethical hacker who only goes by the name 'FC'. The attackers would set up a bank account under a fake or stolen ID, and then route the money to that. Often, the accounts will be international, which makes it harder for authorities in the victim's country to enforce the law.

Layered Protection

Protecting a company against social engineering and BEC attacks involves a range of complementary measures. The obvious answer is training, but not all education is the same, warns Barker. Forget dull courses that replicate a classroom setting, she says: "you want training that shows that this is a real problem, ideally with a demonstration of the attack that is engaging, interesting and relevant to the people in the room."

Companies can layer different technology measures atop each other to increase their protection. Domain-based Message Authentication, Reporting and Conformance (DMARC), DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF) are all protocols that can help to prevent spoof emails from coming in, and should be combined with mandatory two-factor authentication to thwart account compromise, warns Forbes.

He also advises using rules in corporate email systems to label emails according to origin. "If every email you got was green when it came from inside the organization and pink when it came from outside, it would be easier for a user to see at a glance whether this was a phishing email or not," he says.

The other winning strategy is process change. Companies should make staff follow processes that prevent fraud, say experts. "A potential victim can reach out to the supposed sender of an email to confirm that they were not the one who sent it," says Agari's Hassold.

Spitzner adds: "If you're doing financial transactions you also need a two-person rule where two people must verify that a transaction goes through." Following this strictly can eliminate a single point of weakness among employees.

These process changes are important, but they must be supported by a shift in organizational culture, points out Cygenta's FC. If management imposes extra steps in a process and then doesn't give staff the time and resources to follow them, then employees will cut corners. That's why a simple-sounding set of fixes often needs a deeper management focus to implement well.

For those companies that don't invest in those changes? Beware the unexpected email or phone call – it could be your downfall END

Q&A

CHESTER WISNIEWSKI

Chet Wisniewski has been in the security space since the late 1980s and, as principal research scientist for Sophos, spends his days figuring out how to compromise systems in order to protect them. As a well-known public speaker, Chester has mastered the art of conveying cybersecurity to audiences all over the world. Away from his day job, he has a passion for food and cooking

By Michael Hill

How did you get into the information security industry?

I started out hacking my way into/onto the internet/ARPANet in the 1980s. This enabled me to learn a lot about how our communications networks evolved from dial-up modems and x.25 to our modern LAN and broadband technologies. In the late 1990s, there was finally enough demand for good guys in network security for me to move into a full-time security role. I have no formal education, so my entry to the profession was mostly due to amazing mentors who recognized my knowledge and potential and helped me get paid work to prove it.

What's your proudest achievement?

Being involved in the information security community in ways that I can give back. I have long been involved in the local security community in Vancouver and this has provided me many opportunities to be a mentor. I also speak at a lot of regional Security BSides events around the world giving me the chance to share my experience with people all over the globe.

What's your passion outside of infosecurity?

I'm a bit of a foodie. I travel frequently which provides a fantastic opportunity to experience food from almost every culture. I love to cook and bake when I have a few days at home and my passion is for quality and authenticity. I grow many of my own herbs and vegetables and cultivate my own yeast for baking.

What's the worst thing about your job?

It is a toss-up between spending 40 hours a month on an airplane and having to repeat the same basic security advice after a seemingly unending stream of data breaches. Computer security is a complicated and immature subject and sadly that leads to a lot of bad advice being propagated and confusion that leads to inaction.

What's the most interesting thing about information security?

Our role is to figure out how to use things in ways they were never intended to be used. We are almost the opposite of IT at most organizations. IT tries to figure out the quickest and easiest way to build something that will solve some business need or pain. Infosec professionals have to determine all the ways that a system might be abused and find the most effective way to limit that risk. It's like having a real life job as MacGyver!

BIO @chetwisniewski

Chester Wisniewski is a principal research scientist in the Office of the CTO at Sophos. He divides his time between research, public speaking, writing and communicating the complexities of security to the press and public in a way they can understand.

Michael Hill meets the woman whose dedication to making a difference to the lives of others has made her one of the most well-known names in the tech industry

DR SUE BLACK

When you think of the name Dr Sue Black, there are several things that could spring to mind. She's a technology evangelist with an OBE, an author, a digital skills expert, a revered academic and honorary professor, a UK government advisor, public speaker and a campaigner for women in tech. She's also appeared on Desert Island Discs and played an instrumental part in a campaign to save Bletchley Park from closure.

Her list of accolades is seriously impressive and she's pretty much done it all. However, my first impression of Sue as I sit down with her for a coffee in one of her favorite local cafes is that she's warm, welcoming and incredibly down to earth – not to mention that she's rocking some truly awesome bright red hair!

Dr Black's story is an amazing one; I would need a lot more than just the next few pages to even try to do it justice, but indulge me if you will as I recount the tale of a woman who has made a huge difference to the lives of so many over the last 20+ years.

By her own admission, an interest in computing did not come to Sue at an early age: "I'm 56 now and I guess that, in the 60s and early 70s, nobody my age really knew much about computing," she says. "We didn't have computers at school, so that opportunity didn't really come up."

It wasn't until a couple of years after Sue had left school – which she did at the age of 16 – and was in the world of work at an accounting firm that she had her first real introduction to computers. "I used a computer for data entry and I remember being quite excited about what they had the potential to do, but I wasn't the person doing it at that time."

However, Sue did have a brother who was into tech and writing his own programs. With a smile, she tells me that it was during a visit to a computing exhibition with her brother in the early 1980s where she saw him writing code that she first had the thought: "I'd quite like to do that." After all, she had always loved mathematics and problem-solving, so the idea of getting into computing seemed like an enticing prospect.

The realities of life proved difficult though and by the age of 25, Sue found herself a single mother with three young children and out of work, living in a women's refuge for six months before moving into council accommodation in Brixton, London.

"We were starting our lives again I guess," she says. "I reached a point where I wanted to support my kids; we had come out of refuge and were living on benefits. I thought about going back to work, but I realized I didn't have many qualifications. Trying to go back to work with the qualifications I had would have only left me on minimum wage, or just above, and even if I worked long hours I wouldn't have earnt enough to support the kids."

Sue's thoughts then turned back to what she always wanted to do, which was to get an education she could use.

Going Back to School

Sue went along to her local college in Southwark and signed up for an evening mathematics course, which met twice a week and required 20 hours of private study, meaning she could still be around to get her children to and from school.

"Me and my friend there actually came top of the class, which gave me a lot of confidence that I could actually go back into education, so I applied to do computing at various universities and I was accepted by Southbank University, which was the closest one to me."

With an enthusiasm to learn about evolving technology and a determination to excel, Sue spent the next four years of her computing degree developing a solid understanding of the various facets of computer science and using tech to solve real world problems, before the offer of a PhD in software engineering came along during her final year project.

"I told my supervisor I'd love to do a PhD – but what I didn't tell him was that I didn't know what a PhD was!" she laughs. After a quick stop by the library to look it up, Sue was delighted to learn that a PhD would allow her to carry out her own research, and would also give her the opportunity to teach mathematics alongside it.

"We were encouraged to teach and it was a great opportunity for me to earn some extra money," she says, "although it did take away from research time which made it harder as I was one of the ones that had to go home and pick up the kids and stuff, but in the long run it worked out for the best."

It certainly did, as Sue would soon become a full-time lecturer at Southbank University, something she did whilst also continuing her PhD research. It was that research that led her to attend tech conferences and set the wheels in motion for the creation of the first online network for women in technology, the hugely successful BCSWomen.

Creating BCSWomen

"As part of my PhD research I was encouraged to go to conferences and network," Sue says. "At that time, even though I was in my thirties, I was really shy and hated going up to talk to people I didn't know – at the time it was the worst thing you could have asked me to do!"

It wasn't until Sue attended a women in science conference in Brussels in 1998 that, finding herself among a majority of women, she discovered why she had

struggled to network at (male dominated) conferences in the past. "That conference changed my life," she says. "It helped me realize that it wasn't that I was useless at talking to people, it's that when you're in a majority, things feel so much easier."

Sue came away from that event with a fresh approach to networking, and more notably, with an idea: to set up a network for women in computing. "There weren't any UK conferences for women in tech then, so I wanted to create an online network for women so that we could chat to each other about technology. That's what I set up when I got back from that conference in Brussels, and it's still going 20 years later."

Sue tells me that, after the excitement of the network's launch, her and a few hundred women on an email list began brainstorming ideas for what they wanted BCSWomen to achieve. "One of the suggestions was free training in how to set up a website," Sue says, which she was able to secure funding for and organize. "That went really well, we got quite a lot of publicity from that and then a lot more people wanted to join the group – it went from strength to strength from there." Today, BCSWomen has 1400 members.

Saving Bletchley Park

A few years passed with Sue continuing to teach and completing her PhD research, along with developing BCSWomen. As chair of the network, she was invited to attend an annual meetup at Bletchley Park, the site where Alan Turing and his team of code breakers famously cracked German coded messages during World War II.

Of all the things I was itching to ask Sue about, her involvement with Bletchley Park was top of my list. I have always found the story of how the incredible events that took place there in the 1940s not only changed the course of the war, but also inspired future generations in the field of computing, absolutely fascinating. After listening to Sue tell me how she led a campaign that helped save Bletchley Park from possible closure, I am even more enthralled.

> ***"I love the fact that I can tell my story and empower other people to get out there and do things for themselves; to change their life to be the way they want it to be"***

"I got to Bletchley Park, had the meeting, and wanted to have a look around afterwards," she tells me, and she found herself talking to a couple of men who were half way through the rebuild of one of Turing's codebreaking machines. During that conversation, Sue discovered that more than half of the 10,000 people that worked at Bletchley Park were women, something that came as a great surprise to her. "I had no clue about that," she says, and she couldn't find anything about it online either. "I was completely blown away that more than 5000 women had worked at Bletchley Park and I didn't know anything about it."

Sue left Bletchley Park with her next challenge in her sights: to raise the profile of the women that worked there. "I really wanted to capture their stories for posterity, because it was part of the story that was completely missing. I eventually managed to raise some funding to record the oral histories of some of the women that worked at Bletchley Park."

Dr Black has learned to love public speaking, which she now does regularly at events all over the country

At the launch of that project in 2007, Sue gave a talk about why telling the story of the women was so important, before learning from the director of Bletchley Park that he feared the center, in disrepair and in need of substantial renovation, was facing closure due to a lack of money and a drop in visitor numbers. "If they closed, they would never be able to open again, he said," Sue adds.

With a determination to preserve the site's history Sue, once again, set to work. In her role as head of computer science at the University of Westminster, she was well-connected, and she contacted her fellow heads of computing across the country urging them to sign a petition to keep Bletchley Park open. To her delight, some of the most well-known computing professors in the UK pledged their support, as did a handful of journalists who helped Sue to get her voice heard on national television.

"That was the start of the campaign," she explains, "but once I'd done that I didn't know what to do next – I was an academic, I didn't know how to run a campaign."

A eureka moment came in 2008 though, and it was in the form of Twitter. "I realized I could use Twitter to find everyone who was already interested in Bletchley Park and tweeting about it. Quite quickly I realized that was the way to reach the people I wanted to reach, the people who cared about Bletchley Park."

Remarkably, Sue tells me how one of those people was none other than actor, writer and activist Stephen Fry.

"I was on Twitter one evening, saw that Stephen Fry had tweeted a selfie of himself stuck in a lift in London, and I thought 'Stephen Fry you must be interested in Bletchley Park!'" she says.

He certainly was, and what's more, he was already following Sue on Twitter. "I sent him several private messages that night, asking him to get involved in the campaign and I sent him a link to my blog. The next morning he tweeted asking people to read my blog and to sign the petition – that day I ended up being the most retweeted person in the world."

Sue's campaign was instrumental in not only raising awareness about Bletchley Park, but also in securing its future and transforming it into the world-class heritage and education center it is today. No wonder she wrote it all down in her best-selling book, *Saving Bletchley Park*.

Public Speaking, #techmums & a New Book

Sue's time in full-time teaching came to an end in 2012, when staffing cuts at the University of Westminster led to redundancy.

"The university decided that computing didn't have much of a future," she explains. "They were cutting staff by 50%, so I decided it wasn't a great time to be head of computing and decided to leave."

She didn't sever all ties with academia though, accepting the offer to become honorary research associate at University College London, before becoming an honorary professor there too.

So, with some more time on her hands, what's been keeping her busy since then? Well, aside from receiving an OBE for services to technology in 2016 and acting as an advisor to the UK government, Sue has spent the last few years making a name for herself as a public speaker, setting up #techmums and working on a new book on coding.

"Almost every week there's one or two talks in different places with different types of audiences," she says. I ask her if public speaking is something she enjoys. "I do now – I didn't to start with," she says honestly. "I love the fact that I can tell my story and empower other people to get out there and do things for themselves; to change their life to be the way they want it to be. Yes, there's the whole positive technology story, but there's also the fact that you can overcome any hurdles in life."

Sue's current social enterprise #techmums teaches mothers tech skills to encourage them into education, entrepreneurship and employment. "I started running workshops for seven-year-olds, teaching them coding and app design, because at the time there was no coding in schools," Sue explains. "They went really well, everyone loved it, but when we got the parents in at the end of the workshops and encouraged them to have a go too, I noticed in general the dads would step in and have a go and the mums would be quite hesitant."

That sparked yet another idea for Sue: "If I want to try to change the way everyone sees technology to being a more positive thing, maybe I should start with mums," she says. "I found some research which showed that the main positive influencing factors on kids doing well in literacy and numeracy at age 11 are their mother's education and their home environment."

The #techmums program was therefore launched with a sole focus on giving mothers the confidence and knowhow to use technology to enrich both their personal and professional lives. "The whole idea is not to learn absolutely everything in detail, but just to feel more comfortable and have some knowledge to feel you can get out there and do stuff in technology rather than being scared of it."

It's certainly been a whirlwind of a career, and so has my interview with Sue – the time has flown by. There's just a few minutes left to ask my last two questions: what's your proudest achievement and what's the next challenge?

"I'm most proud of my kids," she says glowingly. "I have four children, and I brought them up mainly on my own, but they supported me through thick and thin. I'm just really proud of how they've all turned out, and now I've got three grandchildren too, it's just amazing."

As for what's next, Sue hopes that she can continue to empower women all around the world, and take #techmums to one million users by 2020. "I'm just really keen to change people's lives, particularly people who haven't had the best chances in life, and help them to empower themselves by teaching them tech skills so they can create a better life for themselves and their kids."

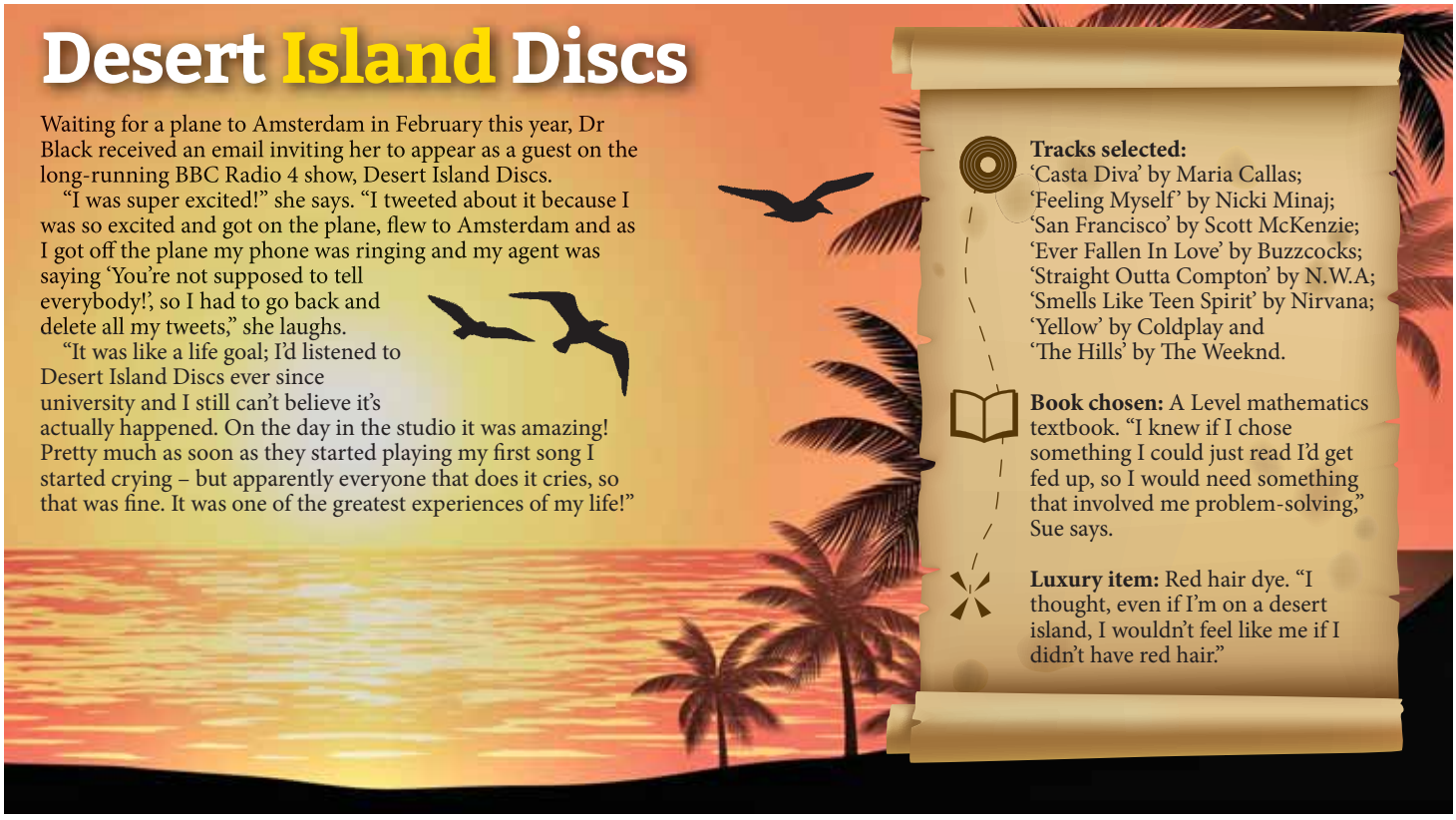
If there's one thing I've learned about you Sue, it's that when you set yourself a goal, you not only achieve it, but you go well beyond it. It's been a pleasure to hear your story! END

Desert Island Discs

Waiting for a plane to Amsterdam in February this year, Dr Black received an email inviting her to appear as a guest on the long-running BBC Radio 4 show, Desert Island Discs.

"I was super excited!" she says. "I tweeted about it because I was so excited and got on the plane, flew to Amsterdam and as I got off the plane my phone was ringing and my agent was saying 'You're not supposed to tell everybody!', so I had to go back and delete all my tweets," she laughs.

"It was like a life goal; I'd listened to Desert Island Discs ever since university and I still can't believe it's actually happened. On the day in the studio it was amazing! Pretty much as soon as they started playing my first song I started crying – but apparently everyone that does it cries, so that was fine. It was one of the greatest experiences of my life!"



Tracks selected:
'Casta Diva' by Maria Callas;
'Feeling Myself' by Nicki Minaj;
'San Francisco' by Scott McKenzie;
'Ever Fallen In Love' by Buzzcocks;
'Straight Outta Compton' by N.W.A;
'Smells Like Teen Spirit' by Nirvana;
'Yellow' by Coldplay and
'The Hills' by The Weeknd.

Book chosen: A Level mathematics textbook. "I knew if I chose something I could just read I'd get fed up, so I would need something that involved me problem-solving," Sue says.

Luxury item: Red hair dye. "I thought, even if I'm on a desert island, I wouldn't feel like me if I didn't have red hair."

THE DARK SIDE OF AUTOMATION

With autonomous technology evolving quickly, *Rene Millman* explores whether machine learning has a dark side and asks what can happen when bots go bad

The concepts of machine learning and artificial intelligence (AI) have grown to become almost synonymous with information security and the protection of data – with more and more enterprises turning to automation and 'cognitive computing' to improve the proficiency of their security efforts. Such tech provides quicker response times, better threat detection, the ability to process and analyze large amounts of data and can free up vital staff time.

However, where there is light there is also dark. Cyber-criminals are constantly looking for the next best, and quickest, way to carry out attacks to the highest impact. According to recent research from ESET, the threat of AI being used as a weapon against organizations has led to a significant amount of IT decision makers (75%) in the US to believe that the number of attacks they have to detect and respond to will increase.

While this fear is lessened among their European counterparts, with 57% in the UK and 55% in Germany concerned about AI-attacks, the worry still exists. What's more, 71% of IT decision makers surveyed believed AI will make attacks more complex.

Where Hackers Use AI

According to Corey Nachreiner, CTO at WatchGuard Technologies, as machine learning and AI is still less than a decade old in security, more often he sees good researchers showing the potential risks in how attackers might misuse machine learning/AI, than he does attackers actually exploiting it in the real world.

"It is not unusual for the good guys to notice potential risks before the bad guys start using them and we probably have to wait a year or two before attackers really start leveraging machine learning for attacks," he says.

"On the other hand, the malicious use of machine learning/AI might not always be immediately apparent. For instance, if an attacker used machine learning to improve the efficacy of phishing emails, all the real world would see is a well-crafted email. It would be hard to know if that change was a result of applying machine learning algorithms to perfect phishing."

He adds that there is at least one company, Darktrace, which claims to have detected attackers using machine learning to learn a victim's network behavior, although he admits he hasn't seen the evidence to support that himself.

Likely Attack Vectors & Greater Sophistication

Attackers are already using automation, so by adding some 'intelligence' to that automation, they get more powerful and become more effective, according to Cesar Cerrudo, CTO of IOActive, a cybersecurity consultancy.

"Currently many attacks are just blind and hitting everything until they hit something vulnerable, with a bit more intelligence attackers can increase attack effectiveness and success rate," he says. "For instance, instead of trying to blindly attack a Linux system with a Windows exploit, which of course won't work, attackers could know exactly what systems they are attacking, what system version, language, time zone etc. and also when they should attack and how they should do it."

He adds that this means they can craft specific, targeted attacks and scale all of this in an easy way. "For example, by having enough data on targeted systems you can profile a company on how long it takes them to patch systems and how often they do it so when there is a new vulnerability they will know what companies could remain vulnerable and for how long, prioritizing what systems to target first."

According to Elliot Rose, head of cybersecurity at PA Consulting, AI systems suffer from several unresolved vulnerabilities which criminals can exploit to create new opportunities for attacks.

"Machine learning algorithms like those in self-driving cars create an opportunity to cause crashes by presenting the cars with misinformation. Military systems could also be misled in a way that could lead to a friendly fire incident," he says.

He adds that AI systems are susceptible to attacks in a number of ways. "Data poisoning introduces training data that causes a machine learning system to make mistakes," says Rose. "Adversarial attacks provide inputs designed to be misclassified by machine learning systems such as teaching an autonomous vehicle to misclassify a stop sign. Attackers can also exploit flaws in the design of autonomous systems' goals."

Rose warns that AI-enabled impersonation is a new threat to systems that can mimic individual voices. "Significant progress in developing speech syntheses that learn to imitate individuals' voices opens up new methods of spreading disinformation and impersonating others," he explains.

Spear Phishing

Just as AI speeds up legitimate activity, it creates opportunities for criminals to increase the effectiveness of their attacks. According to Rose, spear phishing attacks which use personalized messages to extract sensitive information or money from individuals require a significant amount of effort and expertise.

"AI could automate the identification of suitable targets, research their social and professional networks, and then generate messages in the right language. This could enable the mass production of these attacks. AI could also be used to increase the speed of attackers in identifying code vulnerabilities and trends," he says.

Nachreiner adds that two years ago a team gave a talk on 'Weaponizing Data Science for Social Engineering' showing how they used a neural network to create an automated Twitter phishing bot.

"We are not seeing this in real attacks yet, but it is coming. Also, you may not know whether an improvement to an attacker's malware or emails is due to their individual improvement or machine learning solutions," he warns.

> ***"If an attacker used machine learning to improve the efficacy of phishing emails, all the real world would see is a well-crafted email"***

> *"AI could automate the identification of suitable targets, research their social and professional networks, and then generate messages in the right language"*

Tampering with AI Systems

Not only are hackers using AI to attack organizations, they are targeting organizations' own AI and machine learning systems and infrastructure.

Nick Dunn, managing security consultant at global information assurance firm NCC Group, says that although the attack surface consists of the same components as traditional systems, including hardware, data collection pipelines, local storage and cloud storage, organizations are seeing a rise in the number of bespoke attacks being launched against them that involve the compromise of the learning data and learning process.

"The level of interaction in machine learning systems between these components and back-end data is becoming an increasingly viable route for hackers to exploit, especially when voice recognition and fraud detection features play a part in the system," he says.

He adds that the attacks are usually carried out through manipulation of data inputs to systems during either the training stage or the operation phase.

"Whether these are intended to modify or harvest data, there's no doubt that attackers are looking to cause significant damage," says Dunn.

It's also important to be aware of issues arising from the opacity of systems and any legal issues associated with this, according to Dunn. The complex nature of algorithms can create situations where it is not immediately clear that a system is giving an incorrect output, while legally-enforced removal of training data can result in the system no longer functioning correctly or becoming redundant, he says.

Dunn argues that securing machine learning software during the Software Development Life Cycle (SDLC) forms a significant foundation in terms of mitigating threats facing software. Key IT stakeholders across a business need to be aware of threats and the ways in which these can be mitigated from the get-go. "Resilience is also an important consideration, as systems may need to be restored or modified following the removal or correction of training data."

Defending Against AI Attacks

Cerrudo says that organizations need to keep defending as usual but focus on becoming faster and more proactive since, with new technologies, attackers get faster and better. "For instance, they could instantly know when a system becomes vulnerable and attack it. So as an organization you will have less time to apply patches to get your systems secure," he says.

Far from using AI to beat the hackers using AI themselves, Rose says that humans will still be needed to keep systems secure.

"The big technology companies have started recruiting aggressively for experts in the past six months. We need security algorithms to be less of a black box so we can spot deviations in how they work. We also need humans as a check when processing sensitive or personal data, such as data on sexual orientation, health or children," he says.

Governments will also need to step up and play a role in protecting infrastructures from AI-based attacks. "We know that many of the tools used in cyber-attacks come from countries such as Russia and they will be using AI to improve these. The UK needs to think how it can use AI to better defend against such attacks by spotting trends early and providing solutions and guidance," says Rose.

Future AI-Based Attacks

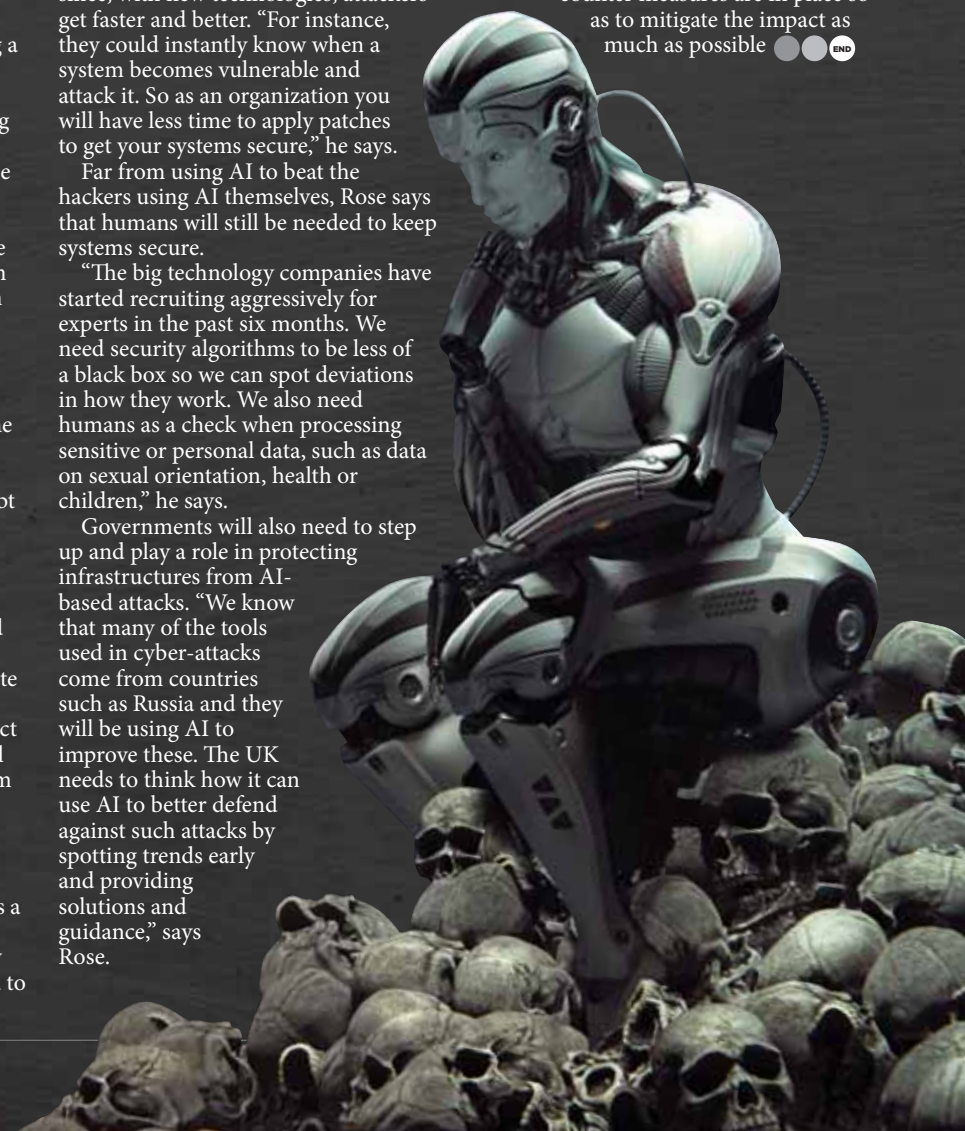
Hackers aren't investing that much in the R&D of AI and machine learning since they tend to do the least effort to get the maximum profit, Cerrudo says.

"Once, however, commercial and open source AI and machine learning software becomes more available and easier to use, cyber-criminals will start to use it for sure."

Nachreiner says although few cyber-criminals leverage machine learning/AI currently, that doesn't mean it won't happen. "Believe it or not, cyber-criminals are usually behind information security researchers," he says.

There are many new attacks and techniques highlighted at conferences like DEF CON and Black Hat long before any criminal attacker weaponizes them, according to Nachreiner. "The fact that cyber-criminals haven't widely started leveraging machine learning yet doesn't mean it's not an upcoming threat, but it does allow you to prepare for these attacks before they happen."

While it is hard to predict exactly when criminals will be widely using AI to mount attacks, organizations must get ready and ensure that the appropriate counter measures are in place so as to mitigate the impact as much as possible END



TOP TEN

Cases of Insider Threat

01 Edward Snowden

A former contactor for Booz Allen Hamilton working at the NSA, Snowden disclosed almost two million files in 2013.
Source: ***Bloomberg***

02 'Kim'

In South Korea, a 24-year-old man was among those charged with leaking 27 million data files from various online gaming website registrations, including names and passwords. He sold them to make $390,919.
Source: ***CSO***

03 Chelsea Manning

The former US army soldier turned over approximately 500,000 documents and sets of information to WikiLeaks in 2010, including diplomatic cables and details on air strikes.
Source: ***Wired***

04 Jason Needham

Needham stole blueprints from the FTP server of his former employer Allen & Hoshall, taking schematics, staff emails and budget and marketing documents.
Source: ***The Register***

DAN RAYWOOD

Insider Threats Can Prove to be Very Real

The insider threat is a constant and tricky problem for cybersecurity. Hard to detect, and often disguising their actions to bypass security controls, it requires the most stringent security measures to catch malicious insiders in the act, which can potentially involve crossing the line on monitoring employees.

There is always a concern that employees may be disgruntled or seek alternative ways to earn money. In a recent case, Amazon investigated reports that employees were taking bribes to leak confidential sales information and internal data to independent merchants selling their products on the site. Employees were reportedly contacted via secure messaging apps, leading to further concerns about how insiders are communicated with.

With this fresh example of how a rogue outsider can get to your employees and impact your data privacy, we bring you the top 10 notorious examples of when the insider threat hit big.

05
Jiaqiang Xu

A former IBM software engineer stole proprietary source code to make software to sell to customers, before voluntarily resigning in May 2014. He was sentenced to five years in prison in January 2018.
Source: ***Reuters***

06
Christopher Grupe

After being suspended and ultimately resigning from the Canadian Pacific Railway, Grupe logged back into the network to delete files and change passwords, leaving admins unable to log into switches.
Source: ***The Register***

07
Walter Liew

Liew was convicted of economic espionage and theft of trade secrets, selling DuPont technology to China for the production of a valuable white pigment.
Source: ***SFGate***

08
Ricky Mitchell

The former network engineer reset servers to original factory settings after finding out he was due to be fired, disrupting business operations at EnerVest for a month.
Source: ***Computer World***

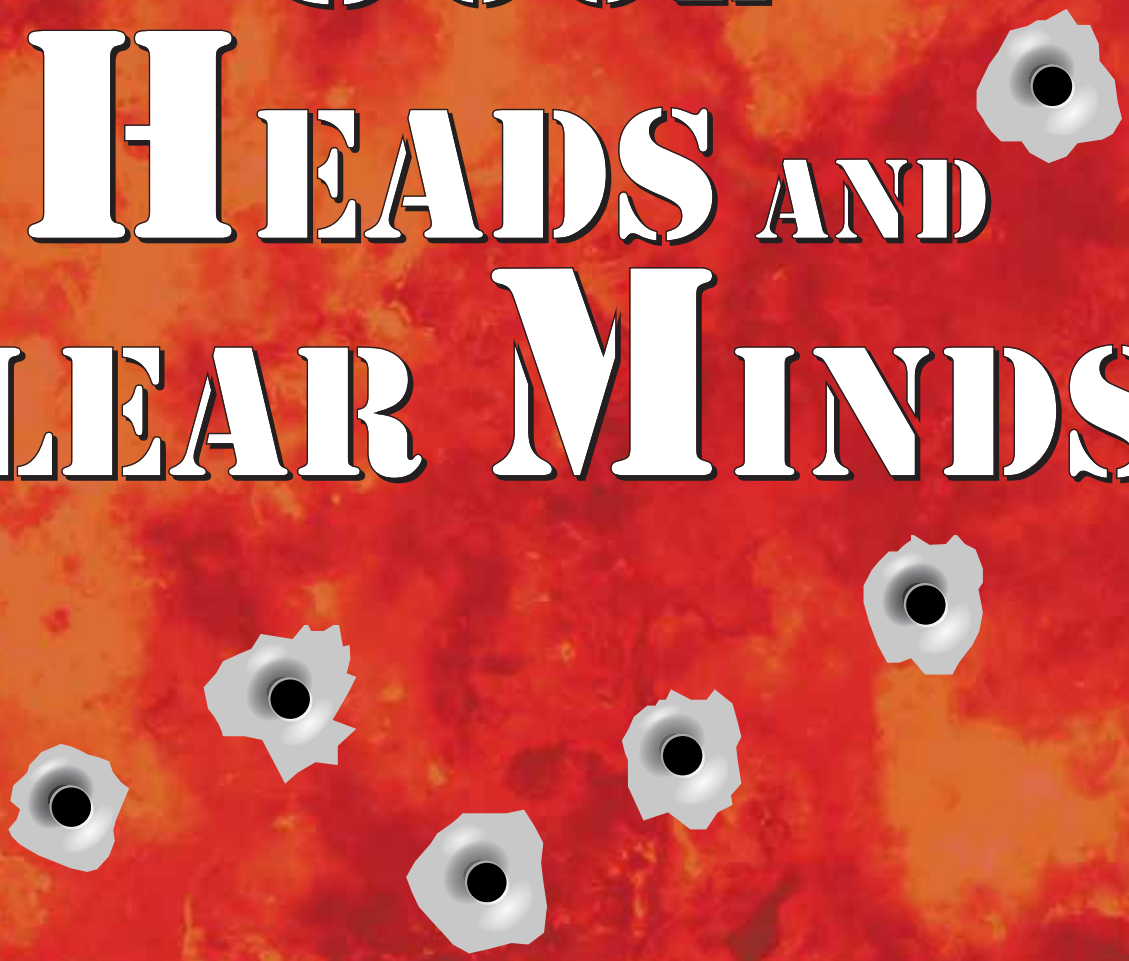
09
Anthony Lewandowski

Before founding Otto, Lewandowski was alleged to have stolen 14,000 confidential files from Waymo when it was a part of Google, his former employer.
Source: ***The Guardian***

10
Nghia Hoang Pho

The 68-year-old man worked at the NSA for 12 years, and between 2010-2015 he stole classified material, such as documents and hacking tools. He was sentenced to five and a half years in 2018.
Source: ***ZDNet***

Cool Heads and Clear Minds:



GETTING YOUR INCIDENT RESPONSE PLAN TOGETHER

In 2018, serious cyber-attacks are inevitable. As a result, effective incident response is crucial to cybersecurity readiness. *Phil Muncaster* investigates

There were a few raised eyebrows when Dido Harding presented her keynote speech to attendees at this year's Infosecurity Europe. Wasn't she the CEO that presided over one of the most infamous data breaches of recent times at TalkTalk: one which stemmed from systemic security failings at the telco and was compounded by catastrophically poor incident response? As it turns out, her presentation was relatively well received: full of contrition over the mistakes that were made and packed with constructive suggestions for CISOs and board members on how to avoid them in the future.

Unfortunately, CEOs and boards the world over have yet to learn the same lessons as Harding. Yet increasingly companies are judged not just on whether they could have prevented an attack, but on how well they respond. Master the art of incident response and you could minimize the financial, reputational and regulatory impact of an attack while potentially even escaping with your job intact.

When, Not If

It's well understood by most in the cybersecurity space today that their organization will inevitably be hit by a successful cyber-attack at some point. A UK government report earlier this year claimed that 43% of businesses experienced a cybersecurity breach or attack in the previous 12 months, while Risk Based Security claimed there were over 2300 reported breaches globally in the first half of the year alone, exposing 2.6 billion records. These stats are both likely to represent just the tip of the iceberg.

That's not to mention the impact of ransomware, cryptojacking attacks, banking trojans and more. The cumulative effect of this new dynamic, weighted in favor of the attackers, is to emphasize the importance of incident response. Spot an attack early on in the kill chain and you could kick your adversary off the corporate network before they've had a chance to exfiltrate much data. If you're too late for this, you could still notify customers before the cybercrime underground has had a chance to monetize the stolen information.

> ***"One of the most important and also complex facts for organizations to understand is that incident response can never be treated as a project"***

The Arrival of the GDPR

Getting incident response right has been added extra urgency after the GDPR was passed – bringing with it a mandatory rule for notification of major breaches within 72 hours. UK data regulator the Information Commissioner's Office (ICO) has a checklist which illustrates the kinds of things it expects. At the very least there should be "robust breach detection, investigation and internal reporting procedures in place," with responsibility for managing breaches placed in the hands of a dedicated individual or team. Also key are processes to escalate incidents internally so the appropriate team can decide if a breach has occurred, and to inform affected customers "without undue delay" if the worst has indeed happened. Interestingly, the ICO claimed recently that organizations "are struggling with the concept of 72 hours" and that some breach reports are being sent incomplete.

The lesser known EU NIS Directive for CNI providers in the region also covers incident response, mandating organizations notify the authorities of any severe incident which might impact service levels "without undue delay," and "take appropriate measures to prevent and minimize the impact of security incidents to ensure service continuity." Both regulations come with major fines for non-compliance, of up to €20m or 4% of global annual turnover.

Learning from Others

It's not hard to find examples of poor practice in this space over the past few years. Equifax is one of the most recent: fined £500,000 by the ICO for its failings. Aside from the fact that the attack came from an Apache Struts vulnerability which it knew about but failed to patch, its response to the breach of over 145 million consumers' most sensitive personal credit details was poor. The firm took around six weeks to disclose, during which time some execs sold shares in the company. Then it directed users to a separate site to get info on the breach: a site some browsers flagged as a phishing threat. Customers reportedly even had a hard time getting the info they needed on whether their data was affected. Then the firm was forced to clarify T&Cs which some customers interpreted to mean that if

> ***"As organizations respond to incidents or as cyber-threats evolve, they should evaluate the effectiveness of the plan and update accordingly"***

they signed up to credit monitoring they would forfeit their chance to participate in class action suit.

Other examples include TalkTalk, which rushed almost too quickly to communicate with its customers following a 2015 breach, first speculating that four million customers may have been affected and erroneously suggesting the suspected theft was the result of a DDoS attack. It was also unclear whether customer data was encrypted. Meanwhile, a National Audit Office (NAO) report on the NHS response to WannaCry, which led to an estimated 19,000 cancelled operations and appointments, revealed the Department of Health's plan had crucially not been tested at a local level.

"As the NHS had not rehearsed for a national cyber-attack it was not immediately clear who should lead the response and there were problems with communications," the report explained. "Many local organizations could not communicate with national NHS bodies by email as they had been infected by WannaCry or had shut down their email systems as a precaution."

Elsewhere, Yahoo is notable for the sheer length of time it took to discover a catastrophic breach of customer data: three years from the 2013 date of the incident before it estimated one billion users were affected, and then almost another year before revealing the actual breach was three-times that size. In Uber's case it was also 'better late than never' but with a twist. In this case, the firm infamously decided to pay off the hackers and keep a breach of 57 million users a secret.

Developing a Plan

So what does best practice look like when developing and executing an incident response plan? Experts agree that it's vital to include stakeholders from all parts of the business including comms, legal, HR and others. SANS Institute instructor, Mathias Fuchs, tells *Infosecurity* that organizations must consider: a communications plan for dealing with press and shareholders, a predefined "circle of trust" governing internal information flows, preapproving any necessary changes like firewall blocks or proxy configuration as standard operating procedure and open lines of communication with law enforcement. It's also important procurement is involved in planning as cloud providers must be chosen with incident response in mind, he adds.

"Assuming a sponsor inside the organization has already been defined, the first step usually is to set up a workshop involving all stakeholders. In my experience, no battle plan survives the first shot, so the key takeaway from this workshop usually is a common understanding of what the organization perceives as a major security incident as well as a basic understanding of where certain capabilities are located, i.e. insourced versus outsourced," he says.

"One of the most important and also complex facts for organizations to understand is that incident response can never be treated as a project. A project manager always assumes that he or she sets the pace and controls what happens. That is fundamentally different in a major incident, where at first the attacker is in full control of the situation. As a consequence, the major goal of successful incident response is getting back and staying in control as fast as possible."

Once the plan has been drawn up, the organization needs to ensure it is constantly updated, according to PwC's US cybersecurity and privacy leader, Sean Joyce.

"After an organization drafts this document internally, external partners should be engaged to ensure the plan addresses best practices, industry, regulatory, and legal requirements," he tells *Infosecurity*. "As organizations respond to incidents or as cyber-threats evolve, they should evaluate the effectiveness of the plan and update accordingly. Organizations can further test the effectiveness of their plan through tabletop exercises which would provide opportunities for stakeholders to understand their roles and receive ongoing training."

Processes and guidelines such as those from COBIT or NIST can help in crafting incident response, especially with remediation techniques, according to former ISACA Chapter president, Ramsés Gallego. He tells *Infosecurity* that organizations must also calculate their Recovery Time Objective (RTO) as well as a Recovery Point Objective (RPO).

"These disciplines are instrumental here and should never be crossed beyond. They are the moment (time) and step in processes (point) from where the company cannot recover its normal operations," he continues. "It is like saying that from those moments onward, the company cannot go back to its desired state and will fail to proceed."

Going Live

Once they've developed an effective incident response plan, companies must stick to it when the bullets start to fly, according to Chris Hodson, director at the Institute of Information Security Professionals (IISP).

"I believe it was Mike Tyson who once said 'everyone has a plan, until they're punched in the face.' It is important that your plans represent the potential in-scope threat events, which could damage your business," he says. "Businesses need to understand 'who does what' and make sure that these people are on-point to execute the response plan. If it's the CEO who speaks with the media, ensure they know precisely what to say – avoid them getting into discussions about types of attack or technical nomenclature."

> ***"It is important that your plans represent the potential in-scope threat events, which could damage your business"***

SANS Institute's Fuchs adds that responders should not rush to kick an attacker out before they've got the full picture of what they were looking at and what has been exfiltrated.

"If they didn't get what they were there for, they will return. Find better ways to detect them and avoid them getting back in the same way they did the first time," he concludes END

How to Get the Most Out of Penetration Testing

Emilian Papadopoulos

President, Good Harbor

Emilian is president of Good Harbor, a premiere cyber-risk advisory firm. He is a graduate of the University of Toronto and the Kennedy School of Government at Harvard University, and teaches cybersecurity as an adjunct faculty member at Georgetown University.

@epapadopoulos

For years, cybersecurity professionals adopted a 'perimeter defense' model for security that focused on keeping bad hackers out of an enterprise's network, much like someone in the medieval ages would seek to protect their castle with walls and a moat. In that model, penetration tests made intuitive sense; since the goal was to keep bad hackers out, a reasonable solution was to hire good (white hat) hackers to test one's perimeter defenses and report where holes existed. These holes could then be patched. This, it was thought, would keep the enterprise secure.

With time, cybersecurity professionals learned that 'perimeter defense' was a failed model; bad hackers could get into the network or, in the case of insider threats, might already be there.

The cybersecurity profession moved on to a 'defense-in-depth' model that accepts the network perimeter will get breached and focuses on layers of internal defenses. More recently, leading professionals have adopted a 'zero trust' model for designing IT systems and networks that puts even less emphasis on the perimeter.

Under these new, more sophisticated models, traditional pen tests are not very useful. They over-emphasize the perimeter. Also, because pen tests are snapshots in time, a pen test may help find and patch a hole today but does little to help stop a new hole from emerging tomorrow, putting the enterprise at risk.

Unfortunately, years of faith in pen tests means that they have become cemented in regulatory regimes and audits. Thus, a traditional pen test may be required for compliance reasons, for example on a quarterly basis. In this case, the best way to do the pen test is inexpensively, spending little of one's precious budget on it, and focusing it on critical systems. The second reason to consider a traditional pen test is because it can be an inexpensive, quick way to persuade a reluctant, incredulous executive that an enterprise's network and perimeter are, in fact, insecure: 'Look how fast the pen testers got in!'

> ***"Traditional pen tests have a few good uses, but budget and personnel resources can be better allocated elsewhere"***

Beyond these two uses, enterprises should skip or minimize the traditional pen test.

Instead, focus on internal hacking assessments: give the white hat hackers credentials for notional accounts within the enterprise and see where in the network they can go, whether they can escalate privileges and gain access, what they can find and do, and whether security systems will catch them. This avoids wasting money or time on the hackers penetrating the network, which is often the easy part. If an enterprise has deployed a defense-in-depth or zero trust model, the hacker in the internal hacking assessment will have a much harder time accomplishing their objectives without being detected.

Enterprises also benefit from investing wisely in continuous monitoring within the enterprise and on application security, especially in an age when more and more enterprises' products include software.

In summary, (inexpensive) traditional pen tests have a few good uses, but budget and personnel resources can be better allocated elsewhere END

Adrian Sanabria

VP of Strategy and Product Marketing, NopSec

Adrian has spent a decade building security programs and defending large financial firms. Prior to joining NopSec, Adrian co-founded Savage Security, an applied research and consulting firm.

@sawaba

Relative to the age of the information security industry, penetration tests are old. They've been commonly offered as a consulting service since the late 1990s. Somehow, they have simultaneously become one of the most common, inconsistent and misunderstood services offered.

Much confusion exists around what the output of a pen test should be and even what a pen test is. At its core, it is an opportunity to test the health of the security program and many of the individual security controls. The idea is to bring someone from the outside to point out any glaring gaps and to see whether or not they could get in, as a criminal might.

> ***"The goal is to test controls, defenses and staff"***

If our goal is to ensure that our vulnerability scanners haven't missed anything, that's not really a pen test, it is a vulnerability assessment. The goal is to test controls, defenses and staff, not to perform comprehensive lists of missing patches and configuration issues.

Understand why you need the pen test and share this information with the firm. Is it for PCI compliance? Did your organization just get hacked? The myriad reasons for hiring pen testers is important. When shopping for a consulting firm, make your goals clear.

Do your research. Consider interviewing a firm and their consultants to gauge experience and see if they are a good fit for your organization.

Who will be actually performing the assessment? That principal consultant you interviewed, are they the ones doing the test or is the firm going to send a junior analyst with apologies about schedule conflicts? If you want a specific tester or just one with more experience, demand that individual for your engagement and have it written into the contract.

Talk to peers and find out who they use or prefer. Recommendations from someone in your professional network is a reliable way to choose. Look for firms that will be familiar with the technology and products you use. Ask for the pen testing methodology used. If the firm has their own methodology, ask to see it. Ask to see sample reports; firms should have actual reports that have been scrubbed or anonymized to safely share with potential clients.

Think about certification. Generally, certifications exist to provide proof of skills when experience cannot. In some cases, they can signal a lot more. A pen tester with their OSCP has gone through some serious training to obtain that cert. Some firms may require certifications like CREST (mostly in the UK) or CISSP (worldwide).

Lastly, be prepared. Define the rules and scope carefully. A narrow scope isn't useful, but if you have devices you know automated scanners will knock over, you may want to exclude them from the test. How do you want the tester to handle success? Should they inform you immediately of any critical vulnerabilities, or save them all for the report? How deep should they go? Should testers siphon entire mailboxes, databases and file shares of data to prove their point, or just enough to prove they've done it?

A pen test is a great opportunity to test your incident response team's ability to detect and respond to attacks. Make it clear to the pen tester if you intend to detect and stop them. Many treat this as the realm of more mature organizations and a job for a red team END

Gemma Moore

Director, Cyberis

Gemma has spent more than 10 years working in the security consultancy industry and has helped customers across a wide range of industry sectors assess their risks and improve their security. She was selected to receive a lifetime CREST Fellowship award in 2017.

@cyberisltd

Good communication and a collaborative working relationship – before, during and after – is key to achieving the best results and value-for-money from a penetration test. The testing team typically comes into your organization for a short period of time, so if they are to interpret the impact on your business of technical risks, they need to understand the context in which the systems operate and what you want to achieve from the test.

An effective pen test starts with a comprehensive scope of work. To do this, you need to understand the requirements of the systems, networks and applications you are assessing. What data assets are present or accessed from these systems? Who are the threat actors you are most concerned about – criminal gangs, hacktivists, malicious insiders or all of the above? What are the key security requirements of the systems in scope – are you most worried about confidentiality, integrity or availability and what other concerns are on your mind? What security controls have you implemented and what do you believe they are doing? What other systems and controls are dependent on the systems in scope and vice versa?

This process will give the testing team as much information as possible about how the systems in scope should be behaving and the principal security concerns. Although a broad generic methodology is often applicable to a pen test, the most effective teams will tailor approaches to ensure that all key security concerns are addressed. Having this additional context also allows security test cases to be addressed explicitly within the report and helps to ensure remedial advice gives the best protection and mitigation.

> ***"An effective penetration test starts with a comprehensive scope of work"***

During an assessment, make sure that test teams have access to key technical stakeholders involved in the development and/or management of the solution. This helps both sides. When the team encounters unusual behavior, they can ask questions about whether it is intentional as part of the design, for example, or try to pinpoint root causes of problems identified. Equally, when a vulnerability is identified, the test team can explain and demonstrate these issues so that technical stakeholders have a good understanding of the root causes.

Debrief meetings are also important. As the consultant who leads your testing is not likely to have a full understanding of the business context, their interpretation of the technical risks will be imperfect. During a debrief meeting, there is an opportunity to have a full two-way discussion about the wider business context and threat landscape, refining the overall understanding of how the technical risks reported fit into the business. It gives stakeholders the chance to ask questions directly and ensure that issues are understood. It is also an opportunity to discuss alternative remediation strategies and whether these might work to reduce or remove the risk.

The best single piece of advice would be to find a pen test provider that you trust and build effective communication with them. The more your pen test team understands about what you are trying to achieve with your business, the better the advice they will be able to give you END

FEATURE

THE PRINTER SECURITY PROBLEM

Michael Hill investigates a significant element of corporate endpoint security that is still slipping under the radar

Enterprise endpoints have posed significant security risks for organizations for quite some time. With more and more connected devices and products finding themselves in the workplace and imbedded into corporate networks, security teams have been forced to move from a traditional perimeter-focused approach to one which ensures individual devices are updated, secured and maintained to a definite level of compliance.

However, whilst both organizations and manufacturers have slowly but steadily developed greater focus on securing devices such as laptops, tablets, smartphones and servers, there has been one commonly found and much-used corporate endpoint device that has tended to slip under the security radar – the office printer.

Security issues surrounding printers are nothing new, with incidents of printed document loss dating as far back as the 1950s and 60s and continuing to cause issues ever since. The big difference in today's digital world is that modern printers are sophisticated devices, and a lot are now being produced with numerous in-built functionalities that are putting them at far greater risk than ever before, without the same sophistication of security to go with it.

This was showcased at DEF CON in Las Vegas this year, when researchers from Check Point released details on two critical vulnerabilities in a popular HP OfficeJet Pro 6830 printer which they were able to exploit by targeting its fax capabilities. With just one simple fax message, they not only quickly gained access to the printer, but also leveraged it for further penetration.

"One discovery led to another," Yaniv Balmas, group manager, security research at Check Point and one of the vulnerability discoverers, tells *Infosecurity*. "By exploiting the fax protocols, we were able to create a malicious file (which appeared to be a color JPEG image file) and send it over the phone line to the target fax-printer machine. The fax-printer then uploaded the 'image' file and stored it in its memory without any file checks being applied."

Hewlett Packard was quick to release a patch for each exploit and, in September, announced the launch of the very first bug bounty program specifically for office printers, offering rewards of up to $10,000 (based on the severity of the flaws discovered) for researchers who correctly identify vulnerabilities in its printing products and software.

"As the first service of its kind in the market, we anticipate our bug bounty program will help many businesses stay ahead in the cybersecurity battle," says George Brasher, managing director – UK and Ireland, vice-president and general manager, HP.

What these two things show is that, not only has an enterprise the size and scale of HP recognized the need to offer potentially hefty sums of cash for disclosures of vulnerabilities solely in its printing products, but that office printers still have easily exploitable but potentially damaging flaws. When you put that together, the obvious question to ask is: how big is the printer security problem in 2018?

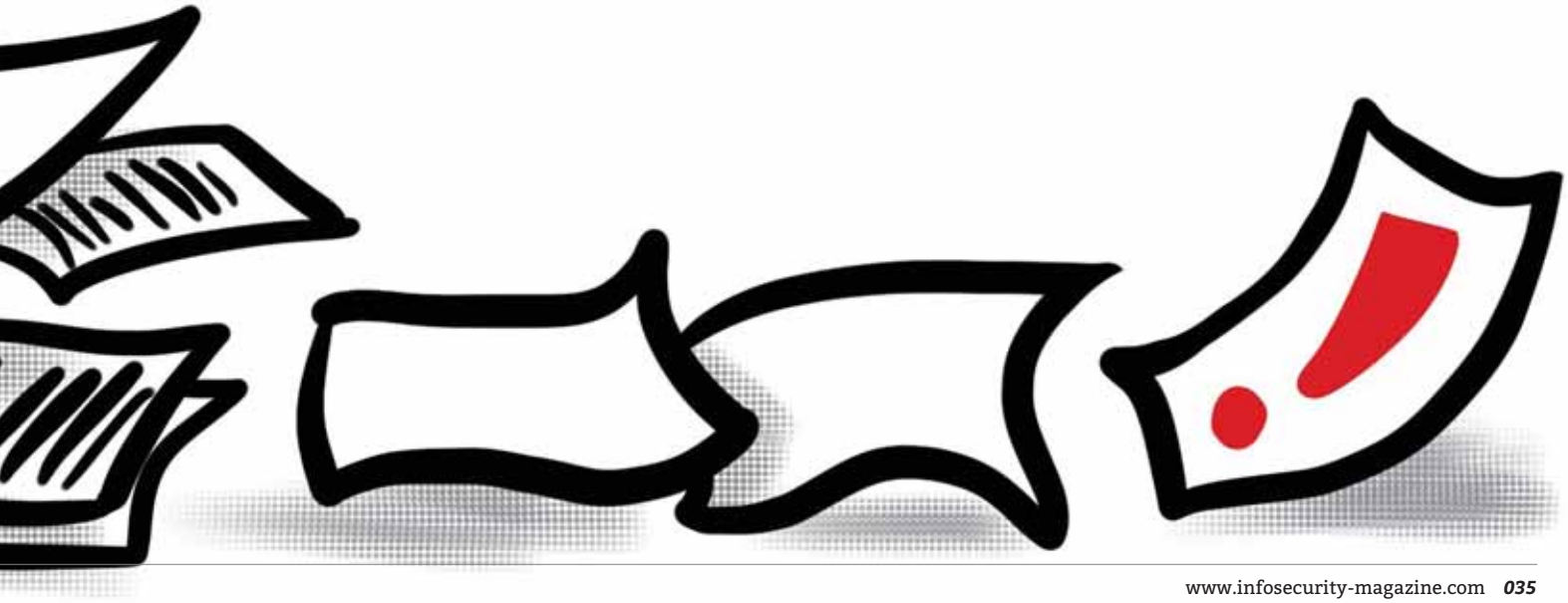
Slipping Under the Radar

According to Sebastien Jeanquier, principal security consultant at Context Information Security, the world of printer security in the enterprise is largely an anachronistic oxymoron.

> ***"Printers don't run security technologies such as anti-virus or host-based intrusion detection services, which makes them easier targets for attackers and more difficult to secure"***

"The state of the role of printers in enterprise security hasn't changed very much over the past decade, with printers continuing to pose a threat to enterprise networks due to their status as largely unmaintained systems with numerous security flaws," he explains. "Printers don't run security technologies such as anti-virus or host-based intrusion detection services, which makes them easier targets for attackers and more difficult to secure."

Conversely, Quentyn Taylor, director of information security at Canon for



EMEA, argues that corporate printer security is better than it was in the past, with both physical and software feature sets evolving to meet an increasing threat landscape and making printers more secure out of the box.

What both experts do agree on though, is that significant printer security problems continue to occur in the enterprise as a result of gaps in security awareness compared to other endpoints and failures to keep them actively administered, with vital updates often neglected.

"Once printers are installed in an environment, often directly onto the local internal LAN, they are seldom updated, meaning that any vulnerabilities identified and fixed by the manufacturer may not be patched on end devices in the field," Jeanquier says.

"Multi-functional devices are, in most cases, the last servers that have been left on the shop floor in most enterprises," Taylor concurs. "In some companies they are the biggest part of IT spend that sits outside of the IT budget and are too easily viewed as being an everyday part of the office landscape, despite the massive amounts of sensitive data that they both hold and process. There is a tendency to underestimate the risks of printers because they are a familiar part of the office."

Greater Functions, Greater Risks

A familiar part of the office they may be, but gone are the days when office printers were simple devices that merely churned out documents and did nothing more. Most corporate printers are now capable of storing large amounts of information in print queues and hard drives, scanning and sending documents of all kinds, receiving emails and have processing capabilities akin to servers – not to mention network, internet and cloud connectivity and protocols enabled by default. That not only makes them a more attractive target for attackers from a data perspective but, due to unsecured vulnerabilities, a more openly exploitable one.

"Printer manufacturers have implemented an increasing number of software features that are intended to be useful, but also bring with them new attack paths via weak network services or even browser-based applications," says Jeanquier.

The public hacking exploits of Balmas and his colleague at DEF CON were a prime example of how "features and functions in these devices – such as fax capability – are easily overlooked, yet can be targeted by criminals and used to take over networks to breach data or disrupt operations." What's more, whilst it was just the work of researchers seeking to do good, the types of vulnerabilities unearthed were very real and, in the wrong hands, have the potential to cause catastrophic damage to enterprises of all sizes.

"Printer manufacturers have implemented an increasing number of software features that are intended to be useful, but also bring with them new attack paths"

The Threat is Real

As Balmas points out, the simple method they used to compromise the OfficeJet all-in-one inkjet printer could easily be manipulated to launch "any type of malware or exploit" – ransomware, spyware, cryptominers – and spread full malicious payloads to the connected network. "Depending on how that network is protected, the damage could be severe and widespread."

Brasher is also quick to warn of the real-world implications of business printers that are open to the network and have complex (and subsequently vulnerable) operating systems. "This isn't theoretical, it's an attack vector that hackers have already used successfully," he says. "A 2017 study by analysts Quocirca found that 61% of all businesses surveyed had experienced at least one printer-related data breach."

Even if the data going through a device is secure, adds Taylor, components within the device can potentially be exploited for other purposes. "Endpoints [such as printers] are still targeted because they continue to produce results," he says. "It may seem trite to suggest that it's easier to exploit a device that either can't be secured or has been badly configured, but it's a fact."

Solving the Problem

So what needs to be done to address an enterprise security problem that appears to have existed for far too long but is yet to be effectively addressed?

For Taylor, the responsibility first lies with manufacturers, who have a significant part to play. "They have an obligation to provide endpoints that are fit for purpose, secure and with privacy built in," he argues.

Jeanquier echoes similar sentiments, adding that "manufacturers should consider adopting a 'less is more' mindset when deciding what network services to implement, prune antiquated services that customers are unlikely to ever need and mitigate initial risks by having such services disabled by default."

Businesses themselves must also bear part of the responsibility too, argues Balmas, and it is "critical that organizations protect themselves against possible attacks by updating their machines with the latest patches and separating them from other devices on their networks."

A corporate printer is only ever as secure as its weakest link and it is up to the information security team to understand the threat that any device like a printer can bring, Taylor adds. "Organizations need to be aware of the risks that endpoints present and specify the non-functional requirements to address the risk. Cheaper and faster may seem more effective until an insecure endpoint on a device allows it to be used for data exfiltration or as part of a DDoS attack."

Key things for an organization to also consider include understanding the type of data its printers process, knowing how users interact with them and making the security choice the default (such as badge-enabled printing or secure guest/mobile printing) and deciding how the printer fits into the wider corporate security setup.

In today's threat landscape, choosing an endpoint device is now a security decision, argues HP's Brasher: "It means that anyone involved in a hardware purchasing decision – however small or large – will have an influence on the security posture of the business."

"Ultimately, security is everyone's responsibility and enterprise-wide security awareness goes a long way in solving the security issues that are familiar in the day-to-day," Taylor concludes END

TWO EXPERTS GO HEAD TO HEAD

Point

CISO on the Board: A Specious

Ira Winkler

President, Secure Mentem
Ira is author of *Advanced Persistent Security* (Syngress, 2017) and president of Secure Mentem. He has more than 30 years of experience functioning in various roles within industry and government in organizations of all sizes.
@irawinkler

With all of the recent cybersecurity-related incidents there has been a great deal of talk regarding placing security experts on corporate boards of directors. The argument goes that proper governance of the organization requires a cybersecurity expert at the highest levels of management. Clearly nowhere is higher than the board of directors, so the CISO, as the top cybersecurity expert in the company, is the one that some suggest should be on that board. While the argument makes sense for the layperson, as well as admittedly biased people within the security profession, it is an extremely specious argument.

While I am not arguing the importance of providing proper cybersecurity for an organization, and such cybersecurity requires that the appropriate experts have the required input into the strategic planning process, the board of directors is not the place for the people overseeing such issues. Likewise, the appropriate cybersecurity experts rarely have the actual expertise required to be members of the board of directors.

While there is no specific definition of tasks for a board of directors, they generally involve:

- Governing the organization by establishing broad policies and setting out strategic objectives
- Selecting, appointing, supporting and reviewing the performance of the chief executive
- Terminating the chief executive
- Ensuring the availability of adequate financial resources
- Approving annual budgets
- Accounting to the stakeholders for the organization's performance
- Setting the salaries, compensation and benefits of senior management

Local jurisdictions may have laws defining required actions by the board of directors as well, however they generally ensure due diligence in the performance of fulfilling their responsibilities.

> ***"While a CISO should brief the board of directors and provide reports, they should not be on the board itself"***

Such responsibilities are strategic and, despite the fact they primarily involve finances, even the chief financial officer is rarely granted a seat on the board, unless they are a founder in an early stage company. Can it be argued that a CISO will provide valuable input into setting policies and ensuring adequate resources go to security? Sure. However, the same argument can be made for almost any responsibility within the company.

For example, isn't the CIO, who is responsible for the overall proper functioning of the computer systems (which would include security), more deserving of being on the board than the CISO? After all, not only is the CIO responsible for securing the computers, they are responsible for ensuring that the computer systems are also properly functioning, have the required uptime and response, are properly staffed and resourced, etc. While security failings have created major problems, system outages from coding errors, power outages and similar malignant issues have caused more losses to date than a malicious hacker's wildest dreams. The COO can likewise make a case that they are responsible for the overall operations of an organization, and therefore deserve a seat on the board.

The best analogy I can give is that since people are critical to an effectively functioning organization, the director of human resources should have a seat on the board, even though the HR director typically reports to the CFO.

However, even if CISOs generally should be on the board, it is rare that they have the other requisite financial background required of a board member.

I do appreciate the need for a board to ensure that there is the proper level of cybersecurity within an organization, and at the end of the day, it does fall to the CISO to make their case. However, while a CISO should brief the board of directors and provide reports, they should not be on the board itself.

It is my mantra that security programs fail because they get the budgets/resources that they deserve, not the budgets/resources that they need. If a CISO believes that they are not getting what they need now, it means that they fail to deserve more. While being on the board might give them more visibility to make the case, they will still fail to make their case. CISOs need to learn to speak and understand business concerns better, and in my opinion any CISO who believes they belong on the board is demonstrating that they actually don't understand business fundamentals, such as board responsibilities and the overall operation of a business END

Counter-Point

Argument vs the Future Path

It's fascinating that most board members and CEOs do not know exactly what the CISO does. Fascinating, but worrying. This could be because it's so difficult to describe the job plainly – after all, the CISO has to defend against threats that haven't even occurred yet. Perhaps, as the CISO is often buried under the CIO, the core messages are overshadowed.

What is clear is that collectively, we require a new breed of CISO. In today's increasingly complex threat landscape, the CISO should be – at a minimum – an advisor to the board, if not a member of it.

The board needs to be represented by members with a firm understanding of the security risks facing the company. If the CISO is to have a place on the board, we need to answer two questions: how do we achieve this goal, and what clean up is required before it can happen? Gaining a seat on the board is complex; even with mega breaches and new guidance, it's not a straight shot to the top.

For a CISO, the board meeting is anything but familiar. Technology topics are rarely discussed, and those that are will rarely involve information security. Even a level down – at an audit or governance committee meeting – things don't get any better. A risk or privacy officer runs the meeting, and will 'represent' a CISO's message. The same can often be said for Executive Leadership Team (ELT) meetings. Information security is not prioritized, and CISO attendance can be rare.

With the CISO often buried in the IT organization, there is a massive hill to climb. The journey to the board must first involve joining the ELT and various board subcommittees, presenting to the board, and then finally having a seat on it. Before this can happen, some clean up must occur on the CISO side – primarily to demonstrate that it's not about security for security's sake. Preparation takes time, but CISOs should focus on some key areas.

Stop Allowing Filtered Messages

CISOs must ensure their messages are never filtered – up or downstream – and critical information is never omitted or made less severe before it reaches them. They need to show their teams they are open to bad news, reducing the possibility of subordinates leaving out details that will lead to hard questions. In the same vein, a CISO should never feel compelled to sugar-coat or 'dumb down' reporting to the board.

Beware the Danger of Proxies

Recent research from Exabeam uncovered pervasive differences of perspective between the C-suite and frontline staff on the adequacy of current technology, staffing and alert workload. The cause? They rarely, if ever, share direct information. Information is instead shared through many layers of middle management who 'improve' or remove the message – an unhelpful proxy. The CISO's absence on the board is another form of this same problem. Board membership and participation will remedy this, but CISOs also need to be conscious of this issue within their own teams and the wider organization.

Don't Get Buried Alive

The CISO is often buried under IT. It may seem natural, but this rarely makes for a good security environment. Ensuring the right reporting structure can go a long way. In many forward leaning organizations, the CISO reports directly to the CEO, with the CISO reporting *into* the board. This is a good first step in the evolution of the CISO role, followed by board observer roles and eventually membership.

Focus on Cooperation, Not Just Budget

Budget is important, but organizational cooperation is crucial. Boards are likely to see the budget alone as a quick fix, not understanding that it takes efficacy, adoption and maturity to actually improve capability. CISOs need to ensure information security remains a priority for the board after an allocation of additional funds.

Offer Perspective

Many board members know very little about the pains of information security; it is the CISO's job to provide the right perspective. Don't 'dumb down' ideas, but remember to use plain language – be clear, concise and compelling. The CISO needs to show they are there to advise, protect resources and insulate the board's time from negative outcomes.

The CISO's journey to the board is a long one. While rapid movements happen during crisis, CISO success is too often in the hands of other teams and priorities are discussed in rooms they are not invited to. CISOs have an asymmetric fight against a host of threats and adversaries, but this often describes the internal struggle – begging for cooperation from those they've committed to defend. Board level visibility, especially membership on it, allows for more than acknowledgement of this fight; it allows for top down cooperation and effective prioritization. Primarily, CISOs need to help the board by delivering the right messages and understanding exactly what information is being shared. It's the road less travelled, but the one the CISO must take

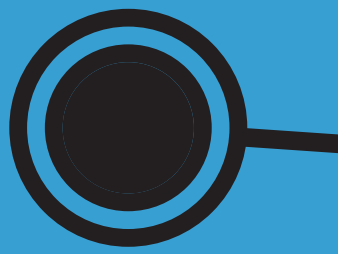
Steve Moore

Chief Security Strategist, Exabeam

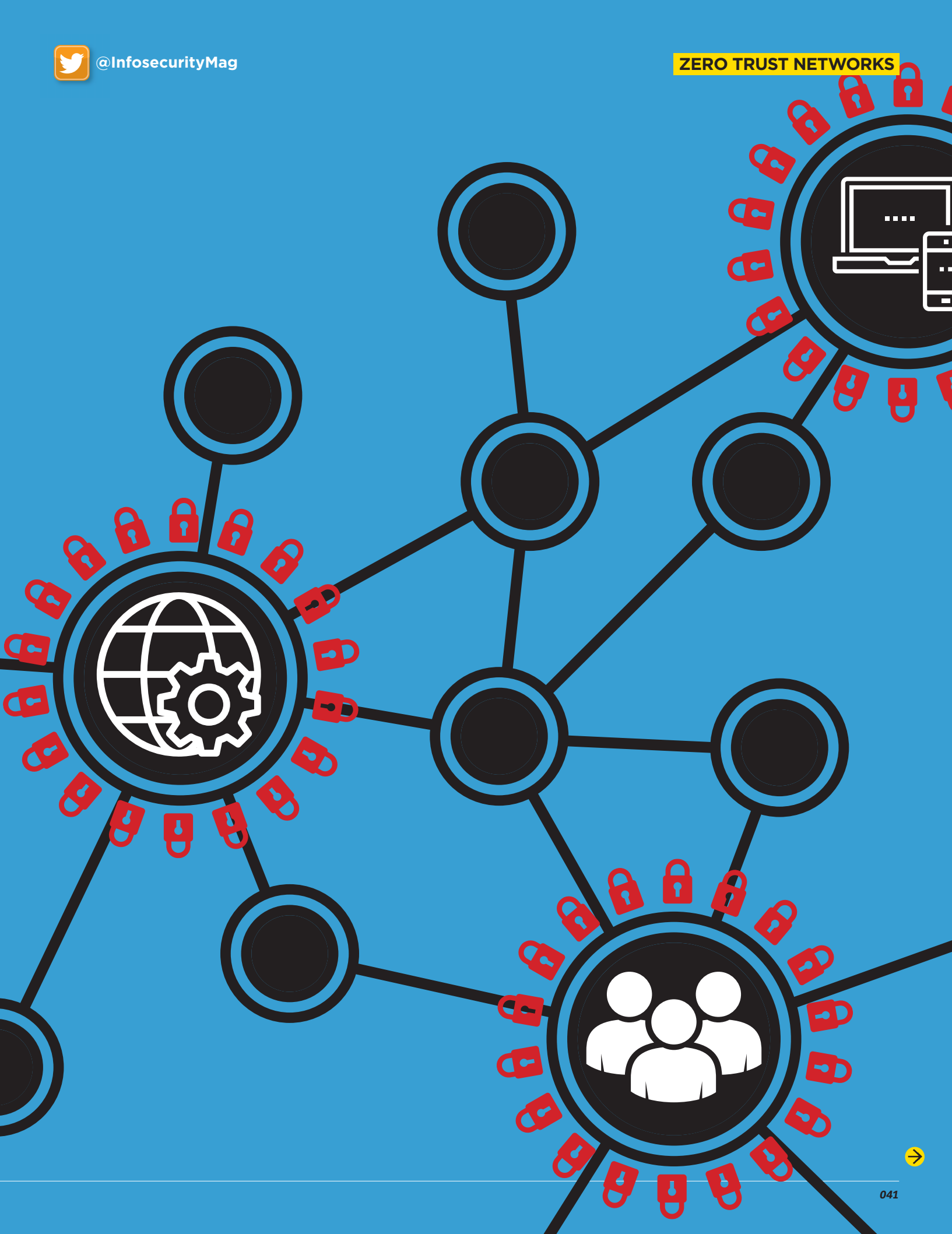
Steve helps drive solutions for threat detection and response, as well as advising customers in breach management and program development. He brings deep experience working with legal, privacy and audit staff to improve cybersecurity. ***@exabeam***

FEATURE

PUTTING FAITH IN ZERO TRUST



The last couple of years have seen the zero trust concept gain fresh traction. What has driven this new interest, and is this the way that security networks should be built now? *Dan Raywood* investigates



Back in September 2010, Forrester researcher John Kindervag published the first of two whitepapers on the concept of the zero trust network. A decade later, the zero trust model has flourished to create concepts for companies to adopt and implement, along with generating a raft of products and deployments based on Kindervag's original idea.

> *"The basic foundation of zero trust is to continue to verify a user's identity and authenticate access at every resource"*

In the Beginning

The November 2010 whitepaper claimed that zero trust was needed as there was a fundamental problem with trust in information security, and it was the trust model that needed to be changed.

"By changing our trust model we can change our networks and make them easier to build and maintain; we can even make them more efficient, more compliant and more cost-effective," Kindervag said at the time.

As a result, zero trust has become one of the de facto ways that cybersecurity can operate, based on its three core concepts: 1) there is no longer a trusted and untrusted interface on our security devices; 2) there is no longer a trusted and untrusted network; and 3) there are no longer trusted and untrusted users.

Ultimately, zero trust mandates that information security professionals treat all network traffic as untrusted. This helps with securing concepts like BYOD and IoT, as well as detecting attackers inside your network – if you assume everything and everyone is bad, and that there is no perimeter, you're making a start on creating a more secure network infrastructure.

Kindervag originally claimed that network professionals "built yesterday's networks at the edge, with the internet connection, and then built inward" with the starting point of the router and routing protocols. The approach requires starting with system resources and data repositories that need to be protected, as well as the places where compliance is required, and a network is built out from that point.

Kindervag recommended starting with protecting data first and figuring out how to do the networking second.

It is now eight years since the whitepaper was published and 10 since the zero trust idea was conceived, but more recently the concept has been cited as a way of working securely. Speaking to *Infosecurity* in 2018, Kindervag explains that the zero trust topic has become a 'buzz word' term for conferences and vendors.

So is he happy that it has become so popular? "It is gratifying as people said I was insane and some vendors told Forrester to kill it, but it was great for me, and great to have some adversarial reaction and to be considered at multiple levels, and in a unique way it has been a blessing."

Industry Acceptance

The concept has led to several vendors offering strategies and tools to aid zero trust. One is Duo Security, who launched the concept of Duo Beyond to follow Google's BeyondCorp and Intel's Beyond the Edge.

Dave Lewis, global advisory CISO for Duo Security at Cisco, tells *Infosecurity* that he prefers to call it "unified access security," and says that while he feels Kindervag did a great service in coming up with the term zero trust as it started driving conversations, all it did was confirm "what we should have been doing all along – network segmentation, asset inventory, user management. Every one of these pieces of the puzzle should have been there all along," he adds.

> *"The principle of zero trust changed as so much has gone off the network between mobility and the move to cloud and SaaS"*

Lewis says that the conversation is starting to permeate, and is being accepted more now as companies realize that they need to be having discussions around the concept.

Speaking to *Infosecurity*, Corey Williams, Centrify's senior director of product marketing, points out that zero trust has been driving conversations over the last year, which shows that "people were looking or grasping for some sort of model to look at."

Williams comments that the principle of zero trust has not changed, but the guiding principle has. "The basic foundation of zero trust is to continue to verify a user's identity and authenticate access at every resource," he says. "The vision is of moving the network closer to the resource and having a limited amount of access to resources."

However, this drive towards it being about access control irked Kindervag, who argues the concept was designed to be a strategy and to be able to work with business leaders to "solve serious systemic issues that security refused to change." He stresses the need to also include packet inspection and logging of all traffic, while access control was only on a "need to know" basis.

The Fallow Period for Zero Trust

So why was the concept not really considered as a way of working between its introduction and its resurgence in 2016?

Rodney Joffe, SVP and fellow at Neustar, says that when Kindervag developed the concept in 2010, zero trust "probably sounded like yet another buzz phrase to most CIO/CISOs." He adds that if they had looked at what was being suggested, they would have agreed with it.

"In the interim, practitioners have recognized that breaches are inevitable, and now they are able to use John's phrase to describe what they now realize is a must."

Lewis claims that the reason for the silence around zero trust was "because there was an increase in data breaches which got exponentially larger and we realized we had to do something." On the other hand Williams believes that the principle of zero trust changed "as so much has gone off the network between mobility and the move to cloud and SaaS." The concept of zero trust therefore needed to evolve, he adds, and that is why the access management conversation began.

That period saw breaches including Target, where a zero trust network could have prevented the supply chain attack, and Uber, where attackers were able to

> *"It makes it extraordinarily difficult for data to be exfiltrated and easy for authorized people to analyze in an appropriate way"*

gain access to servers using credentials collected from a Github account.

Kindervag says that the idea of zero trust is that it is designed to stop breaches, but it is actually about protecting "data apps assets services" and by doing that, "it makes it extraordinarily difficult for data to be exfiltrated and easy for authorized people to analyze in an appropriate way."

Just Like Starting Over?

Lewis explains that enabling zero trust doesn't require networks being built from scratch or even being rebuilt, "as we have all the moving pieces, it's just about implementing them correctly." He adds that where those pieces are missing, that's where tools like multi-factor authentication come in.

Lewis says that the focus has to be on realizing what you're trying to solve, as no vendor will say "these are your requirements" – you have to identify the requirements of what you are trying to address.

Dinis Cruz is CISO of Photobox. He believes that the best way to adopt zero trust is to start the project small and scale up. "It is not one of those things where you say 'let's pick five examples' as we moved to cloud platforms and explored further, but you want access from everywhere so build an isolated environment and start with one and move to others."

He likens this to an internal development process, where forms have to be signed in order to gain access, and changes are made in an isolated environment.

Cruz points to the need for better visibility, as one way to create zero trust is to understand what is happening in your environment. "If one app is being attacked I should be able to build a sandbox around it, and why should it talk to other things and allow untrusted access? If we have visibility of that behavior to know what is going on, then that becomes an easy process."

Ultimately, Kindervag says, zero trust is "still at the baby stages" and in his role as field chief technology officer at Palo Alto Networks he is still trying to get people to take on the idea, as once they grasp it "the idea sells itself."

Kindervag had previously claimed that zero trust is something "you augment your existing network with, and that you do in incremental stages" and while zero trust is one way of working and enabling access, it is not perfect and not suitable for everyone. Yet in these times of concern about remote access from untrusted and unverified sources, this may be one way of solving a security woe END

Zero Trust at Google

by Max Saltonstall, Technical Director, Information Technology, Office of the CTO

Passwords are terrible. Scratch that: we're terrible at remembering them, phishing them is easier and password theft and reuse are both on the rise. At Google, we emphasize security keys as a core part of our trust calculation, and that strong authentication has become the core of our zero trust system, BeyondCorp.

The phrase zero trust gets thrown around a lot; at Google, we mean that we put zero inherent trust in any network. We don't assume access is trustworthy because it came from inside the office. Instead, each connection needs to earn trust by showing strong authentication, authorization to access the requested resource, and a fully encrypted connection. There are three pillars to this.

Authentication

Access to an internal resource can only be granted if we know who is making the request and to help Googlers prove their identity – everyone gets a set of security keys on their first day at work. Following the FIDO Alliance standards, they do an encrypted handshake with the server to ensure that authentication only occurs with a validated server. Using these keys has reduced the success rate of phishing attacks drastically: Google has no reported or confirmed account takeovers since implementing security keys – and we suggest everyone adopts them, especially admins with access to sensitive resources.

In addition to authenticating the person, we want to authenticate the device. Establishing and revoking trust from devices complements the user trust element – if a device is compromised, we can detect that with our inventory metadata tools and revoke trust quickly, flagging that device for remediation.

Authorization

Now that we know who's asking for a resource, and what device they are asking from, we can test to see if they are actually allowed access. All traffic to internal services flows through a reverse proxy, and the proxy prevents the request from even reaching the back-end if that person does not have the right permissions. We can authorize access according to group memberships, job role, location, employee type and numerous other factors.

Encryption

With a trusted device, a trusted login and a check for the right permissions, we need to secure our connection. By requiring encryption we mitigate man-in-the-middle attacks or other situations where an unknown listener is on our communication channel. Our reverse proxy terminates TLS to understand the request, re-encrypting as necessary to communicate with other internal services as it routes the request properly.

Outcome

The rollout of BeyondCorp, starting in 2010, was not without its challenges, but the ultimate outcome is that our workforce is more mobile, collaborative – and safer – than ever.

FEATURE

GDPR: SIX MONTHS ON

Cordery's *Jonathan Armstrong* reflects on the first six months of the General Data Protection Regulation

The General Data Protection Regulation (GDPR) came into force around six months ago, on May 25 2018. You would have had to have lived in a cave to miss it, but has it lived up to the hype? The simple answer is yes and no. There has clearly been a lot of GDPR action in terms of complaints, live investigations and some early enforcement activity. The pre-GDPR 'fake news' has been shown to be just that – there weren't millions of fines on day one (this was never likely), businesses didn't close down en masse (also not likely) and the Thames didn't flood (again, not likely). We have seen a lot of activity though and some pointers to the shape of things to come.

Reported Data Breaches on the Rise

One of the easiest predictions to make was that the number of reported data breach actions would rise. Pre-GDPR, only a few EU countries had data breach reporting restrictions. The UK had a voluntary process which the GDPR replaced with the obligation to report data breaches to data protection authorities (DPAs) unless the data controller could show that the personal data breach "is unlikely to result in a risk to the rights and freedoms of natural persons."

Where feasible, this report has to be made within 72 hours of the breach being discovered. Pre-GDPR, some of us said that the 72-hour deadline was too short a time to make a proper assessment. Early evidence under the GDPR regime would suggest that this is true. In June 2018 alone, the Information Commissioner's Office (ICO) received 1792 data breach notifications. The rise has continued across Europe, for example the Data Protection Commission in Ireland said in August that it was receiving about 230 breach notifications per month. Some of those notifications might prove not to have been necessary, but it is understandable that since the burden is on a data controller to prove that a data breach is unlikely to result in risk, organizations reporting breaches will err on the side of caution. This is a trend that we are likely to see continue.

As a result, there's been a sharp focus on rehearsing breach reporting and investigation. We've trained over 300 individuals in the skills needed and, for some, the skills they have learned in those rehearsals have already been tested in the heat of battle.

There is a different threshold for reporting a breach to those who could be affected. Here the data breach must be likely to "result in a high risk to the rights and freedoms of natural persons." DPAs are worried about breach notification fatigue – an issue in the US where individuals don't take breaches seriously because they get so many notifications. We have seen significantly fewer notifications to individuals because of this different test, and in recognition of data breach notification fatigue. Having said that, the UK has seen some mass notifications including those from Dixons Carphone, British Airways and Facebook.

Significant Volumes of Complaints

Complaints to DPAs are also on the rise. The ICO in the UK received 4214 complaints in July 2018 alone and again we have seen this trend across most of Europe with just under 4000 complaints in France in the first four months of the GDPR being in force. There are also a significant number of cross-border complaints – the new European Data Protection Board (EDPB) met on May 25 to allocate the first cross-border

complaints made by Max Schrems' pressure group European Center for Digital Rights (or NOYB for short). There were more than 100 complaints designated as cross-border by mid-July and these are likely to be significant. A number of pressure groups are also involved in making 'super complaints' including NOYB, La Quadrature du Net in France and a well-funded group targeting the advertising industry. We are likely to see some significant announcements in some of these complaints in the next few months.

A Rise in Subject Access Requests

There has also been a substantial rise in the number of Subject Access Requests and those that are being made have increased in complexity. We are seeing a significant number of current and former employees make wide-ranging Subject Access Requests and it is more difficult to narrow down the search under the GDPR than it was before. We have also seen the first examples of mass Subject Access Requests being coordinated to almost work like a DDoS attack on an organization.

Fines Are Not the Only Penalty

In the run up to the GDPR, much was made of the high levels of fines available to DPAs under the new regulations. However, DPAs get far more powers, some of which (in some circumstances) can be more damaging than fines. On July 6 2018, the ICO issued what is thought to be the first 'stop processing' notice against AggregateIQ, a Canadian entity which is on the ICO's radar because of its connection to the investigation into Facebook and Cambridge Analytica. The notice required AggregateIQ to stop processing data on UK and EU citizens. AggregateIQ has appealed, with the appeal having been lodged on July 30 2018. This will prove to be an interesting early look at the additional powers of the ICO and the extra territorial reach of the GDPR.

> ***"The GDPR won't live up to the Doomsday scenario painted by many – but that was never realistic. It will, however, change the way we use data for good"***

Civil Actions on the Increase

As well as giving more powers to regulators, the GDPR puts more power in the hands of individuals. They can enforce their rights and in some circumstances they can hold DPAs to account as well. Pre-GDPR we had already seen a rise in civil actions – individuals using the courts to claim compensation after a data breach or a mishandling of their information. Examples like the Vidal-Hall case showed us that our courts were willing to grant compensation for multiple claimants, although the Lloyd case in October has shown it is not as easy as some may have thought to bring these cases procedurally. In the US, civil actions after data protection breaches have become commonplace. The GDPR has accelerated the rise of a similar class action culture in the UK. The 'where there's a blame there's a claim' culture has been prevalent in some of the pre-GDPR data breaches – for example, in the BA breach, class action lawyers worked over the weekend to send a letter before action to BA claiming damages. That's just a taste of things to come.

What's Next?

It's clear that the GDPR is having a real effect on companies big and small. In the next year we'll see some big fines – but not at the top level. We'll see a rise in citizen policing of the GDPR as individuals make more data subject requests and litigation kicks in. We'll also see an even greater concentration on information security and data breaches as organizations realize they've reported significant numbers of breaches and they're living in the last chance saloon. The GDPR won't live up to the Doomsday scenario painted by many – but that was never realistic. It will, however, change the way we use data for good END

FEATURE

CYBER INSURANCE: THE NEXT STEP IN CYBERSECURITY PREPAREDNESS?

Kathryn Pick examines the recent growth of cyber insurance and the impact of this new but quickly developing form of indemnity

Companies across the globe have been facing an increasing threat of being attacked by cyber-criminals. From hacks on British Airways passenger data through to ransomware threats targeting the NHS, the corporate network is a prime target.

What's more, as we have seen in the headlines, the financial impact of these attacks can be huge – even catastrophic – to a firm.

In October 2018, Tesco Bank agreed to pay out £16.4m as part of a settlement with the Financial Conduct Authority over a cyber-attack in 2016, but even bigger sums have been brought.

Tools to protect a business have long been a feature in a boardroom conversation, but in recent years, the extra layer of protection offered to a company's wallet by cyber insurance has become the new topic.

So what benefits can cyber insurance bring to businesses in the Wild West of cybercrime, and are there any downsides for those looking to invest in the new protection?

What is Cyber Insurance?

For those new to the topic and asking what cyber insurance actually is, Daniel Kennedy, research director for information security at 451 Research, describes it as simply a "form of risk transference" for a business.

"It allows an organization to identify the potential impact of an outage, data breach, or other financially damaging event caused by a security issue," he says.

"Then, they can build an ability to leverage and pay for outside forensics services/expertise and financial recompense to their set of planned responses."

So, whilst you put locks on your doors to protect your worldly possessions, you still make sure your home insurance is up-to-date in case burglars successfully break in. Cyber insurance offers you that same reassurance for the precious goods locked in your data center.

A 2018 report from IDC by analyst Sabitha Majukumar recommends that over the next 12 months, businesses consult with risk management professionals and financial analysts to determine whether it is the right move to make. Then, within the next 24 months, have their policy implemented and ready to give that double lock safety assurance.

Why Has it Grown in Popularity?

According to *The Betterley Report,* a cyber/privacy insurance market survey, the compound annual growth rate of cyber insurance globally was 31% between 2010 and 2017, so it is clearly a hot area. The worldwide market is also estimated to be around $4bn, with 90% of the premium income underwritten in the US.

A survey by the Department for Culture, Media and Sport in the UK found that around 9% of businesses have cyber insurance, and this figure grows to 24% for large businesses.

However, Juergen Weiss, managing VP of financial services at Gartner, says this is much smaller than across the Atlantic, estimating only between 5%-10% of the market is bought on British shores.

"There is also less understanding about the complexity of cyber insurance," he argues. "A recent survey from the DAS UK Group, a UK legal expenses insurer, and HSB Engineering Insurance showed that nearly one-third of UK brokers admit to having only a 'poor' or 'very poor' understanding of cyber-risks and cyber insurance."

Although, the market, and in turn the understanding of it, is only predicted to rise, with Allianz and other brokers estimating it will reach around $20bn come 2025.

Even with that trajectory, Weiss says: "You need to be aware that cyber insurance represents only a small fraction (less than 1%) of the global insurance premium volume."

Be that as it may, why is it on the rise?

Weiss says the reasons are pretty obvious, naming Europe's General Data Protection Regulation (GDPR) as a key factor.

It may have only come into force in May this year, but the new rules enforcing CIOs to have tight consent management processes and effective data rights management systems to protect what the EU considers their "most valuable asset" (data) come with stiff penalties.

Those found to be in breach of the new regulations can be fined up to 4% of annual global turnover or €20m – whichever is greater – and as much as 2% for not having their records in order.

Joseph Ahern, cyber policy adviser at the Association of British Insurers, says: "GDPR has raised the profile of information issues such as security, and also increases the potential cost of data breaches to businesses.

"The greater maturity of the US cyber-market is intrinsically linked to the passage of mandatory breach reporting laws in the vast majority of

> *"It allows an organization to identify the potential impact of an outage, data breach, or other financially damaging event caused by a security issue"*

US states. By premium, around 85% of cyber insurance is written globally for US risks."

Then there is the financial pain already being felt by firms. Thousands of attacks are being launched on networks daily, and according to Statista, the average cost of cybercrime in the US alone last year was over $21bn, which makes the need for cover an obvious one.

Yet, according to an estimate by MunichRe, only 5% of these losses are currently insured.

Heidi Shey, a principal analyst at Forrester, says: "Over the past year, major data breaches and ransomware attacks, such as Equifax, NotPetya and WannaCry, made headlines and affected companies globally.

"It's these serious events that remind business leaders just how much their organizations have at stake and why they need new or more cyber insurance.

"The CEO of Lloyd's attributes these events as the reason that cyber insurance is the fastest growing product segment at her firm."

What Support Does it Provide Organizations?

Kennedy says having that safety net of cyber insurance provides businesses with the ability to recoup losses from business interruptions, extortion – like ransomware – and data breaches.

"It is that last category that gets a bulk of the attention from practitioners I've spoken to," he says.

"It includes things like the costs associated with forensic investigation to determine the scale of a breach, customer notification – which isn't easy as state level breach notification laws are a patchwork of requirements – credit monitoring for affected customers, call center support, regulatory or payment card industry fines, and so forth."

Ahern argues that cyber insurance does a great deal more than simply pay claims in the event of a breach or cyber-incident.

"It also provides practical advice and support to prevent breaches from happening in the first place," he says.

"The exact support and policy coverage provided by insurers to their customers will differ depending on providers and the level of cover that is purchased.

"However, the core parts of cyber insurance have some common aspects, such as preventative support, beginning during the underwriting process, which provides an opportunity for firms to consider and address major vulnerabilities within their business, leveraging the expertise of their insurer.

"Support will typically continue throughout the duration of the policy through services such as online risk management support."

However, Shey says companies must do their due diligence when finding the right fit for the business.

"There are more factors to consider than which carrier offers the best coverage for the best prices," she says. "Assess their cyber-acumen, review their service panels, check their claim approval rates and ask to speak to a customer reference who's been through that process."

> *"Some of the issues for buyers are high premium costs and insufficient aggregate limits"*

Majukumar agrees, adding: "CIOs should carefully evaluate whether cybersecurity insurance is appropriate for their organization. This evaluation should include an assessment of the level of risk that would be covered by the policy and overlapping coverages that may already exist."

Is There a Potential Downside to Cyber Insurance?

Ahern simply says no, "not unless you see paying a premium as a downside – but that's part and parcel of having a good insurance policy in place."

However, Kennedy says that while it offers many benefits, cyber insurance is merely a piece of the puzzle for keeping yourself protected. "Policies typically have limits on pay outs, number of records/customers affected, and a myriad of other limitations to be aware of," he warns.

There are more risks too.

"The first is of course a false sense of confidence around what cyber insurance is able to cover, and a possible de-emphasis on the due care required around detective, preventative and incident response controls," explains Kennedy.

"Using Equifax as an example, despite multiple cyber insurance policies in place, insurance only covered a fraction of the actual breach-related costs, and could never cover things like reputational damage."

Kennedy says there is also a question about an encouragement for the extortionists. "Today, there is a very low percentage of organizations reportedly paying ransoms for ransomware type situations. Does the advent of insurance coverage therefore make it 'easier' to pay an extortion? In the medical field, for example, it can be easier to pay out on even dubious medical malpractice claims today because the cost equation has shifted.

Weiss says there are problems for both buyers and sellers in the market. "Some of the issues for buyers are high premium costs and insufficient aggregate limits, confusion about terms and conditions, non-standard products, complex pre-screening and complacency.

"For sellers there is the rating and pricing complexity, profitability considerations, adverse risk selection, moral hazard, reinsurance capacity, target market segmentation and the accumulation of risks."

Shey adds that you must look hard to find the right provider for you. "Cyber insurance policies are long and convoluted, and so is the list of providers in the ecosystem," she says. "Evaluate your broker, carrier and post-breach service options closely, and scour through your policy to minimize stringent sub limits and coverage gaps."

We all know that ignoring cybersecurity comes at yours and your business' peril. Now, the growth of cyber insurance is giving organizations something else to think about. It may seem like just another element on a long list, but if done right and evaluated first, it could be something to save you and your company in the long run

END

@InfosecurityMag

SLACK SPACE

Grumbles / Groans / Gossip

01 Crafty Ransomware Doesn't Bother Scottish Brewery

Drinkers faced the prospect of beer running dry when Arran Brewery was hit by ransomware.

According to reports by the BBC and *The Register*, attackers sent an email with a malicious PDF which infected the network with the Dharma variant. Attackers then demanded two Bitcoin (around £10,000 or $13,000 at the time of writing) to decrypt.

Well, the Scottish brewery said that the cost to decrypt was more than the value of what was encrypted, so it simply restored from backups and only lost three months' worth of sales data from one infected server.

"However, the ransomware had encrypted all attached file shares, including those that recent online backups had been saved to, so it was only offsite backups which were available," Gerald Michaluk, managing director of Arran Brewery, said. "The most recent of [these] was some three months old."

Ransomware is rarely targeted, and in this case the brewery was the victim, although there is something of a happy, 'glass half full' ending with them refusing to pay the ransom and being able to restore without major loss.

Apparently, Arran Brewery had been advertising a vacancy which had yielded many applications; perhaps that point of contact provided the details the attackers needed to hop into action.

It seems that the brewers came out of this scenario with a smile on their faces, as production seemed to be unaffected, and they were reportedly back up and brewing soon after the incident.

Raj Samani, chief scientist and McAfee fellow at McAfee, called the infection "really simple but very ingenious," as it allowed criminals to sneak in a malicious document amongst the barrage of applications.

"It appears the ransomware variant is one that there is no decryptor for right now, but the first course of action for all of us should always be to check on NoMoreRansom to determine if a free decryptor is available," he added.

"It's great that the company did not pay, and only by affecting the RoI of ransomware developers are we likely to dissuade more people in distributing ransomware."

02 Kinks in the Password

There was potential embarrassment all round when it was discovered that a popular fetish app was storing users' passwords in plain text, according to *Engadget*.

Whiplr bills itself as the "first and largest community for kinksters" – providing a platform for open-minded people to find, meet and chat with potential 'play partners', all within its feature-filled, location based messenger. It's believed to be used by millions of people across the world.

Well, they may have found a niche market for people looking for kinky kicks, but they certainly seem to be lacking in the security department. Apparently, users received a message asking them to verify their Whiplr account by entering their password in plain text format – which means that's exactly how it was storing credentials in its database, without any form of encryption.

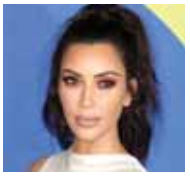
Whilst Whiplr isn't the first business to be guilty of storing passwords in this way, when you consider the obvious anonymous nature of the app (there's rarely real names used, profile images are few and far between and normally obscured to keep identities private...you get the picture) it's particularly shocking.

Think of the possible ramifications – if the company suffered a breach, an attacker could have easily accessed the data and used it to work out the true identity of users – it does hark back to the notorious Ashley Madison breach of 2016, and we all remember how that turned out!

Whiplr was quick to apologize for the faux pas and insisted that it has taken steps to improve the security of its stored passwords with one-way encryption. The fact is though, companies are breaking no laws by storing user credentials in plain text format, so whilst this incident is certainly eyebrow-raising, it probably won't be the last of its type to hit the headlines.

1. Glass half full for infected brewery

2. A fetish faux pas!



3. Kim K was 2018's 'most dangerous celeb' to search for

03 Risky Celeb Searches

Be careful who you search for online, as media powerhouse Kim Kardashian has been revealed to be the most dangerous celebrity to search for in the UK in 2018.

Research from McAfee assesses the risks surrounding online searches by tracking bad web links (known for installing malware, delivering malicious links and even stealing credentials) associated with celebrities on the internet. It found that Kim Kardashian, the daughter of OJ Simpson's lawyer and mother of Kanye West's kids, was the top result. Kim beat Naomi Campbell in second and her sister Kourtney in third place, with Adele and Caroline Flack coming in fourth and fifth places.

Sean Sullivan, security advisor at F-Secure, said that about 10 years ago a standard Google search would quite possibly result in malicious links on the first page of results, but by 2011, the problem really wasn't prevalent at all.

"Now a minority of people actually 'search' for content rather than just allowing the auto-suggest algorithm to finish their query," he explained. "Now, there is SEO poisoning that goes on in the wild, and certainly there is a lot of content farming that utilizes 'popular people' to drive engagement to low-quality sites, and those sites are far more likely to host malvertizing, etc."

Tim Helming, director of product management at DomainTools, added: "This is further evidence that consumers need to exercise extreme caution when online. Kim Kardashian is an incredibly popular pop culture figure with a range of products available, making cyber-squatting on her name a hacker's dream. We have identified 29 active domains via our PhishEye technology with a risk score of over 70 associated with her name, meaning it is highly likely that malware or another form of malicious activity is or soon will be taking place on the domain."

Whilst it's clear that this prestige will not be added to Kim K's wall of fame, it does mark a turnaround for female celebrities, as last year's dubious honor went to Craig David. In the case of Kim Kardashian, she had over 58 million Twitter followers at the time of writing and almost double that on Instagram.

So, is it a surprise that a search for Kim can be so dangerous? After all, she initially found fame thanks to a 'private' tape of her with then boyfriend Ray J, and looking for adult content can lead you down a rabbit hole of nefarious links. So keeping up with the Kardashians may just be an online error.

To share your thoughts with us please contact us at ***infosecurity.press@reedexpo.co.uk***

Parting Shots...

Dan Raywood, Contributing Editor

According to statistics published in October, there are around three million vacancies in the cybersecurity industry.

The research came from (ISC)² and of 1452 survey recipients, the highest gap is in the Asia-Pacific region with 2.14 million unfilled roles, partly due to its growing economies and new cybersecurity and data privacy legislation being enacted throughout the region. This is followed by North America with 498,000 vacancies, and 142,000 and 136,000 across EMEA and Latin America respectively.

It feels like these conversations come around constantly: where are the new people coming from? Do they want jobs in cybersecurity? Is this an attractive enough industry to work in? What sort of certifications are needed? What efforts are being put into academia by industry to ensure the next generation are aware? And so on.

The truth is that there are efforts being made, but the problem continues to be reported and surveyed. Is this endemic of cybersecurity focusing too much on the problem and not on the solutions or successes?

We have seen many efforts to solve the skills issue – numerous cybersecurity challenges have been held and participants have been made aware of the career opportunities that exist (with many taking full-time jobs as a result). We've seen universities expand their offering beyond straightforward computer science courses, we see conferences offer special student rates and university societies producing their own conferences highlighting both internal and external research.

Despite all of this, it always feels like we dwell too much on the negative side of the issue. One effort to make a difference took place in October in London; it was an event which brought those looking for a job and those looking to hire together. It was called Cyber Recoded and as well as focusing on education around areas such as extra-curricular activities, certifications and apprenticeships, the event offered multiple opportunities for organizations to engage with the delegates.

Whilst on stage chairing a panel, I did notice in the audience several pairings of teenagers and parents, most likely there for the careers fair opportunity. This reminded me of careers fairs that I attended whilst I was preparing for GCSEs back in the early 1990s.

In one instance, I was disappointed to find that the local newspaper group had not showed up. Was I put off a career in journalism because a certain prospective employer did not show? Of course not, I managed to forge my career based on my own enthusiasm and education, but for those seeking a career in the field of cybersecurity, it does pay to keep your options broad.

The (ISC)² study found that the four areas cybersecurity professionals feel they will need to develop most, or improve on over the next two years in order to advance in their careers, include: cloud computing security, penetration testing, threat intelligence analysis and forensics. Of those four areas, pen testing and forensics remain exceedingly popular because of the offensive skills and investigative challenge that it proposes, not to mention the popularity of team contests like Capture the Flag.

Here at *Infosecurity*, we make our own effort to aid the next generation of cybersecurity professionals, with a section specifically dedicated to promoting future cybersecurity stars, which we launched in 2017 (https://www.infosecurity-magazine.com/next-gen-infosec/). Since then, over 100 articles have been published by those seeking an opportunity to get their work and research distributed, and featuring those making an effort to help the next generation achieve their aims. Several next generation audio productions have been made, both as part of our Online Summit events and as a stand-alone webinar. What's more, at Infosecurity Europe in June this year, we gathered together three of the people we have featured for a live video panel discussing getting a job.

> ***"With new options for getting a job and the broad range of possibilities open to the next generation, maybe we will go some way to filling those three million positons"***

This level of education and awareness can only be positive, as the next generation now have opportunities available to them to begin a career. The (ISC)² study found that 34% of respondents said that "unclear career paths for cybersecurity roles" was the biggest career progression challenge, but with new options for getting a job and the broad range of possibilities open to the next generation, maybe we will go some way to reducing that number and filling those three million positons

» FOLLOW US ONLINE

AND STAY UP-TO-DATE WITH THE LATEST DEVELOPMENTS IN THE INFOSECURITY INDUSTRY

TWITTER: **@INFOSECURITYMAG**

LINKEDIN: **INFOSECURITY MAGAZINE**

FACEBOOK: **INFOSECURITY MAGAZINE**

GOOGLE+: **INFOSECURITY MAGAZINE**

WWW.INFOSECURITY-MAGAZINE.COM

Government certified to the HIGHEST STANDARDS

iStorage®

Promo code
IMIS10
Get 10% off on checkout!

CESG Certified Product
Commercial Product Assurance (CPA)

General Intelligence and Security Service
Ministry of the Interior and Kingdom Relations
Baseline Security Product Assessment (BSPA)

NATO OTAN
NATO Restricted Level

FIPS VALIDATED 140-2
FIPS 140-2 Level 3

PIN authenticated, hardware encrypted data storage devices ranging from 4GB to 12TB.

To receive 10% off, enter promo code "IMIS10" on checkout online at www.istorage-uk.com.
Promotion valid until 31st December 2018.

www.istorage-uk.com | info@istorage-uk.com | +44 (0) 20 8991 6260