


info security

EXPLOIT FREE	TROLLING \$3000	PHISHING \$4000	HACKER TRAINING \$4000	BROWSER HISTORY \$1500	ID THEFT \$5000	FACE PROSECUTION
MONEY LAUNDERING \$2000						SPAMMING \$6000
HACKING \$1600						SQL INJECTION \$7000
INTERNET SERVICE PROVIDER \$1500						INTERNET ACCESS TAX PAY \$100
KEYLOGGING \$1400	<h2>The Monopoly of Cybercrime</h2>					BOTNETS \$10,000
REQUEST JAIL BAIL	DDoS \$1000	INCOME TAX PAY \$200	MALWARE \$800	TREASURE CHEST	RANSOMWARE \$600	COLLECT BITCOIN AS YOU PASS GO

Q3, 2018 / Volume 15 / Issue 3

THE NHS AT 70

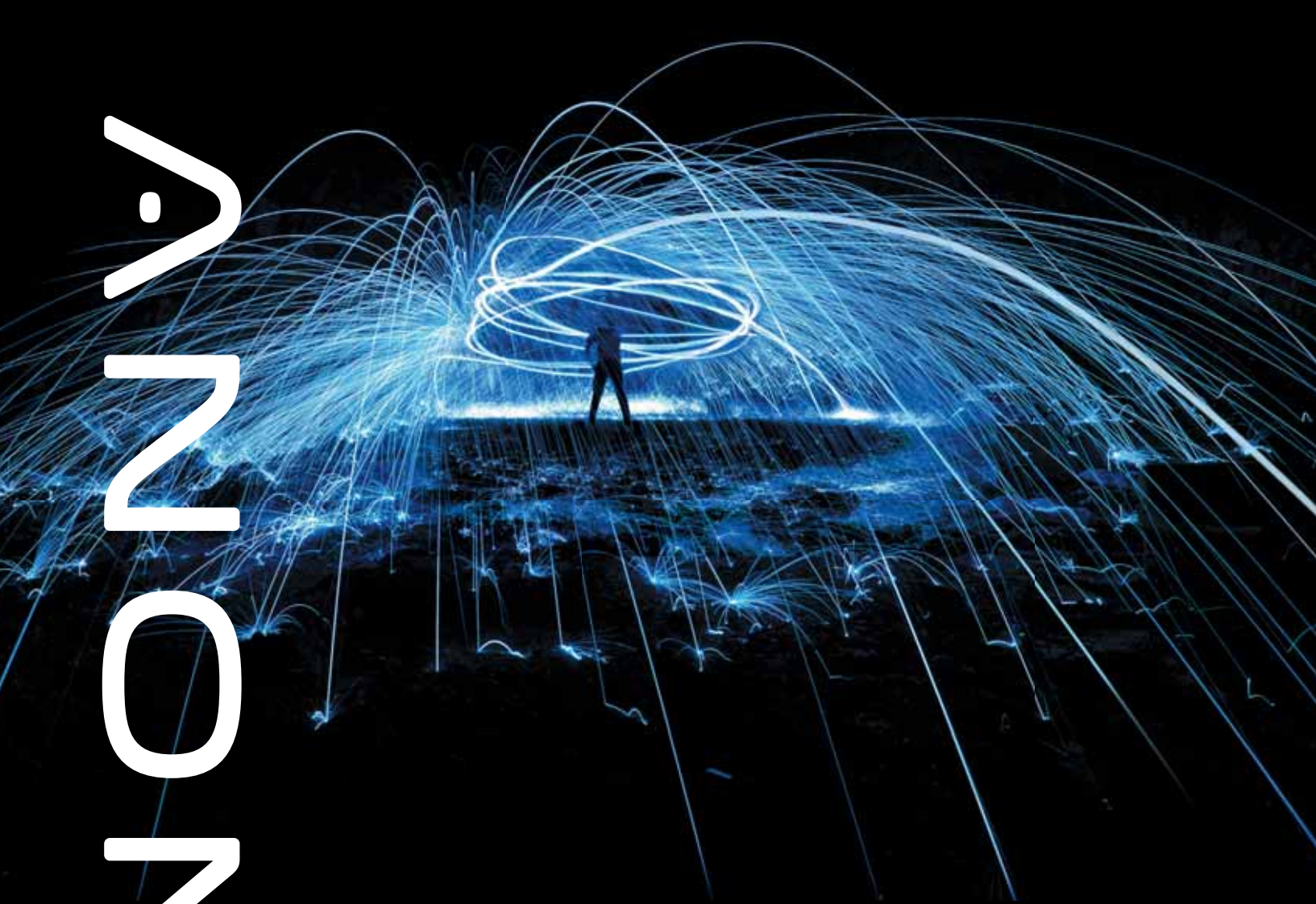
Growing old and growing threats

BREACHES GETTING WORSE

A spiraling epidemic?

ZERO-DAY MARKETS

Rise of the exploit shopping space



Be Cybersecurity Enlightened

We help your organisation become cybersecurity enlightened. With Anomali you can detect threats, understand adversaries, and respond effectively. The threat intelligence platform enables organisations to collaborate and share information among trusted communities and is the most widely adopted platform for ISACs and leading enterprises worldwide.

Learn more: www.anomali.com

COVER FEATURE

12 Dark Economics

Infosecurity investigates the rapidly evolving role of the cybercrime-as-a-service model

FEATURES

8 LORCA: Driving Startup Growth & Innovation

Infosecurity reports on East London's new center for cybersecurity advancements

22 Breaches Getting Worse

Despite increased budgets, better awareness and improved board buy-in, data breaches are not only becoming more common, but also more explosive

28 Zero-Day Trading

Zero-day exploits are now hot property among hackers and researchers, and a thriving online marketplace has arisen as a result

34 NHS at 70: Growing Old & Growing Threats

As the NHS turns 70, Infosecurity assesses the evolution of information security in the healthcare provider

40 Are Blue Teamers the True Heroes?

The time has come to recognize those tasked with defending and recovering from incidents

28 The Rise of Zero-Day Trading



ON THE COVER

12 The Evolution of Cybercrime-as-a-Service



44 Barack Obama

The highlights from Barack Obama's keynote address at Oktane 2018

46 SIEM: The Security Model that Refuses to Die

Is the SIEM model an endangered species or still an essential mainstay in the security posture puzzle?

ONE TOPIC, THREE EXPERTS

32 How to Run an Effective Cybersecurity Awareness Program

Three experts share their thoughts on getting the best out of security awareness programs

POINT-COUNTERPOINT

38 Authentication: Security Improvements

Maritza Johnson assesses how modern authentication is improving the security of information

39 Authentication: Creating New Problems

Raef Meeuwisse explores why new authentication methods are not equating to better data security

INTERVIEWS

11 Interview: Dido Harding

Dido Harding opens up about the infamous TalkTalk breach, her lessons learnt and plans for the future

16 Interview: Martha Lane Fox

From founding her own company to learning to walk again, Martha Lane Fox reflects on her incredible journey

18 Interview: Kevin Mitnick

Eleanor Dallaway meets the man known as the 'world's most famous hacker'

REGULARS

7 EDITORIAL

26 TOP TEN: Regulatory Monetary Penalties

49 SLACK SPACE

50 PARTING SHOTS

The Contributors...



Eleanor Dallaway

Editor & Publisher

With a decade in the industry, Eleanor knows more about infosec than most English graduates should. Any small gaps in her social life are reserved for a good book and even better glass of wine.

@InfosecEditor



Michael Hill

Deputy 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



Infosecurity Magazine



Infosecurity Magazine



Infosecurity Magazine



@Infosecurity Mag

info security

Editor & Publisher Eleanor Dallaway
eleanor.dallaway@reedexpo.co.uk
+44 (0)20 89107893

Deputy 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@pmmmediauk.com

Online US News Editor Kacy Zurkus
kacy.zurkus@kszfreeslance.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 Karina Gomez
karina.gomez@reedexpo.co.uk
+44 (0)20 84395463

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

Copyright

Materials available in Reed Exhibitions Limited's *Infosecurity* magazine and websites are protected by copyright law. Copyright ©2018 Reed Exhibitions Limited. All rights reserved.

No part of the materials available in Reed Exhibitions Limited's *Infosecurity* magazine or websites may be copied, photocopied, reproduced, translated, reduced to any electronic medium or machine-readable form or stored in a retrieval system or transmitted in any form or by any means, in whole or in part, without the prior written consent of Reed Exhibitions Limited. Any reproduction in any form without the permission of Reed Exhibitions Limited is

prohibited. Distribution for commercial purposes is prohibited.

Written requests for reprint or other permission should be mailed or faxed to:

Permissions Coordinator
Legal Administration
Reed Exhibitions Limited
Gateway House
28 The Quadrant
Richmond
TW9 1DN
Fax: +44 (0)20 8334 0548
Phone: +44 (0)20 8910 7972

Please do not phone or fax the above numbers with any queries other than those relating to copyright. If you have any questions not relating to copyright please telephone: +44 (0)20 8271 2130.

Disclaimer of warranties and limitation of liability

Reed Exhibitions Limited uses reasonable care in publishing materials available in Reed Exhibitions Limited's *Infosecurity* magazine and websites. However, Reed Exhibitions Limited does not guarantee their accuracy or completeness. Materials available in Reed Exhibitions Limited's *Infosecurity* magazine and websites are provided "as is" with no warranty, express or implied, and all such warranties are hereby disclaimed. The opinions expressed by authors in Reed Exhibitions Limited's *Infosecurity* magazine and websites do not necessarily reflect those of the Editor, the Editorial Board or the Publisher. Reed Exhibitions Limited's *Infosecurity* magazine websites may contain links to other external sites. Reed

Exhibitions Limited is not responsible for and has no control over the content of such sites. Reed Exhibitions Limited assumes no liability for any loss, damage or expense from errors or omissions in the materials or from any use or operation of any materials, products, instructions or ideas contained in the materials available in Reed Exhibitions Limited's *Infosecurity* magazine and websites, whether arising in contract, tort or otherwise. Inclusion in Reed Exhibition Limited's *Infosecurity* magazine and websites of advertising materials does not constitute a guarantee or endorsement of the quality or value of such product or of the claims made of it by its manufacturer.

Copyright © 2018 Reed Exhibitions Limited. All rights reserved

Online Summit

INFOSECURITY MAGAZINE

BRAND NEW INFOSECURITY MAGAZINE ONLINE SUMMIT

11th - 12th September 2018

14 Sessions | 12 CPE's | 2 Days | 1 Device | 0 Travel



Watch industry thought leader panel sessions covering key industry challenges, case studies & offering real world learnings



Attend short form 30 minute "HOW TO" sessions featuring technical specialists



Download some of the latest whitepapers, webinars, presentations, product information sheets and other data in our resource center



Network & knowledge share in real time with industry peers globally through our new chat room



Earn up to 14 CPE credits towards your SSCP®/CISSP®, ISACA & EC council certifications - fully integrated with your Infosecurity Magazine account

**REGISTER
YOUR
PLACE
TODAY**

The full agenda and speaker line-up
is available on our website.

WWW.INFOSECURITY-MAGAZINE.COM/ONLINE-SUMMITS/

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 effectively, 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...

Reflections

History has a habit of repeating itself.

This saying is particularly true of the information security industry, and also this editorial. Three years after I last bid you all a temporary goodbye as I went off on maternity leave to have my son Wilbur, I'm leaving once again to bring Mini @InfosecEditor 2.0 into the world. As a result, I am temporarily leaving *Infosecurity* in the very capable hands of my deputy editor Michael Hill.

The last three years have been nothing short of groundbreaking for the industry and *Infosecurity* has surfed that wave spectacularly, if we may say so ourselves. Our outreach has exponentially grown, our community has developed and strengthened and our content output is something we continually improve and invest in. I adore my job and it's what makes this – albeit temporary – goodbye just as hard as the last.

As a tip of my hat to the last three years, please indulge me in a trip down memory lane as I share some of my personal highlights as editor of the very best information security magazine and news site out there.

5: Learning How Much You Love *Infosecurity*

Earlier this year we launched a reader survey and we asked you, our fabulous readers, to tell us how much you love us, what you like, what you don't like and what you want more of. When the results came in and it transpired that you actually love us *a lot*, it was incredibly humbling. Everything we do, we do so with our readers in mind. Our website, our magazine, our events, our webinars, our online summits – they are all carefully crafted with our audience at the

heart of every decision we make. So getting confirmation that we're hitting the spot makes it all worthwhile.

4: Interviewing Mitnick

It may have taken me 12 years to meet and interview the 'world's most famous hacker' but it was absolutely worth the wait. I very rarely get nervous before interviewing, but as I stood waiting for Kevin, I felt genuinely anxious. I needn't have. Kevin was an absolute joy to interview and within a couple of hours he was performing magic tricks for me and had called his girlfriend to join us for a chat. I actually feel privileged to have heard his incredible story first-hand and get a glimpse into his incredible vault of knowledge. I hope you enjoy reading all about it on page 18.

3: Launching Women in Cybersecurity Events

In 2017, I had the idea to run a women in cybersecurity networking breakfast at Infosecurity Europe. I didn't know if it would get much traction but I took a leap of faith. I never imagined it would be as successful as it was. Hundreds of people (mostly women, but a big shout out to the men that came!) joined us and the event proved to be insanely popular. I repeated the event this year and it was even more successful, with the feedback even more heartwarming. I love being a woman in this industry and it was wonderful to be in a room with like-minded people.

2: Barack Obama

When Okta approached me to attend its annual security conference in Las Vegas,



1: Dream Team



2: My Hero



3: Who Runs the World?

with a note explaining that Barack Obama would be keynoting, it was an absolute no-brainer. Wild horses couldn't have kept me away. Sitting front row to listen to one of my heroes was truly overwhelming (you can read all about what Barack Obama had to say on page 44). Thank-you so much to everyone that made that trip so incredibly special. I couldn't have dreamt it up.

1: My Wonderful Team

As teams go, the *Infosecurity* Magazine team are the crème de la crème. We're a core team of nine (myself, Michael and Dan in editorial, Becca and Karina in marketing, James in sales and Phil, Kacy and Erin in the news team) but we also sit within the wider Infosecurity Group team (organizers of Infosecurity Europe and Infosecurity North America amongst other events). Our team members are not only talented, dedicated and really smart, but they're also easy to work with and just genuinely great people. A special shout out goes to my partner in crime, Becca. We've worked together on *Infosecurity* Magazine since 2011 and never have I worked with someone with more talent and more commitment. Together we've built *Infosecurity* into the powerhouse that it is today and I could not have done it without her. Thank-you B, you're the best.

Appropriately nostalgic, I'll sign off now and leave you to read on, officially handing over to my noble steed, Michael Hill, who is currently making himself comfortable in my editor's chair. I'll be back in time for Infosecurity Europe 2019 so I look forward to catching up with many of you there.

For now, enjoy the issue and take care.

Eleanor Dallaway,
Editor

LORCA: DRIVING STARTUP GROWTH & INNOVATION

Michael Hill attended the official opening of East London's new center for cybersecurity advancements and reports on the new development

In April of this year it was announced that a new £13.5m cyber center would be developed in East London's Queen Elizabeth Olympic Park, with the aim of helping to secure the UK's position as a global leader in the growing cybersecurity sector.

The London Office for Rapid Cybersecurity Advancement (LORCA), run by innovation center Plexal from its headquarters in Here East, opened its doors for the first time in June. LORCA is supported by partners Deloitte and The Centre for Secure Information Technologies (CSIT) at Queen's University Belfast, with funding from the Department for Digital, Culture, Media and Sport (DCMS) as part of the UK government's five-year £1.9bn cybersecurity investment.

LORCA's primary focus is on supporting 72 later stage startups over the next three years, enabling them to serve the information security marketplace faster and more innovatively, source follow-on investment and scale their proposition. The official opening of the center on June 26 2018 saw the first cohort of 10 businesses welcomed onto the scheme.

Speaking on the day, Matt Hancock, then secretary of state for Digital, Culture, Media and Sport, said that LORCA is going to do vital work to foster the new products that are going to keep people secure online.

"I can tell you this," he said, "having started my career in a tech business and

now being the minister responsible in government, I know for sure that if we [government] try to come up with the ideas, we wouldn't come up with a tenth of them compared to you [businesses working with LORCA].

"This center will be home to startups that are on missions in so many different ways," he added, "and mission-led businesses are the ones who are going to solve problems for other people in the future."

Hosts with the Most

As hosts of the scheme, Plexal will play a central role in maintaining and developing the center's objectives, bringing its specialism in helping high-tech startups in artificial intelligence, augmented reality and the Internet of Things.

Lydia Ragoonanan, director of LORCA, tells *Infosecurity* that Plexal's opportunity to run LORCA is the result of an incredible collective effort to make the UK the safest place online and grow the impact and number of the nation's most promising cybersecurity companies.

"We are thrilled to have the opportunity to support this goal," she adds. "The team has significant experience in designing and running impactful innovation programs that help companies scale and bring their solutions to new markets. We are particularly skilled in molding and

matching emerging innovators who have solutions to large companies' challenges."

The Plexal City at Here East is a 1.2 million sqft digital and creative hub, designed as a 'mini-city' – a hyper-connected campus combining specialized innovation services with state-of-the-art work and event facilities to support digital entrepreneurs.

"The center will be joining Plexal's community of problem solvers including entrepreneurs, big business, academics and investors who are focusing on collaboration and commercialization to help refine and scale innovations of the 4th industrial revolution," continues Ragoonanan.

Key Collaborations

An element that is going to be pivotal in LORCA's success is collaboration, and Plexal has two particularly strong partners in CSIT and Deloitte.

CSIT will deliver cutting edge academic research insights and engineering resources, explains Dr Godfrey Gaston, CSIT director and LORCA executive board member.

"Since 2009, CSIT has spun out and supported a number of cybersecurity startups, collaborated with numerous others on research and development projects and has a track record of working with large companies such as Thales, BAE Systems, Allstate, and others on significant contract R&D engagements," he says.



There are 11 startups that have graduated from the CSIT Labs program in just the last couple of years with a further five enrolled in 2018, and CSIT is a cofounding member of the Global Ecosystem of Ecosystems Partnership in Innovation and Cybersecurity, which now represents 21 members in 13 countries across North America, Europe, Asia and Oceania.

"CSIT brings all this cybersecurity innovation expertise, global market insight and connectedness to the initiative," Gaston adds.

With the academic and research approach covered by CSIT, it is the cyber team at Deloitte that will support LORCA innovators and markets through a global client base.

"Also, as one of the world's largest cybersecurity consultancies, Deloitte will bring domain expertise to amplify the impact of LORCA members," providing committed access to smart-connected cyber people, data and facilities, adds Stephen Wray, director of cyber innovation at Deloitte.

Gov Gets Going

There's also the significant involvement that the UK government will have, and whilst the investment of £13.5m is substantial, funding will not be the only government-linked ties LORCA will benefit from.

Robert Hannigan served as director general of GCHQ between 2014 and 2017, and is now the chair of LORCA's

industrial advisory board, a role in which he works with a group of international peers to provide strategic perspective on the future needs of the cyber industry and advise how companies coming into the sector can meet them.

"The government's ambition is to make the UK cybersecurity industry dynamic, export-orientated and a place that people want to come to to start new companies," he tells *Infosecurity*. "They're keen that the various incubators and centers across the country should work together and get critical mass, which is another role of the London center."

What a Start!

There's no doubting that LORCA provides a fantastic opportunity for startups, particularly because the six-month programs it offers are uniquely designed to fit the individual needs of the companies taking part.

"Every entrepreneur's journey is different," explains Ragoonanan, "and so we are offering a bespoke program of support to help hasten the speed to new market and provide insight on how to grow successfully."

"Organizations may need support around how best to reach new markets, or to grow their team, to prepare for Series A or for further funding."

One of the first companies joining the scheme is Ioetec, whose mission is connecting users to their IoT devices securely and ensuring they remain safe.

"Our target is giant commercialization, so that Ioetec becomes ubiquitous and immediately associated with safe, secure IoT communication," says CCO John Tolhurst. "LORCA will accelerate the process to achieve those ambitions. LORCA is a high-profile initiative offering Ioetec an almost unique opportunity to open doors that would otherwise be hard to open."

"During these six months, we'll secure those early projects and relationships, win new customers and seed investment to ensure we are able to capitalize on this opportunity and outrun our competition."

For Cybershield, a security startup focused on stopping phishing attacks and alerting employees about deceptive emails, and another of the first LORCA intake, access to a strategic partner such as Deloitte will prove invaluable in understanding and catering to the needs of enterprise customers.

"We are already finding the program is advancing our capabilities," explains Paul Chapman, co-founder of Cybershield, "and we hope to have a number of customers signed up for Cybershield's solution 'Sentry' by the end of the program."

Opportunities for All

It's not just startups that can benefit from involvement with the center though. There are a variety of opportunities for other parties too.

"Large organizations who have cybersecurity challenges are welcome to become partner members," Ragoonanan explains, "and there are a number of partnership options available that will enable organizations to have direct contact with innovators who have possible solutions, attend networking events and have a presence at our annual event."

"Finally, we have a Finance Forum that is convening the investment community. This Forum will have direct access to some of the UK's rising cyber stars."

In its first three years, LORCA aims to bring in £40m worth of investment for the supported innovators and create up to 2000 jobs, highlighting just how much of an impact it hopes to have on the security industry, both in practical terms and in fostering a generation that aspires to create the next best startup or product in the UK



Matt Hancock (4th from left) with several members of the first LORCA cohort

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



BLACKDUCK
by synopsys

 egress

 ipswitch

LastPass...

 ManageEngine

 mimicast

 SailPoint

 STORMSHIELD

 TITANIA

 tripwire

 WhiteSource

DIDO HARDING

You can't hear Dido Harding's name without thinking about the TalkTalk breach. Three years on, in her new role at the NHS, a member of the House of Lords and a non-executive director at the Bank of England, Baroness Harding is leaving the past in the past and using her experience to make a difference in the public sector

By *Eleanor Dallaway*

➔ How do you feel about 'the breach' three years on?

I no longer think about it every day, but it's impossible not to still feel emotional about it. We made a conscious decision to be open and honest and once you've done that, you can't go back. I feel like it's my responsibility to share what I learnt. Part of me feels quite good about it. TalkTalk acted well and honorably towards our customers. So many talking heads and CEOs thought we were doing the wrong thing, but organizations need to be more open and honest and that will create less of a taboo.

➔ In hindsight, what would you have done differently in response to the breach?

I wouldn't have spent half a day negotiating with Met police about getting data back. Also, going out with the news late at night created more noise and panicked people – I regret that. Of course I wish it hadn't happened, but there's no point in wishing things had been different. Instead, we need to focus on what we learnt.

➔ What positives can you take from TalkTalk?

One of the privileges that came from the breach was getting to meet some of the best minds in the industry and getting explanations that I didn't get before. I loved running TalkTalk, despite the ups and downs. The next phase is taking what I'm good at – guiding large consumer-facing organizations through technology driven change – and using it to help the public sector.

➔ Quick-fire Q&A

Who does the ultimate responsibility lie with when a company is breached?

The chief executive. I was pushed to blame someone else but I knew it was just me.

What is one of the most important considerations when a company is breached?

Go public very quickly to increase your chance of weathering the storm. You always need a plan.

What advice would you give to CISOs for presenting risk to the board?

Get better at speaking truth to power. Be braver and speak in plain English.

As a CEO, what concerns you the most about cybersecurity?

Cybersecurity teams that say everything is OK. Really good people are always slightly dissatisfied and think they can do better.

Should CISOs report into the board?

Sitting on the board isn't the be all and end all. Boards need to be reasonably small to function best. You want a CISO reporting into the board.

BIO

➔ Dido Harding spent seven years as chief executive of TalkTalk, leading the telecoms company through one of the UK's most high-profile cyber-attacks. As one of the UK's most well-known digital leaders, Dido became a Conservative Life Peer in 2014, serving on David Cameron's Business Advisory Group. She now works as chair of improvement at the NHS.

<div>EXPLOIT</div> <div>FREE</div>	<div>COMPUTER FRAUD</div> <div>\$2200</div>	<div>CHANCE</div> <div>?</div>	<div>CYBER-EXTORTION</div> <div>\$2400</div>	<div>HACKER TRAINING</div> <div>\$3000</div>
<div>MONEY LAUNDERING</div> <div>\$2000</div>		<div>DARK ECONOMICS</div> <div>?</div>	<div>INTERNET SERVICE PROVIDER</div> <div>\$1500</div>	
<div>BOTNETS</div> <div>\$1600</div>			<div>KEYLOGGING</div> <div>\$1400</div>	
<div>REQUEST</div>	<div>BAIL</div> <div>JAIL</div>	<div>VIRUS</div> <div>\$1200</div>	<div>ID THEFT</div> <div>\$1000</div>	<div>CHANCE</div> <div>?</div>
				<div>DDoS</div> <div>\$1000</div>

EVOLUTION OF THE CYBERCRIME-AS-A-SERVICE EPIDEMIC

As global cybercrime continues to generate huge revenues annually, *Phil Muncaster* investigates the rapidly developing role of the as-a-service model



INCOME
TAX



PAY \$200

MALWARE

\$800

TREASURE
CHEST



RANSOMWARE

\$600

COLLECT
BITCOIN AS
YOU PASS



INTERNET
ACCESS TAX



PAY \$100

EXPLOITS

\$10,000

REMOTE ACCESS

\$7000

PHISHING

TARGET SELECTION

\$1500

\$4000

\$4000

They used to say “crime doesn’t pay.” Well, the new reality of global cybercrime is very different. A thriving underground economy of buyers and sellers, tech experts and novices has evolved over the past decade to the point where global cybercrime revenues today are estimated at anywhere between \$600bn and \$1.5tn per year. Cybercrime is highly professional and organized, holding a dark mirror up to the ‘real world’. It’s also an economy that is, to an extent, fueled by the continued inadequacies of corporate and home security.

dark web. A 2018 Center for Strategic International Studies (CSIS) report sponsored by McAfee claims a figure of \$600bn (0.8% of global gross domestic product - GDP), up from \$500bn in 2014 (0.7%). A recent Bromium report written by Michael McGuire, senior lecturer in criminality at the UK’s University of Surrey and titled *The Web of Profit*, points to a sum of more than double that: \$1.5tn, which is equal to the GDP of Russia.

A separate study into the Cybercrime-as-a-Service (CaaS) phenomenon by MIT researchers cites figures claiming

in smaller, more manageable skill-sets,” the Europol report continues. “When they require something outside their own area of competency, they need only to find someone offering the appropriate tool or service in the digital underground.”

So what exactly is on offer as a service? According to that MIT report, *Cybercrime-as-a-Service: Identifying Control Points to Disrupt*, no part of the cybercrime value chain has been left untouched. That means everything from vulnerability discovery and exploit development, to deception and obfuscation, payloads, security checks, payload repackaging, botnets, traffic redirection, bulletproof hosting, reputation escalation, target selection, domain knowledge, money laundering, mule recruitment, reputation, value evaluation and even hacker training.

From threats to infrastructure and human support, no stone has been left unturned by the vast underground cybercrime economy. Here the ‘customer’ experience is king, competition can be intense and prices fluctuate according to demand. The Bromium report claims zero-day iOS exploits can sell for as much as \$250,000, while SMS spoofing will cost you just \$20 per month, for example.

The Platform is King

It’s also an economy spread across larger multi-national ‘organizations’ that can pull in profits of over \$1bn, to smaller ‘SMEs’ where returns of \$30-\$50,000 are more likely, according to the University of Surrey’s McGuire. So-called ‘platform capitalism’ is at its heart, with those larger players the providers and facilitators of CaaS. McGuire tells *Infosecurity* there are three main dangers associated with this trend.

“Firstly, for cyber-criminals, it is a much more efficient method of making money and they know this. Secondly, the risk of being caught is reduced as they are not directly committing first order crime. This makes it much harder for police to intercept, or even disrupt cybercrime channels, so the bigger operators are getting away with committing crime, while a couple of the lower level guys may get caught,” he explains. “Finally, legitimate platforms that were built before the sophisticated tools of today were developed have gaps in their security, which criminals can exploit. There is a lot of evidence to suggest that these legitimate platforms are being abused by cyber-criminals.”

From Facebook to Amazon and Uber, these data-driven platforms have not only proved the inspiration for the underground CaaS model, but are also valuable channels in their own right: for cyber-criminals to acquire data, spread malware, launder money and

“For cyber-criminals, it is a much more efficient method of making money”

Over the past few years, the as-a-service model has both broadened and deepened the overall cybercrime threat, “productizing malware and making cybercrime as easy as shopping online,” according to Bromium CEO, Gregory Webb. Exactly what role does it play today, how is it evolving and what hope do we have of disrupting or mitigating the threat it poses to organizations?

Democratizing the Threat Landscape

Experts aren’t yet agreed on the size of the underground cybercrime economy, which isn’t surprising when one considers that much of it operates on the

cybercrime generated revenues of \$3tn in 2015 and further, is on track to hit a staggering \$6tn by 2021.

What they can agree on is the fact that the as-a-service model has become an increasingly important component of the underground cybercrime economy, democratizing the means to launch attacks so that even those with few technical skills can grab themselves a piece of the pie. Europol’s 2017 *Internet Organised Crime Threat Assessment (IOCTA)* explains how, unlike any other type of criminality, cybercrime allows novices to “rub virtual shoulders” with veterans.

“Instead of even attempting to learn everything, cyber-criminals specialize





much more. A recent investigation by journalist Brian Krebs revealed over 100 private discussion groups on Facebook that had been facilitating cybercrime and fraud for years. It took an estimated two hours for him to find them, which raises question marks over the social network's commitment to security on its platform.

Disrupting the Disruptors

So is there any way the white hats can hope to fight back? The CSIS/McAfee report cites law enforcement estimates that although cybercrime is massive, "a

so when one market is disrupted, another quickly appears," he tells *Infosecurity*. "The second is that they are as fast or faster at adopting new technologies as the defenders, and use it to generate new 'products' very rapidly. Tor and cryptocurrencies help criminals deal with some of the trust problems. I wonder sometimes if law enforcement efforts are too much like a game of whack-a-mole."

So is the only effective way to combat the unstoppable force of cybercrime simply to improve baseline corporate security across the board? After all, make yourself a harder target and, even with the low barriers to entry afforded by the as-a-service model, the ROI from attacks becomes less attractive to the criminals.

SANS-certified instructor and founder of Open Security, Matthew Toussain, agrees that "organizations must become their own first line of defense," arguing that law enforcement is by its very nature too reactive at times.

"Today, proactive defenses are necessary. Understanding the risks inherent in one's own network is a required

first step; information security assessments help to solve this shortcoming," he says.

"The next strategic factor for organizations to focus on should be the attack types preferred by actors in their threat model," Toussain continues. "Often these attacks include DDoS, exploitation and ransomware. Solid network defenses and the ability to restore critical systems from backups are key components of any defensive posture here."

The bottom line is that as long as there's money to be made from

much smaller number of individuals may be responsible for the bulk of the most significant cybercrime offerings." This would seem to make disruption by police a plausible way to tackle the CaaS epidemic.

In fact, there have been some notable successes. Earlier this year, Europol trumpeted its takedown of webstresser.org, thought to be the world's largest DDoS-for-hire platform. Trend Micro has also had success, teaming up with the UK's National Crime Agency in an operation that led

"There is a lot of evidence to suggest that these legitimate platforms are being abused by cyber-criminals"

to the conviction of an individual responsible for selling crypting and Counter Anti-Virus (CAV) services. Its work with the FBI also saw two of the ringleaders of the notorious Scan4You CAV platform brought to justice.

However, James Lewis, director of the technology and public policy program at the CSIS, is pessimistic.

"There are two dilemmas: many of the best criminals operate out of sanctuaries,

cybercrime, and the platform capitalism model continues to function largely undisturbed, there will be no end to CaaS. While the information security industry can help, support and publicize those law enforcement wins when they come, a bigger impact will arguably come from simply improving corporate cybersecurity around the world. There are few quick wins in a long-running battle like this



The Bigger Picture

Unfortunately, the growth of the cybercrime economy is most likely having a major impact on rising global crime rates. Bromium's *Web of Profit* report claims that around 20% of revenue or \$300bn is reinvested annually in activities including drug manufacture, human trafficking and terrorism. For example, the arrest of a Dutch money laundering gang led to the discovery of equipment used to make ecstasy. Meanwhile, one British-born Al-Queda follower is said to have made \$3.5m from card fraud.



That's not to mention the large sums of revenue reinvested into cybercrime ventures. Larger cybercrime gangs are said to plough money back into expanding their operations; this could include buying more crimeware and infrastructure, paying money mules or investing in more technical support and human resources. The continued growth of the industry has also been a boom for nation state hackers looking to take shortcuts, says the UK's University of Surrey's Michael McGuire.



MARTHA LANE FOX

Baroness Martha Lane Fox may be best known for founding Lastminute.com but this is only one of her many impressive accolades. She's an active crossbench peer, serves on the board of Marks & Spencer, Twitter and Channel 4, was appointed as the UK's Digital Champion and has co-founded Doteveryone, Antigone and LuckyVoice. Despite these professional achievements, she considers learning to walk again her proudest accomplishment

By *Eleanor Dallaway*

➔ Is it harder to make it as a woman in technology?

It's hard if you don't have the resilience. As a woman, you get shit (sic) all the time. It's no wonder that women don't feel the industry is for them. The tech industry is becoming more dominated by artificial intelligence and Blockchain and this is going to make the gender issue worse. It's not that women aren't technical or able, they just often haven't gone into those disciplines, and we don't have the plans or interventions to make sure the [gender gap] doesn't get worse. Look at the products of some of these technologies; at families shouting instructions at Alexa, a woman's name. This takes us backwards, it's not OK.

➔ You recently keynoted at Infosecurity Europe, what one key message did you present to the audience?

That I'm a technology optimist, not a tech utopian. For every challenge we face, we can use technology to improve the outcomes. We need to keep humans at the heart of this though, we need to help legislators and individuals understand technology better. We're moving away from humans – but just because we can, doesn't mean we should.

➔ If you'd set up Lastminute.com in 2018, what would you have done differently?

Technology is so unimaginably different now. We built a business without Google or Facebook so today we'd have to use those platforms. The travel industry has changed so much. We made mistakes all the time, it was basically chaos.

➔ What are you most proud of?

Learning to walk again [after being severely injured in a car accident in 2004]. In a professional sense, I'm most proud of the work I did in government. The opportunity to establish a new government department was an extraordinary experience. I loved working in the public sector – I have a strong sense of public service and always wanted to be an MP to contribute to society.

➔ Do you think much progress has been made in terms of digital literacy?

There is a recognition of the digital skills issue, but not enough has been done for the digital divide. It's easy to help people learn a checklist of things, but much harder to help people understand technology and be empowered by it. People still don't understand. There needs to be big public campaigns and more and better legislation.

BIO

➔ Martha Lane-Fox co-founded and led lastminute.com. Martha was appointed the UK's Digital Champion by Prime Minister David Cameron with a remit to bring every UK citizen online and help them develop vital digital skills.

04-06 JUNE 2019

SAVE THE DATE FOR INFOSECURITY EUROPE 2019

EVERYONE AND EVERYTHING YOU NEED
TO KNOW IN INFORMATION SECURITY

infosecurity®

EUROPE

04-06 JUNE 2019 OLYMPIA LONDON

"It's great for networking,
seeking out specific
companies to speak with and
also for high-level overviews
of new companies."

Becky Pinkard VP Intelligence,
Digital Shadows Limited

KEEP IN TOUCH WITH
EVERYTHING INFOSECURITY

   @Infosecurity #infosec19



Kevin Mitnick's reputation precedes him. *Eleanor Dallaway* meets the man known as the 'world's most famous hacker' and finds that there's a lot of smoke and mirrors around Kevin and his mind-blowing journey from villain to legend

KEVIN MITNICK



Kevin Mitnick and I meet at the W Hotel in San Francisco. After 12 years writing about information security, meeting the 'world's most famous hacker' is actually a really big deal. I've heard so much – some good, some bad – about the man who had the FBI running in circles and who spent a year and a half in solitary confinement, so I am uncharacteristically nervous as I wait for Kevin.

Within a minute of shaking his hand, however, I feel completely at ease. Kevin is warm, friendly and admirably candid. It's just the two of us, no nervous PR person waiting to tell him to slam on the breaks if he says too much. It's just Kevin and his hypnotic tales, and me, wide-eyed and captivated by his story.

The first thing I ask him is who is 'the real' Kevin Mitnick and interestingly he responds with what he is passionate about rather than what he considers himself to be – perhaps in Kevin's mind, the two are intrinsically linked. "I'm extremely passionate about technology and I started hacking from my love of magic and doing tricks for friends and family," he tells me.

Growing up in LA, Kevin recalls days on end of watching the sales guys in the local magic store doing tricks for customers and observing them until he learnt their secrets; a necessity "because I couldn't afford to buy the tricks," he explains.

In the 1980s in high school (Kevin was born in 1963) Kevin's love of magic segued into the hobby of phone phreaking. "I met this kid who could do magic by hacking a phone network with an ordinary phone and I got hooked on understanding how it worked." It was innocent, he insists, but admits that he later learnt that his antics cost "some poor company somewhere. It was wrong, but I didn't know," he says.

Not all of his 'victims' were completely accidental, though. "There was a guy

who really annoyed me one day, so I reprogrammed his phone remotely so that when he called his saved numbers, he actually got through to Weight Watchers LA, Weight Watchers San Francisco, Weight Watchers New York," he laughs. It's the first glimpse I've had into Kevin's exceptional sense of humor and love of mischief.

Later in our conversation, he tells me about a McDonald's prank where he remotely took over the drive-thru windows. "When a customer drove up, rather than getting the guy with the headset ready to take their order, they'd get me, but obviously they wouldn't know that. I'd say something like "As you're the 100th customer today, your order is free so please drive forward," he laughs.

"I'd actually be hiding across the street and would wait for overweight people to put in their order of Big Mac, fries, coke, apple pies... and I'd say 'based on the make, model and weight of your vehicle and the weight of your occupants, I suggest you change your order to the McSalad.'" He's laughing, I'm laughing and I'm captivated by his stories.

"Magic, Like Technology, is a Tool"

A friend of Kevin's suggested he take a computer class in high school, despite his apparent lack of interest, but when he spoke to the computer science instructor he was told he was "below the requisite for the class" as he was lacking credits in physics and calculus as a freshman. The instructor soon changed his mind when Kevin demonstrated that he could fix a problem the tutor was facing: having no phone number in the lab for his wife to call him on. After Kevin got a number for him, he was permitted entry.

The random serendipity of this tale blows my mind. Imagine the paths that

Kevin could have taken if that one friend hadn't persuaded him to inquire about the class, or if the instructor had not accepted the bribe. Having said that, his passion for technology would surely have led him down a certain path at some point.

Kevin started to write code at 16, reading manuals and spending a lot of time at California State University, Northridge "because they had all the manuals for all the computer systems." At that stage, Kevin wrote code to run on the terminal in the computer lab that simulated the computer. "It was like the first phishing program – it tricked users into giving up their password."

When the teacher logged into his computer, he actually logged into Kevin's program. "I took his password, logged in, and just had a huge smile on my face that it worked." That same week, Kevin ran out of time to do the official class assignment but when the teacher threatened to kick him out of the class, he said "I actually wrote a better program to steal your program." Kevin proudly recalls how the teacher beamed, declared it "cool" and patted him on the back. That program, Kevin considers, was "how it all started."

From that very first phishing attack that he engineered, Kevin insists that he never, ever had ambitions of financial gain or causing harm. He categorizes himself as a "funster," motivated entirely by 'trophy hunting'.

"It was my playground and it's what I did instead of playing basketball. I wanted to conquer the Mount Everest of hacking – I wanted to have access to all phone company computers throughout the United States and I decided to go after the NSA from the computer lab in high school."

You'd be forgiven for questioning whether hacking the National Security Agency could ever be truly considered

the behavior of a “funster,” but sitting across from Kevin, there’s something about his openness, his candid words and his wide eyes that make me believe that he at least totally believes what he tells me.

“Magic Lies in Challenging What Seems Impossible”

It may have been the hacker’s equivalent of climbing Everest but Kevin, at the age of 17, successfully wiretapped the NSA. “I compromised the phone switch to allow me to listen in to their conversations, which I did for about 10 seconds.

“It wasn’t about listening,” Kevin insists, “I couldn’t care less what they were saying, it was just about capability. I was setting myself seemingly impossible goals but managing to carry them out.” Back then, Kevin recalls, there was no law against computer crimes. It’s therefore unsurprising that the first time Kevin “got into trouble” was not for a computer crime, but for burglary, in the form of a social engineering attack carried out by him and a friend who gained entry to a phone company building to access their computer systems manuals.

Years later, Kevin’s attorney told him that his earlier antics were used to convince Congress to pass a law to criminalize computer crime. “It surprised me because I never viewed myself as a criminal, just a prankster, but as they started to criminalize this stuff, I just thumbed my nose; I was hooked so I decided to continue.” A decision he now considers “both stupid and incredible” and that landed him “in a whole boat load of trouble.

“It was a vicious cycle. I got busted, did it again, got busted, did it again. In a way, I still do it today...but now I just get permission from my clients and get paid.” I ask him whether he was addicted, whether the hacking was a result of an addictive personality. He considers this and eventually settles on a response: “I couldn’t stop because I was totally hooked.” In my book, that’s an addiction.

He was first prosecuted as a juvenile, but recollects how the press didn’t go as easy on him as the law. “They played me up to be a dark magician of cyberspace that could literally take over the world.” He tells me how *USA Today* superimposed his photo onto Darth Vader on its front cover, something that clearly and justifiably hurt him.

“I had made a very bad decision to hack into telephone company manufacturers that made phones like Nokia and Motorola at the time. I wanted to get access to the firmware, go after the source code and get the secret recipe on the chip.” He insists this was not an espionage attack, but merely a case of curiosity. He then uses a line

“I wanted to conquer the Mount Everest of hacking”

which he repeats multiple times during the interview: “I just wanted to understand how it worked.”

It was his 10 years of snooping in the Digital Equipment Corporation (DEC) network that eventually led to Kevin being caught by law enforcement. A decade after he first gained access, the computer manufacturing company released a new operating system called VMS. “One of my hacking friends and I wanted to get the VMS source code to analyze, find flaws and become better hackers.”

DEC engineers realized they had a hacker when Kevin and his friend transferred the VMS system source codes to USC in California. “This started a war – their tech engineers versus me. They thought I was a team from Russia, they’d keep knocking me off their network and I kept breaking us back in.”

Things went sour when Kevin had a falling out with his hacking friend who decided to turn them into DEC. “He was an idiot because he got himself convicted of a felony. He didn’t go to jail but basically that’s how they got me.”

“A Little Magic Can Take You a Long Way”

The consequence of this desire to understand how things work landed him in very serious trouble with the law.

“I started compromising all the Bell operating companies in the USA. That’s when I wanted to gain control of the entire United States just for the challenge and the trophy.

“What really pissed the FBI off is that when they traced the calls I was making, I had them routed to some random business; they’d serve a search warrant, but of course, they’d find nothing and they’d then have a lot of egg on their face because I was playing with them.” He reflects on this as “a lot of fun” and considers that “it was like injecting myself into a TV show. I was playing cat and mouse with the government and I didn’t realize that what I was doing was crazy.”

As the cat and mouse game intensified, Kevin left Vegas for the Rocky Mountains with only one suitcase filled with \$5000. He officially became a fugitive.

Landing in Denver, Colorado, Kevin looked at job advertisements and tailored his resume 95% to match his applications. “Through my ability to control the phone network, I set up phone numbers to various pay phones so I could give myself references.” The name he gave himself was Eric Weiss, the real name of Harry Houdini and a

nod to his passion for magic and his mischievous nature. Under this cover, Kevin got a job at a law firm in Denver as a system operator.

Kevin knew the government were monitoring his family, so used his ability to control the phone network to maintain communication with his mum and his grandmother when he was on the run. “We got pagers, we had a list of 20 casinos in Las Vegas and we had a code to say ‘emergency’ or ‘call when you can’. There was no way in hell they would be able to trace the call because I knew exactly how long it would take to trace.”

Being apart from his family was the hardest thing about his fugitive years and the thing that he later tells me is his biggest regret.

“The way I was able to psychologically deal with being a fugitive was to pretend I was an undercover operative on an assignment, I adopted a cover identity, I became an actor,” he admits.

“Disbelief in Magic Can Force a Poor Soul into Believing in Government and Business”

After a well-publicized pursuit, the FBI arrested Kevin in 1995 at his apartment in North Carolina, on federal offenses related to a 30-month period of computer hacking, which included computer and wire fraud.

Kevin served five years in prison, including over a year in solitary confinement in 1989. When writing about his past shenanigans in one of his four books, *Ghost in the Wires*, he says “putting it all onto paper, I’m actually surprised I only got five years!” He explains to me that he has always separated his various hacking incidents in his mind, but when he looks at the past 20 years as a whole, “I think ‘oh my god, no wonder I was public enemy number one.’”

He says that without doubt, solitary is the hardest thing he has ever done. “I was in a high security prison with killers. They’d let me out – in handcuffs – for an hour a day. It was a very scary time and I spent every day thinking there’s no light at the end of the tunnel.”

I’m curious as to how a hacking case resulted in solitary. All these years later, Kevin seems equally as bemused. “I thought I’d get out on bail,” he remembers. After all, it was a hacking case that involved no money. “I ended up in federal court. The prosecutor said not only do we have to hold Mr Mitnick without bail





because he's such a great danger to national security, we also have to make sure he can't get access to a phone."

The judge, who Kevin recalls was in his seventies and had probably never used a computer, believed the prosecutor's insistence that Kevin, with access to a phone in jail, "could call up NORAD, whistle into the phone and launch nuclear weapons." As a defendant, Kevin committed the ultimate mistake – he laughed at the judge in court. "He got really pissed at me laughing, but this claim was ridiculous. How could a grown man say something so stupid?"

The prosecutor, insisting that Kevin had the capability to start World War III, ordered that he be held in solitary without access to a phone. "I was in solitary for a year based on this myth that I could whistle the launch codes."

Assange and Snowden, he eventually settles on himself for that title. "I guess it fits," he grins. I ask him whether he considers himself a black, white or grey hat and after giving it extensive thought he says "I guess I fit all three."

Today, Kevin runs Mitnicksecurity.com, a penetration testing and red team consultancy, and he does a lot of the work himself – again due to his perfectionist nature. "If a client hires me for a week and I don't get in, I'll spend an extra week at my own expense because I never ever give up."

Kevin is also a 50% partner in KnowBe4, a security awareness training company. Through a chance encounter with KnowBe4 founder Stu Sjouwerman, Kevin learnt about the company and was keen to accept Stu's offer of a partnership. Now with series A and series B investment, KnowBe4 is going from

surreal," laughs Kevin, clearly very aware of the irony. Almost as ironic as the fact that both the FBI and NSA have hired Kevin to speak at events.

His public speaking takes him around the world – despite his fear of flying – and rarely gives him time at either of his LA or Vegas homes, which is why he takes his girlfriend wherever he goes.

"Always being on the move" is one of the positives he takes from his fugitive days. "I really like the lifestyle of just moving around," he explains.

Public speaking is something he loves doing and Kevin draws parallels with his dream of being a magician. "When I'm on stage, I'm demonstrating exploits and how the bad guys practice their trade craft. I'm a performer of hacker magic." When I ask him what the future holds for him, he tells me that he plans to build out his public speaking business even further because he adores performing.

All of his friends, he says, are magicians. "Like David Copperfield," he casually adds, "oh and Teller from Penn and Teller. I know him really well, he calls me for advice on hacking." I tell Kevin that I too love magic. "Want to see a trick?" he grins at me. His trick is actually very impressive and we spend some time talking about what it is about magic that captures us.

His other passions include travel, going to the movies, jet skiing or wave running and reading, but mainly books about computer research and information security.

"You Have to Make the Magic Happen"

I want to end our time together not by focusing on Kevin's misdemeanors, his regrets or his darker days, but instead on what he looks back on with warmth and pride.

"I started off in this world as a hacker and got myself into a lot of trouble, so being able to turn that around to being a respected security expert, a successful business man and a *New York Times* best-selling author, makes me very proud," he says.

He compares his story to that of Frank Abagnale of *Catch Me if You Can*. Again, his obsession with illusion, with magic, with pretending to be someone he's not is apparent. It's fascinating, but resisting the urge to psycho-analysis, I am pleased that Kevin seems legitimately happy and largely at peace with his past and regrets.

It was magic that led Kevin to become the world's most famous hacker, and all these years later, he is still utterly hooked on the magic of magic. I wonder where it will lead him next.

It took me 12 years as an information security journalist to meet Kevin, and it was very much worth the wait ●●●

"When I'm on stage, I'm demonstrating exploits and how the bad guys practice their trade craft. I'm a performer of hacker magic"

Kevin is adamant they had no genuine belief that this was true, "They just did it because they were annoyed I'd made a fool out of them."

"Magic Becomes Art When it Has Nothing to Hide"

Kevin says he hugely regrets the trouble he got into for two reasons. "Firstly for causing a bunch of hassle for all my victims, and secondly for the hardship I caused my family in dealing with my antics for all those years."

He's emotional when he talks about his family. "My mother and grandmother were so supportive of me no matter what happened and what I did. My grandmother passed suddenly and my mum was fighting lung cancer for five years." Luckily Kevin was out of prison when she passed away, "but I still feel awful because of all the time I lost as a fugitive. I wish I could go back in time."

Even given the luxury of time travel, however, complete redemption seems unlikely. Kevin, whether willing to use the word 'addiction' or not, was unquestionably hooked on hacking and striving to become the absolute best.

His website calls him "the world's most famous hacker" and I ask him whether this is true. After considering Julian

strength to strength. "My whole life I have never been unsuccessful at compromising a target, so I liked Stu's idea."

At the time, Kevin had been working on an idea for security awareness videos with actor Kevin Spacey. Wide-eyed, I ask him to expand. "He actually got in contact with me because he wanted to make a movie about my life, so we went to lunch a couple of times but I told him I couldn't do the movie because I was under a restriction with the federal government for seven years. He actually tried to get me to do it anyway, holding the money secretly to give to me later, but I didn't trust him, so I said no."

"The Real Secret of Magic Lies in the Performance"

Kevin doesn't take being the world's most famous hacker lightly, investing a lot of time into continuing his hacker education. "I'm a public speaker so to keep up-to-date with the trade craft I take week-long classes to beef up my skill set," he explains.

"After a keynote I gave, all these people queued to take photos and have autographs like I was a rock star," he recalls fondly, remembering that one 'fan' was an FBI agent who flashed his credentials in the photo. "That was

WHY ARE BREACHES GETTING

Despite increased budgets, better awareness and improved board buy-in, data breaches are not only becoming more common, but also more explosive. *Kacy Zurkus* asks why

Those who have been working in information security over the past decade or more have witnessed the evolution of the industry with the creation of positions such as the CSO and CISO to help strengthen enterprise defenses. While much has changed within organizations over the past several years, hackers and the vulnerabilities they are exploiting remain largely the same.

Although larger enterprises may have increased information security budgets and introduced better security awareness training, that's not universal, which is problematic in today's interconnected world. Some of the classic problems of passwords and failures to segment networks continue to create risks for companies that have not advanced their overall security posture.

For the most part, the vulnerabilities that have been used in many high-profile attacks are ones that have existed for a long time. They've been patched

and sometimes even patched again. Unfortunately, many organizations are not updating their software or operating systems, which is one reason why breaches are getting worse despite increased awareness of cyber-threats.

To Patch or Not to Patch

"A large number of vulnerabilities are because of bad patching practices," says Erika Powell-Burson, CISO, Bentley University. "It takes very little effort to exploit a vulnerability that hasn't been patched, and it shouldn't take a lot of effort for companies to patch their systems."

Some organizations aren't patching despite the understanding that patching helps to mitigate risks, largely because they are still running legacy systems upon which they are very dependent. Moving to next generation technologies takes time, and organizations have to weigh up the risk and reward. "In some cases, it isn't possible to move from legacy systems, and those systems are no

longer supported by the vendors. Plugins may not be compatible, which often means they can't bring systems up to speed without replacing them," Powell-Burson adds.

For those organizations that have upgraded, though, there remains the issue of constantly defending against the attackers. It's what Jamil Farshchi, CISO at Equifax, calls the 'problem of one'.

"Attackers only need to be right once, whereas organizations defending against them need to be right 100% of the time. As businesses grow, they inevitably introduce new technologies, larger attack surfaces and a greater number of digital assets – all of which present a number of new, enticing vulnerabilities for attackers to try to exploit," Farshchi says.

Given that today's adversaries can access data or other assets with relative ease, monetizing sensitive data has become its own business. Malicious actors are typically well-funded and have myriad motivations which all translates to not

WORSE?

only ample reason, but also resources and incentive, to try to break-in.

Where Are the Funds Going?

While organizations may be spending more on their security budgets, the last couple of years have seen the threat landscape evolve in ways that companies weren't prepared to defend against, such as with the advent of ransomware and cryptomining. "A lot of CISOs, rightly so, concentrate on protection," explains Bill Brown, CISO, Houghton Mifflin. "There's a balance to strike there that leans more towards resiliency than towards prevention and detection."

Criminals are not only stealing corporate assets but they've also leveraged the theft of machine time to mine cryptocurrency. "There has been a lot of nuisance attacks and password spraying where criminals might not be targeting an organization, but they find a soft

underbelly and see where they can turn a profit. Still, the largest factor is that the landscape that needs to be protected is getting exponentially wider," Brown adds.

One side effect of digitization is that the perimeter is disappearing, creating more risk through third and fourth parties. According to a new survey from CrowdStrike, 66% of global organizations have experienced a software supply chain attack.

"Everybody is moving to the cloud, so they might not know their third party and downline vendors, which is why they need a vendor risk management program," argues Powell-Burson. "Cloud may be – or in some cases is – safer, but just like anything, they need to check and assess what data is moving through. They have to do their due diligence by doing a risk assessment."

Often risk can be both industry- and company-specific, which can make it difficult for organizations to understand their own risk if they aren't doing a risk

assessment. "Healthcare is a huge target," something Powell-Burson learnt in her previous experience as the first CSO in a department of one at a hospital. "They are non-profit, and while some are bigger than others, many of their budgets are constrained."

Outside of the financial sector – where enterprises are shoring up their security with layered defenses in place – other sectors don't have a security methodology; whether it's securing the application lifecycle or policies from prevention to response.

Advent of the Automated Adversary

In the same way that defenders are relying on automation to expedite tasks, cyber-criminals are using automation to attack faster. "They can put on the same malicious offenses with great speed and depth. While AI is not a fully accessible tool for cyber-criminals just yet, its

“Attackers only need to be right once, whereas organizations defending against them need to be right 100% of the time”

weaponization is quickly growing more widespread. These threats can multiply the variations of the attack, vector or payload and increase the volume of the attacks,” according to *Security Intelligence*.

The ability to use technology to increase the scale and scope of their attacks gives cyber-criminals an advantage, particularly over companies that have not yet invested in automated tools. Even in these large scale attacks, the methods are – in the most part – nothing new. The technology only allows attackers to increase in scale.

As the attacks are fundamentally the same, Farshchi says: “Focus on the fundamentals and put operational rigor around people and processes rather than investing in the latest and greatest shiny new technology – things like asset management, patch management, network segmentation.”

Doing the fundamentals will stop the vast majority of attacks. It’s also important to keep in mind that despite the fact that many organizations have implemented these security tactics, there are still companies – some of which could be in an organization’s downline – that have not taken these basic steps to prevent attacks. “Attackers almost never need to do anything sophisticated or high-tech to breach a system. They look for the weakest link and try to exploit it,” Farshchi points out.

The People Problem

After much attention being drawn to the need for top-down support, there has

been progress with board buy-in.

“Boards always want to know how we are doing compared to our peers,” Brown says. Yet, down in the trenches, defenders are still fighting their greatest risk, which continues to be the people problem.

End-users are vulnerable because hackers are growing more sophisticated in their ability to impersonate human behavior. “The problem is that we make certain types of mistakes,” explains Ina Wanca, professor at NYU’s Center for Global Affairs and John Jay College of Criminal Justice and former director of cybercrime prevention initiatives at the Citizens Crime Commission of New York City.

“People get frustrated, they repeat passwords, and these behaviors are what hackers are leveraging, especially when using social engineering tactics,” Wanca adds. With the growth of social media platforms, it is easier than ever for hackers to figure out how to trick end users into clicking on links. In virtually every platform, users share a lot of personal information, not only about where they work and the position they hold, but also about their likes and interests.

“The attackers only need to spend a few minutes looking online at what people are sharing to then personalize and send a phishing email. We are creating our own risk, and in large part we don’t know about cognitive biases when we interact online,” Wanca says.

That’s bad news for the organization because in the end, it doesn’t matter

what technology they have as they still need humans to interact with it.

The data breaches that have occurred in the past year or two were the result of preventable human error, Wanca says. Mitigating the risk of human error goes back to awareness training, which in large part is a generic, one-size-fits-all process from which employees will zone out.

“A lot of the time the trainings are created for a large audience, which is dry. Given that each person exhibits an individual cognitive bias, security awareness training needs to be tailored to that personal bias. It needs to be individualized,” Wanca argues.

More effective training would look at each individual’s behavior to discern what exposes them when they interact online. In that way, the training can then focus on preventing cybercrime through promoting cyber-awareness by correlating risks with specific triggers in an individual’s behavior.

“Companies need to be aware that breaches will continue to occur because we are adding more devices to our networks. Data will be shared, transmitted through multiple devices, and different communication channels, and it is better to invest in training than in lawsuits or losses,” Wanca argues.

One of the most important things the industry can do to defend against current and emerging threats is to collectively come together as a security community and share things like intelligence, lessons learnt and strategies for success versus working in silos or as competitors.

“Everyone who works in security has had some sort of experience managing through incidents – and we all stand to learn something from each other,” Farshchi says. Atlanta for the Advancement of Security (ATLAS) is one such effort to bring CISOs together and to take a meaningful approach to sharing advice and expertise. As the whole is greater than the sum of its parts, partnerships, according to Farshchi, are paramount.

The largest data breach of 2018 affected Aadhaar with

1.1 billion

records breached, according to Barkly. Exactis ranked second with 340 million records stolen, and Under Armour came in third with 150 million records compromised.

In 2017 the number of data breaches hit an all-time high with

1579 breaches,

up 44.7% from 2019, according to the Identity Theft Resource Center.

IBM’s 2018 *Cost of a Data Breach Study* found that the average cost of a data breach globally is

\$3.86m,

with the average cost of \$148 per compromised record. On average, it took organizations 196 days to detect a breach.

Companies that suffered a loss of one million records faced losses of \$40m, according to the IBM study, while the cost of a ‘mega breach’ – in which up to 50 million records were compromised – was

\$350m.

Companies able to maintain a breach in fewer than

30 days

saved over \$1m. Those organizations with incident response teams reduced the cost of a breach by \$14 per compromised record.



» DEDICATED TO SERVING THE INFORMATION SECURITY INDUSTRY

IN PERSON, IN PRINT & ONLINE



VIRTUAL CONFERENCES

ALL THE BENEFITS OF A NORMAL CONFERENCE FROM THE COMFORT OF YOUR OWN HOME. QUALIFY FOR CPE CREDITS ON ATTENDANCE.



WEBINARS

KEEP UP-TO-DATE ON NEW TECHNOLOGIES, BEST PRACTICES, HOT TOPICS & ISSUES IMPACTING THE INDUSTRY. FOLLOW A WEBINAR AND EARN CPE CREDITS.



E - NEWSLETTERS

ALL THE NEWS, REVIEWS AND INDUSTRY DEVELOPMENTS FROM THE INFOSECURITY TEAM DIRECT TO YOUR INBOX.



WHITE PAPERS

DOWNLOAD FREE TECHNICAL ARTICLES GIVING YOU IN-DEPTH INSIGHT INTO SPECIFIC INDUSTRY ISSUES.

WWW.INFOSECURITY-MAGAZINE.COM

TOP TEN

Regulatory Monetary Penalties



01

Genesco

VISA issued a \$13.3m fine to Genesco after a credit card breach in 2010. The retailer claimed that the fines were unjustified and unenforceable under the law.

Source: *Computer World*



02

Advocate Health Care

Advocate Health Care paid \$5.55m for HIPAA violations relating to three reported data breaches.

Source: *Beckers Hospital Review*

03

The University of Texas

The University of Texas MD Anderson Cancer Center lost an unencrypted laptop and two USB drives affecting 33,500 people, and was fined \$4.3m.

Source: *HHS*

04

Computer Sciences Corporation

The Securities and Exchange Commission fined two former executives of Computer Sciences Corporation \$4m over NHS contract shortfalls.

Source: *USA Today*



DAN RAYWOOD

The Severity of Regulatory Fines



The fine issued to Facebook by the Information Commissioner's Office - the UK's data protection regulator - over the Cambridge Analytica scandal marked the first time that the ICO had handed out its maximum £500,000 monetary penalty.

The fines, which were added to the regulator's enforcement powers in 2010, had not reached the maximum amount in the previous seven years, but they did come close with penalties issued to NHS trusts, while Google avoided a major fine over data collected by its Street View cars in 2013.

Monetary fines often mark the final action regulators will take, normally preferring to take other action to work with the victim who reported the violation. However, now that we are in the era of GDPR - where fines could potentially reach up to €20m, or 4% of turnover (whichever is greater) - the amount of money being paid for infringements could get serious. With this in mind, *Infosecurity* looked at some of the highest regulatory fines when compliance gets severe.

05

The Feinstein Institute for Medical Research

The Feinstein Institute for Medical Research was fined \$3.9m when a laptop containing the details of 13,000 patients and research participants was stolen in 2012.

Source: Beckers Hospital Review

07

The Children's Medical Center of Dallas

The Children's Medical Center of Dallas was fined \$3.2m over lost devices and non-compliance with HIPAA.

Source: Careers Infosecurity

06

Fresenius Medical Care

Fresenius Medical Care reported five incidents in 2012 incurring a \$3.5m fine.

Source: Fierce Healthcare

08

The University of Mississippi Medical Center

The University of Mississippi Medical Center was fined \$2.75m over several unreported data breaches.

Source: HHS

**09**

Cardionet

Cardionet was fined \$2.5m after a laptop theft revealed insufficient risk analysis and management processes.

Source: Healthcare IT News

10

MAPFRE Life Insurance

MAPFRE Life Insurance was fined \$2.2m following the loss of an unencrypted USB drive containing 2000 personal details.

Source: Careers Infosecurity



THE MURKY MARKET FOR ZERO-DAY BUGS

With zero-day exploits now hot property among hackers and researchers, *Danny Bradbury* shines a light on the thriving online marketplace that has arisen as a result

EXPLOITS FOR SALE

Two decades ago, arms dealers focused on physical weapons like missiles, guns and ammo. Today's weapons include the digital kind. Zero-day bugs – information about security flaws in products that vendors have not discovered or patched – can be the keys to the kingdom, getting attackers inside sensitive systems. They are so important to some players that entire markets have developed for trading them online.

Researchers selling their zero-day bugs through these online marketplaces can earn some serious coin, says Stephen Sims, who teaches courses on advanced exploit writing at training company SANS and regularly sells his exploits through various zero-day markets.

The buyers in these markets are typically intermediaries such as boutique intelligence companies around the DC area that will purchase useful security flaws from researchers and then sell them on.

"They are known to buy research from you at a higher price. Their customers are typically government entities or arms of such," Sims says, noting an ethical trade-off: "Sales to these types of buyers can yield a much higher return, but your research may be used to attack others as opposed to remediation."

The Rise of the Zero-Day Market

Once you sell the bug, you are not allowed to talk about it with anyone and it could take up to six months to get paid, Sims explains.

Zero-day markets that enable researchers to sell their exploits for more money include Zerodium, the DC-based organization originally founded by French security firm VUPEN. Zerodium, which did not respond to interview requests, took the unusual step of publishing its security flaw price list in 2015. Since then, it has offered bounties including up to \$500,000 for bugs in Linux and BSD variants and \$1m for Tor browser vulnerabilities. Zerodium exists on the 'regular' internet, and its CEO has publicly asserted that it only sells the bugs to "major corporations and government organizations from western countries."

Some companies have stepped away from zero-day markets, warning that they are more difficult to navigate ethically than they were in the past. Adriel Desautels began his career as a zero-day finder by earning \$16,000 for his first vulnerability – an MP3 player exploit – in the early 2000s.

He later founded DC-based Netragard to buy and sell these exploits online, but found the market shifting. "The industry

wasn't mature enough and the players became grayer with their ethical boundaries," he says.

Netragard listed Italian cybersecurity consulting firm The Hacking Team, which evolved into a zero-day broker, as one of its clients. After someone attacked the Hacking Team and posted its secrets online in 2015, Desautels discovered that his client had been providing exploits to governments with oppressive regimes. Netragard apologized in a now-deleted blog post.

When he realized that he couldn't tell who he was really selling to, Desautels could no longer participate and left the zero-day brokering market altogether. Instead, he focuses on finding bugs for vendors.

A Lack of Regulation

Part of the problem is that these markets are not regulated, warns Lamar Bailey, director of security at Tripwire. "There are no regulations, especially no enforceable ones," he says. "The closest thing is an NDA that some companies make researchers sign before compensating them for their vulnerability disclosure. On the black market, it is a free for all and vulnerabilities are often sold multiple times to multiple people and organizations."

Regulation is difficult in a world where the products are digital and marketplaces can pop up in the internet's darkest corners. The advent of black markets for zero-day attacks is a good example. These markets include 0day.today, TheRealDeal, 0day.in, and L33ter (the latter selling drugs and other illegal items alongside its core line in digital exploits). They are less scrupulous in who they deal with.

"There are multiple examples of hoarded bugs ending up in exploit kits or ransomware"

Laurie Mercer, solution engineer at crowdsourced bounty company HackerOne, argues that the dark web markets are unreliable. "You very rarely find hacking kits and if you do it's quite obvious that it's a rip-off," he says. "So most of it now is these private groups and forums which are invite only and these secret, protected barriers around them, which is suspicious."

The secrecy and elitism of the high-end zero-day world makes it even more sensational for the media, but experts argue that the buzz around zero-day exploits is often overblown.

"The actual usage of zero-days is really very rare. Attackers will use the simplest, cheapest tool to get the job done. In most cases, that does not require a zero-day," says Ian Pratt, president and co-founder of virtual browsing security firm Bromium.

Nevertheless, the right type of flaw can generate significant rewards from the right buyer. A recent Bromium report on the cybercrime economy put an Adobe zero-day vulnerability at \$30,000 and a hitherto unfound iOS-busting bug at \$250,000.

Nation states invest in these bugs because they can be powerful weapons against high-profile targets, explains Sims. He cites Stuxnet, the malware used in the 2010 cyber-attack against Iran's nuclear fuel enrichment system, as an example. "Whoever was responsible for it burned four zero-days against one target and they got in and that campaign lasted a while," he adds.

Stuxnet is a good example of why governments are prepared to invest in zero-day exploits. Collecting them gives intelligence agencies the tools they need to get important targets in those rare instances when a simple commonplace exploit isn't enough.

The Dangers of Hoarding

Brian Gorenc, director of Trend Micro's Zero Day Initiative, which buys bugs from researchers, doesn't agree with

governmental bug stockpiling. "There are multiple examples of hoarded bugs ending up in exploit kits or ransomware," he says. "We believe bug hoarding by any group creates problems. Just because something is not public doesn't mean you're the only one who knows about it."

Perhaps the most famous of those incidents occurred in 2017, when an anonymous team of hackers called the

ShadowBrokers claimed to have stolen a collection of exploits from a hoard of NSA vulnerabilities. After failing to secure a buyer, they decided to publish the whole thing online.

Among the goodies was EternalBlue, an exploit that took advantage of a flaw in the Windows implementation in the Server Message Block (SMB), allowing attackers to create a rapidly-spreading worm. This resulted in the WannaCry ransomware, which overwhelmed Western networks and which the White House attributed to North Korea.

EternalBlue has since shown up in cryptojacking software, and researchers have ported three other exploits in the same leaked NSA weapons cache, EnternalSynergy, EternalRomans and EternalChampion, to other Windows versions.

US legislators have tried to address this issue. One introduced a 2017 bill – the PATCH Act – to strengthen the government's existing process for deciding whether to disclose zero-days that it finds. It doesn't seem to have gained much support, though, and more than a year later, the Bill has gone nowhere.

Vendors Need Deeper Pockets

If lawmakers won't act, perhaps vendors will. They don't like governments secretly hoarding their exploits. After the NSA hack, Microsoft's president and chief legal officer Brad Smith criticized the agency, likening the hack to the US army having missiles stolen.

Vendors that are serious about this issue should embrace market economics and dig deeper to reward security researchers, says Desautels. "You incentivize hackers by having vendors offering the same kinds of rewards for a zero-day that they would see in the real world. Vendors can afford it."

Incentives can happen in several ways. Vendors can pay researchers directly, or

they can issue a bug bounty through a crowdsourced bug discovery program, run by companies like HackerOne. These avenues offer peace of mind to researchers who want to know that their zero-day bugs will be used only to fix the affected products rather than attack them.

Bug bounty programs generally don't pay enough though, argues Sims. "Most of the bounties are on the web app side," he says, adding that these generate lower payouts.

Mercer says that the average payout from HackerOne is \$500, but adds that payouts follow power distribution laws and that there are some bounties for non-web bugs. In July, Intel made the biggest payout so far via HackerOne: \$100,000, for processor-related vulnerabilities linked to the first SPECTRE variant. This aligns with Sims' suggestion that bugs in browser kernels and hardware are the most profitable and the hardest to find.

An alternative route for researchers wanting to sell their zero-day bugs purely for remediation is to offer them to a 'white' zero-day market operated by a security vendor. Gorenc's Zero Day Initiative passes the bugs that it buys onto vendors. The company benefits from seeing those vulnerabilities first and building its own patches before the vendors get around to it. On average, Gorenc claims that Trend Micro can protect its customers 74 days before the vendor issues a patch.

"In just the first half of 2018, we've awarded more than \$1,000,000 to researchers," Gorenc says.

Steps Towards Structured Disclosure

Formalizing the rules for disclosing bugs may also help bring some transparency to the process of finding and paying for them by holding vendors more accountable.

In a report on software vulnerability disclosures, EU think tank the Centre for European Policy Studies (CEPS) recommended an effective policy framework for disclosure. One vehicle for this could be the proposed European Cybersecurity Certification Scheme under the European Cybersecurity Act, which would see companies certifying their products against standard cybersecurity measures.

Governments are unlikely to stop buying bugs if researchers keep selling them. After all, unless all governments agreed to do so, those that stopped hoarding bugs would quickly be disadvantaged. The direction of the zero-day market therefore depends on its capacity to reward researchers for selling zero-days to those that won't weaponize them. Ultimately, that comes down to the vendors' budgets, and the researchers' ethical boundaries

COMING TO NEW YORK

WHEN:
NOVEMBER 14 -15 2018

WHERE:
**JAVITS CONVENTION CENTER
NEW YORK, USA**

- Keep up with the evolving threat landscape and learn from end user speakers and inspirational thought leaders
- Earn CPE/CPD credits to further your professional education
- Solution showcases from global vendors
- Immersive learning experiences: live SOC, escape rooms and more
- Discover the latest solutions from innovative start-up companies
- Find your perfect match - network with new and existing peers

REGISTER NOW

www.infosecuritynorthamerica.com

   @infosecurity #infosecna18

How to Run an Effective Cybersecurity Awareness Program



Candice Carter

Team Lead, NASA Aeronautics Research Institute
Candice is a cybersecurity expert with over 15 years of experience in the areas of counter-terrorism, counter-intelligence and criminal cyber-investigations. She works at Imperva and is an assistant professor and chair of the MSC CyberSecurity program at Wilmington University.

Before building a security awareness program, it is important to document a baseline of security knowledge for the organization. This will allow you to identify gaps and measure the rate of success.

Most programs start as the result of an audit and compliance issue, therefore setting the tone of security awareness in the organization as ‘checking a box’. Moving from this and instead igniting a behavioral change entails security to become a core value of an organization.

Treating security awareness as a brand can be an effective method of delivering the message. Providing simple but impactful examples of security incidences that occur will keep the members of your organization engaged. Communicating at a relatable level that is consistent with other company messaging helps the organization embrace security into the culture. Security culture changes over time with training, workshops, newsletters, speakers and blogs; keeping the user community informed and aware.

To be effective in growing this long-term commitment to security requires the support of leadership at all levels. Use your leadership team to identify champions within each department of the organization.

The security champions are liaisons between security and the department to keep the lines of communication open.

It is important to give the organization a means of reporting security concerns without repercussions, for example, by using a mailbox. There is no single size of security training that fits all.

program. Reporting should clearly reflect a baseline and progression of results. The budget should correlate with what needs to be accomplished to close the gaps in awareness and training.

“Security awareness is critical in the success of an organization and should be part of the company’s culture”

The security champion concept brings the ability to curtail security awareness training specific to particular areas. Awareness works if the user benefits personally, and integrating awareness with modern culture – using mobile devices or social media – is another method to get users engaged.

Methods of security awareness that only occur annually through computer-based training with no other security interaction are not successful. Also, out-of-the-box phishing emails that do not seem real to the users will not grab their attention enough for them to think they are genuine.

Reporting can impact the effectiveness and budget of the security

program. However, the amount of face time that information security gets with the user is critical to the equation.

Security awareness is ongoing and interactive; it requires collaboration at all levels to continually get the message out there.

Security awareness is critical in the success of an organization and should be part of the company’s culture. The user community should be able to identify electronic, social and physical attacks.

When a company is effective with training, everyone can be on the offensive side of security. In and out of the office there is exposure, if employees understand their role in the bigger picture of an attack, they can relate and respond

**Dr Jessica Barker**

Dr Barker is a leader in the human nature of cybersecurity, has been named one of the top 20 most influential women in cybersecurity in the UK and recognized as one of the UK's Tech Women 50 in 2017.
@drjessicabarker

For effective cybersecurity awareness-raising, use a variety of methods and channels to get your messages across, such as short videos, hands-on workshops and face-to-face sessions. Everyone learns in a different way and the best training campaigns take this into consideration. Rather than simply telling people what to do, show them why it's important and how they can have better security. For this reason, we do a lot of cyber-attack demonstrations for our clients. When you show people how an attack is actually carried out and what happens on both the attacker and victim end, then people 'get it' on a more fundamental level. However, it's vital not just to scare people in an attempt to change their behaviors: you need to empower them with the tools and confidence to pursue better cybersecurity. A positive tone is much more engaging than a negative one.

I sometimes see companies making the mistake of rolling out computer-based training and expecting that it alone will have a fundamental, positive impact on cybersecurity culture. Of course not all computer-based training packages are equal, some are much better than others, but many lack depth and are seen as something to simply

'click through' by people taking them. On their own, I question the value of computer-based training packages, but I do think that well-designed ones have a place as part of a wider campaign (for example, for refresher training).

Getting the right 'hook' for your audience will help your awareness-

security practices. Sessions focused on cybersecurity at home are really successful, because most people welcome better security in their personal lives and like being able to pass this on to their children, parents, siblings or friends. Finally, I recommend collaborating with your internal

"On their own, I question the value of computer-based training packages"

raising efforts have a bigger impact. Use examples that are relevant to the vertical industry, know how the business works, what tools are in place and what the culture is like. When I'm planning a training campaign for a client, I like to host focus groups to find out where there are awareness blind spots throughout the business and what security workarounds are common. I then build the training to respond to those themes.

Rather than using awareness-raising training to simply tell people what to do, use it to respond to their issues and show them how they can still get their work done whilst maintaining good

communications team as they can help you tailor the messages and complement other corporate communications.

Security awareness does not need to be costly, there are lots of things you can do on a budget. A really effective way of scaling up security awareness is to establish a network of cybersecurity champions, who act in a similar capacity to first aiders in a team, disseminating cybersecurity information and being a friendly face for people to turn to with an issue or incident. The champions do need support and training but, with the right structures in place, this approach is not only cost-efficient but also really effective 🍌

Kai Roer

Security Culture Specialist, Author and Speaker
Kai provides organizations around the world with advice on assessing, building and maintaining good security culture using the Security Culture Framework.
@Kairoer

Our research is quite clear when it comes to what works in raising security awareness: openness and dialogue. For organizations, this means they must actively share incidents with their employees, engaging with them on what happened, why it happened, what is being done to manage it, the impact the incident has on the organization and what is being done to avoid similar incidents in the future.

I have seen this done very well in organizations where they set up workshops for employees after major incidents, as well as when they do simulated incident training exercises. Engagement and involvement is proven to be very effective in transforming culture in organizations.

Our research also suggests that there are methods that consistently fail/underperform. For example, forcing employees to do things like mandatory training is not working well in many cases, instead it seems to be demotivating and thus creating negativity towards security.

We see similar things with phishing assessments and training. In the case of one client of mine, we had to completely rethink how to build a resilient workforce after they had paid for a few rounds of phishing assessment products. The phishing assessments were set up in

a way that made a large number of employees feel like they weren't trusted.

They felt punished by the security team because when they failed an assessment, they were being forced to do some training or sit in on a video lesson, or even have a one-on-one with someone from the security team. When your security

of these people may require more from a security perspective, and most of them will benefit from a targeted approach.

I also strongly suggest a risk-based approach: know who in your organization has access to valuable information and use that knowledge to tailor your security controls, including awareness.

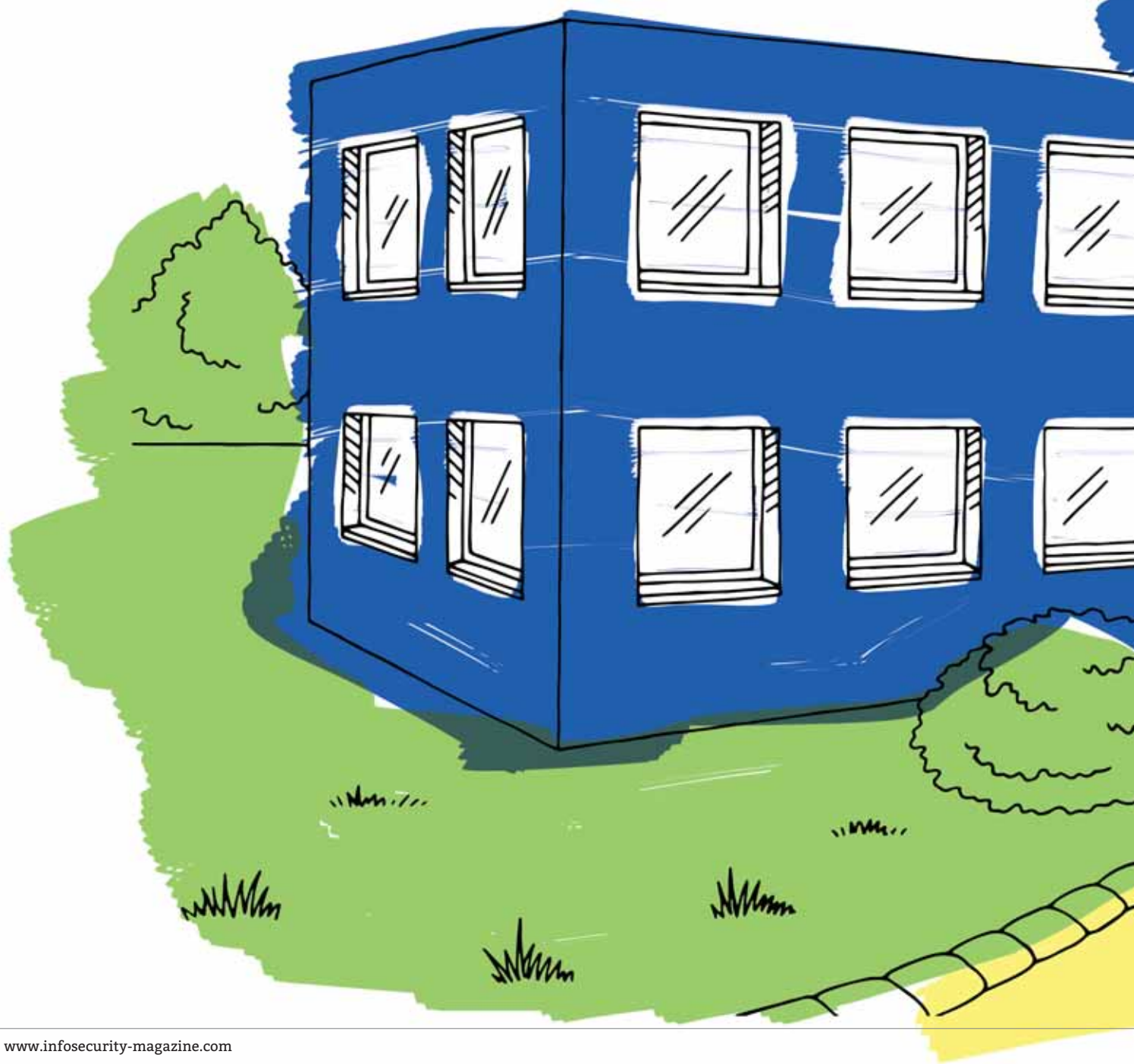
"The one-size-fits-all approach of security awareness programs needs a change"

training and awareness activities create such strong negative emotions from your colleagues, I strongly suggest you change your approach. Let's be honest, everyone is susceptible to falling victim to phishing – no training can ever change that fact.

The one-size-fits-all approach of security awareness programs needs a change. We suggest a more tailored approach, based on the principles of the free and open Security Culture Framework: understand your audience. People are different, they have different roles and tasks; they may use different tools and have different priorities. Some

Creating a program that works doesn't have to be expensive. In my book *Build a Security Culture*, I describe approaches that can be replicated. A few key tips include being creative and engaging employees. Invest time in low-cost, high-impact activities like lunch-and-learns, workshops and meet-ups for those that are interested. Use online sources which provide low-cost and free tools, training content and more. Most importantly, start with a risk analysis, map out your needs based on the results and identify the low hanging fruits for your organization 🍌

NHS AT 70: GROWING OLD & GROWING THREATS





As the NHS turns 70, *Kathryn Pick* assesses the UK healthcare provider's evolution of information security

Celebrations have been taking place across the UK to mark a massive milestone in the history of the country's healthcare system – the National Health Service (NHS) has turned 70. However, rather than sitting back with a cup of tea and taking up gardening, the organization needs to get more agile as it gets older.

The institution was shaken to the core by last year's WannaCry ransomware attack, and is increasingly a target for cyber-criminals looking to make an impact.

So what technology challenges does the NHS face in the coming years?

Threats Gone By

The core principles of the NHS – to meet the needs of everyone, be free at the point of delivery, and be based on clinical need, not ability to pay – may not have changed over the years, but the threats it faces to the security of its information have.

Tim Sewart, a lawyer specializing in technology for Memery Crystal, explains how past threats focused on hitting systems rather than personal data.

“Threats in the past were really all about disabling systems, and those threats were limited because historic healthcare service provision was not wholly dependent on data,” he says.

Steve Roberts, CEO of cybersecurity and surveillance consultancy Online Spy Shop, adds that access to those NHS systems was also easy for cyber-criminals.

“In 2011, an informal group of hacker-activists warned the NHS that they'd found a way into a NHS network and even posted admin and user details to prove it,” he says. “The NHS played it down, but this was embarrassing, even for 2011.”

The NHS Digital team is a key part of dealing with the threats the service faces, responsible for information, data and IT systems across the NHS.



“Threats in the past were really all about disabling systems, and those threats were limited because historic healthcare service provision was not wholly dependent on data”

Chris Flynn, head of operations at NHS Digital's Cyber Security Centre, admits his field had never been a topic at board level until as recently as 18 months ago, but things are changing.

“The idea that the IT department will sort it all out is diminishing and organizations understand that solutions start from the top,” he adds. “The risks we face are commensurate to any other industry, and it's often the methods of exploiting those risks that change on a more regular basis.”

Unique Challenges

Of course, all large organizations on both sides of the Atlantic face threats on the cybersecurity front, but the NHS – and all healthcare organizations – face some unique challenges in comparison.

“Patient care will always be at the forefront of healthcare providers' priorities,” says Flynn. “That's why every one of us comes in to work; to help deliver the best patient outcomes we are able to.”

The service itself is a matter of life and death, and this means healthcare organizations should think of security, not just in terms of technical risk, but as a business risk too, says Lynne Dunbrack, research vice-president at IDC Health Insights.

“What happens to patient care and other services in the event of a systems outage as a result of a cyber-attack?” she adds.

“What happens if access to mission critical applications, such as EHRs or CPOE, is disrupted?”

“What about the damage to the healthcare organization's reputation if there is a privacy and security breach?”

Sewart says medical data is regarded as especially sensitive, both by the law and the population. “This means the rules around data sharing are restrictive,” he adds, but advances in healthcare are often driven by sharing that data. “The tension between data

privacy rights (and expectations) and advances driven by data-sharing are more pronounced in healthcare than in any other sector.”

Roberts agrees that there is a specific challenge in finding the balance between exploiting data for health outcomes and securing it to stop it getting into the hands of cyber-criminals. “Digitization of healthcare data, and the real-time sharing of that data between devices – for example between a lab and a consultant on a ward – is extremely valuable from a clinical point of view. However, the same data is also extremely attractive to criminals.”

“The temptation could be to over-protect patient data to win the war against cyber-criminals, at the cost of using that same patient data to save lives, cure disease and improve outcomes. The challenge is to find that balance.”

Global Difference?

Dunbrack explains that many of the challenges the NHS faces are mirrored in the US.

“Many of the same worldwide trends that promote the widespread deployment of healthcare IT solutions are also making healthcare organizations more vulnerable to cybersecurity threats,” she says.

“More electronic health information is widely available and data volumes are growing exponentially, creating larger, more attractive targets. Healthcare organizations are consolidating and consumerization of technology has resulted in near ubiquitous adoption of mobile devices.”

She also points to a shift from wired to wireless networks, leading to a wide range of ‘at risk’ endpoint devices, many of which are not under the direct control of the IT organization.

“Healthcare organizations are increasingly under attack, experiencing thousands of threats on a daily basis,” says

Dunbrack. “[They] simply cannot keep up with the level of attacks levied against them by cyber-criminals whose arsenal is evolving rapidly with greater levels of sophistication and insidiousness.”

Then there is also a question of resources. The debates on healthcare funding in the US have always been pronounced, and the NHS in the UK is used as a political football between parties.

The priority in the US is strengthening security posture in the sector and building internal security awareness. For Salvatore Schiano, researcher at analyst firm Forrester, the biggest issue in the US has again come down to a lack of resources.

“Compared to other US industries, healthcare spends the least on IT security as a percentage of their overall IT budget,” he says. “Worse, 51% of security decision-makers at US healthcare organizations report that spending will stay the same in 2018.”

Greg Day, VP and CSO at Palo Alto Networks, argues that the NHS is quite different. “I’m not sure there is a bigger centralized healthcare system that has been in place as long as the NHS has,” he says. “Today, many medical facilities around the world run more independently, which means they have fewer such open and interconnected processes and systems.”

“This has inherently created a far more segmented model that creates some barriers that segments risk.”

Likewise, he adds, with many other health organizations either being privately owned or not having been in place as long, they don’t suffer the same degree of technical debt, which can stifle both IT and cybersecurity innovation.

“The more fragmented the cybersecurity controls, the greater the human workload and so business cost to support them.”

There is also the issue of compliance with regulation – a problem that differs from country to country.

Daniel Kennedy, research director for information security at 451 Research, says: “Brexit didn’t save UK organizations from the General Data Protection Regulation (GDPR) which is causing all companies affected (including US companies with EU customers) to undergo serious evaluations of the protections around the more expansive concept of ‘identity’ data covered,” he says.

“We have heard anecdotally in our interviews of some UK organizations whose entire security project schedules were being pushed aside for internal review of GDPR compliance.”

Threats at 70

The challenges of the healthcare sector globally are stark and somewhat different to your average large organization, but what are the big issues going forward for the elderly organization that needs to stay young?

The major threat facing the NHS, and indeed other healthcare systems around

the world, is the fact they are now an attractive prospect for cyber-criminals.

Sewart says: “The NHS has benefited, from a cybersecurity perspective, from being disparate, not joined-up and historically holding relatively rudimentary data. It has not, therefore, been a very interesting target. That is all changing now, and I would expect, in the short- to medium-term, some enormous – and potentially scandalous – losses of NHS data and services arising from cyber-breaches, or other information security lapses.”

However, Sewart adds: “We have to accept these losses as a price we pay for progress and a continuing reminder to invest in systems and processes that mitigate the risk of data loss.”

Roberts again raises the issue of the organization’s continued reliance on legacy systems and software, which will leave it open to threats in the future. “This makes keeping [systems] secure, with regular updates, a costly and difficult process, if it’s possible at all. The WannaCry ransomware attack was made possible due to the vulnerabilities associated with these systems.”

Salvatore says ransomware attacks have “skyrocketed” in the industry and out-of-date operating systems leave machines with long lifespans vulnerable.

He adds: “Flat hospital networks allow infections to propagate from IT to clinical networks much easier than they’d be able to if the network was segmented.

“For example, if the hospital café’s POS system is hacked, it shouldn’t be able to spread to the network where Protected Health Information (PHI) data is held.”

It is also a case of a need for downtime to make those upgrades. Salvatore says:

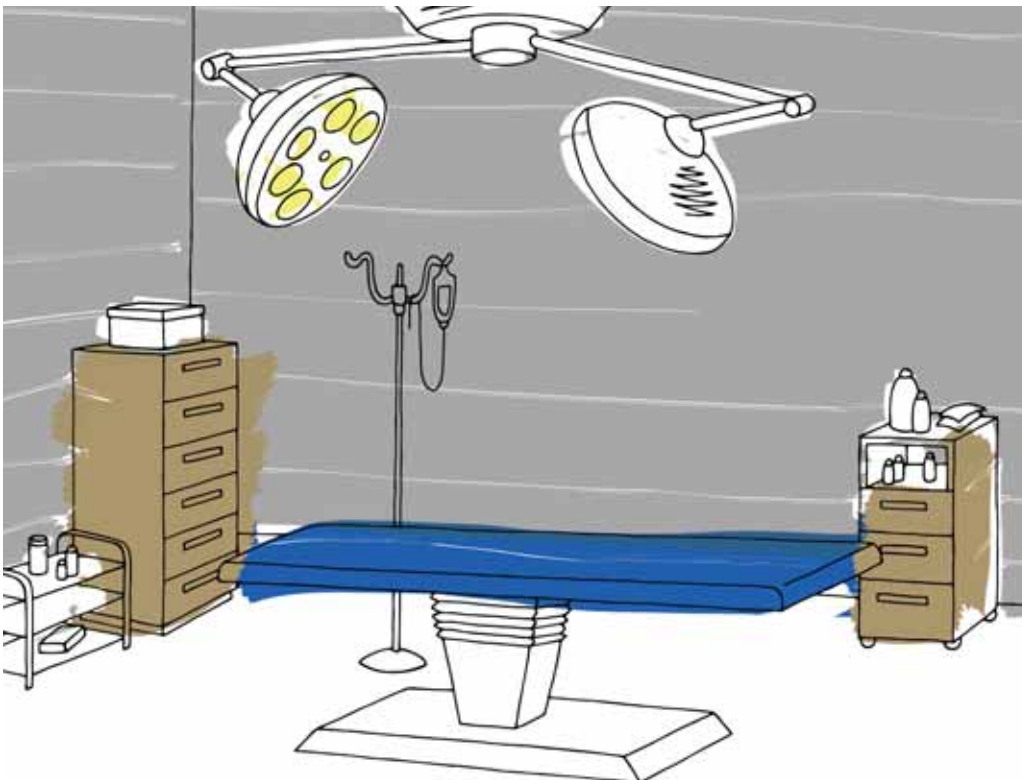
“Even if the downtime is brief, it complicates everyday processes at hospitals dealing with fragile patients.

“The ransomware attack on the NHS exemplified this, leaving it unable to address non-critical emergencies.”

NHS Digital is trying to face the issue head on though. “We are helping organizations by procuring technology and services that we know will help improve the overall security posture of the NHS centrally and providing them free of charge to NHS organizations,” says Flynn.

“Windows 10 is a good example of this – making licenses available to NHS-funded organizations for the next five years so they are able to ensure their operating system remains supported as well as taking advantage of the Advanced Threat Protection (ATP) service.”

Perhaps these challenges are worth thinking about if you are looking to get the NHS a birthday present



Point

Advancements in Authentication: Impro



Maritza Johnson

VP of Research and Privacy, SafeGuard Cyber

Maritza is a security and privacy researcher by training and typically works on helping people better understand the privacy and security decisions they encounter in their daily lives. She earned her PhD at Columbia University. [@maritza_johnson](https://twitter.com/maritza_johnson)

There are more headlines each day about hacks and data breaches that can be blamed on authentication shortcomings, yet industry news claims that new authentication methods are making us more secure. Certainly we have better authentication techniques today than in the past, but does that make us more secure? We do have new tools and techniques that position us well to improve security, and there is still ample room for improvement in the authentication space.

Let's highlight two types of improvements we're seeing: tweaks that make it easier for people to live with passwords, and new second factors to supplement or replace user-generated secrets (passwords).

Well-designed password meters – solutions grounded in empirical research on how people actually use passwords – help users cope. These are the indicators that dynamically guide the user to create a strong password. When the user is given concrete feedback on why the password is weak and how it can be improved, a stronger password is possible.

This approach enables us to focus on solutions that address real problems. Better passwords is an improvement and modern password managers help users in more substantial ways by generating long, random passwords, recommending unique credentials and auto-filling.

The exploration of new second factors also improves security. Push-based notifications via a mobile app to deliver an authentication request verifies that the user is in possession of the smartphone associated with the account, and security keys introduce a physical token for hardware-based protection. Both of these help address the shortcomings of passwords and are designed to be more human-centered and usable.

Let's embrace improved authentication solutions while also minding the gap

between the user behavior required to achieve the desired security properties and the user's actual behavior. Employees are hired for their skills in a specific domain. Yes, they need to adhere to the security policy, but it is the CISO's responsibility to deploy a realistic security policy that matches the threats employees face while giving them reasonable tools to achieve those goals. It's futile to proclaim employees must do

and figure out how the authentication choices mesh with your plan. Next, embrace your role as an educator: design your policy and teach employees how it complements their workflow instead of hindering it.

Once you know what services are being used, security policies can be crafted accordingly. Use your judgment and require or recommend two-factor when it makes sense, it's almost always

“Businesses that can adapt to this new model, and close the gap between policy and behavior, will succeed in improved security”

something for security's sake or decree that a useful third-party digital channel, like Slack or WhatsApp, can't be used. Make it easy to do the right thing, and users will more easily oblige with security protocols.

It's important to do your homework. Start by looking at which services and tools your employees are using to accomplish their goals. It's become increasingly common for an employee to need a variety of third-party services to do their job: are you aware of all of them? Enterprise security is no longer about managing your own network. For example, collaboration tools like Slack are de facto requirements to work productively. Also, markets increasingly rely on WhatsApp for business communications. Adjust your threat model to accommodate new technology,

better than a naked username and password. Unfortunately, despite advances in authentication, passwords are still the most widely deployed authentication method. Deploy a password manager and train your employees on how to use one effectively.

CISOs must understand which services their employees are actually using to do their job. Once they have that information, they will find it's more straightforward to create and implement a reasonable authentication policy. Authentication is only one piece of your organization's overall security policy. The system doesn't stand alone, and you must ensure security plans match the reality of your company's employees. Businesses that can adapt to this new model, and close the gap between policy and behavior, will succeed in improved security 🍌

Counter-Point

Living Security vs Creating New Problems

When faced with the simple question of whether personal authentication is easier than it used to be, the vast majority of people will acknowledge that increased security has meant increased checks and complexity. When it comes to authentication, there are even bigger issues.

Let me start by asking these questions:

- How many passwords do you have today compared with 10 years ago?
- How much longer are those passwords than they used to be? Are they longer or shorter?
- For your most secure items, for example, your bank accounts: How complicated has setting up and using the authentication process become? Is it easier or harder?
- How secure do you think each authentication process you use really is?
- Are you making secure transactions (for example, payments or digital signatures) more frequently or less frequently than a few years ago?
- If your bank account was compromised due to unauthorized access, would the organization be accepting the blame or using their authentication features to blame you (the user) for leaking information that made the intrusion possible?

Most of the latest and 'best' authentication technologies rely on capturing significant amounts of personal information. They want to understand the people that need to be authenticated – their location, habits, working times, face, fingerprints, voice and more. This information can help authentication technologies run many different checks, often without needing to disturb the user.

The difficulty is that there is usually more than one entity that wants that same information from you. The company that employs you may want that for their authentication systems, but so

does your bank, your home devices, your favorite web applications, and so on.

If all those entities have that information, is that really making you more secure? Is it really making the authentication process stronger? Also, what else might they use that personal information for?

It certainly doesn't feel like I have improved security. It feels like there is more information about me online than there ever was.

From a capabilities perspective, there is no doubt that authentication security technologies have improved significantly. The issues are that these advancements have made managing access harder for the users of systems. Improvements in authentication have mostly relied on building out more personal information about who you are than you may even know about yourself.

These enhanced authentication techniques also mean that unlike passwords, where we really could have something unique for each system, most of us only possess, for example, a single face – and it turns out that it is pretty hard to encrypt your face. Your face can get photographed, scanned and each time a new technology claims to have achieved a new level of facial recognition security, an article comes along shortly afterwards about how the latest facial recognition security has been cracked.

If you thought authentication was a pain in the neck for regular people, it is even more complex for security functions inside companies and government organizations. Getting the rich diversity of internal, cloud, mobile, smart and other applications to use a common access and authentication architecture is usually significantly harder than herding a flock of cats towards a barking dog.

The main executive and critical departments within an organization

must fully trust their security function, which must contain or access the right expertise and have a deep, accurate understanding of the business requirements of their organization. These things rarely exist together.

If you are a miracle worker and you have managed to get that executive support to mandate a standard access and authentication architecture, then you still have a further problem: What should you buy?

Gone are the days when authentication was a binary deal. Now even your authentication options have options. Even if you get the initial choice right, how long will the authentication work effectively for? Are there any legal or privacy concerns with the way any component in the authentication techniques work? Will you really be able to use it for everybody? For example, if your suppliers or customers have to use something else to access your systems, what holes in the authentication security does that create?

Although there are better authentication technologies available, the lack of government e-identity or a single trusted standard means that most people are using a more complex range of authentication techniques than ever before.

To conclude:

- There are too many authentication technologies
- Enterprise authentication solutions are expensive
- It's a confused market with too much noise and choice
- Trust in 'free' authentication platforms has eroded
- Getting an enterprise to coordinate their access and authentication policy is like being effective at herding cats

Authentication may be more sophisticated than ever, but for most of us, it is not in a better and more secure place than in the past ☹



Raef Meeuwisse

CISM, CISA, Author of Cybersecurity for Beginners

Raef is an ISACA certified information systems auditor and information systems manager. His operational roles have included global security and privacy program director at a FTSE 100 company and interim CISO. He now spends much of his time writing cybersecurity publications and presenting at conferences.

@RaefMeeuwisse

ARE BLUE TEAMERS THE TRUE HEROES?

The cybersecurity industry has long exalted those capable of breaking technology and coming up with fresh new attack techniques, but is it time to recognize those tasked with defending and recovering from incidents? *Dan Raywood* looks at the case for the blue team

In last year's Q3 issue of *Infosecurity* we looked at the concept of red teaming: exploring where it came from, who red teamers are, what services they typically offer and why businesses should care about red teaming. Now, a year on, it seems that there is a sea change in attitudes towards those on the other side of the test, the blue team.

He says: "Maybe we are breached, we just don't know it yet? Maybe the defense worked today, but will it be as effective tomorrow? I think these are some of the things that put offensive in the forefront over defensive."

On episode 206 of the *Southern Fried Security* podcast, host Martin Fisher said that he was tired of people saying

security researcher might choose to focus on."

The issue seems to be that there is not so much glory in being on the defensive side. Jardine says that while there are plenty of people that work on the blue side and focus on helping to defend against and stop the bad guys, the appreciation for the job they do is just not there.

Quentyn Taylor, director of information security for Canon Europe, tells *Infosecurity* that the problem is "we venerate [too much] the red teamers and attackers" who claim they can break into a company in 10 minutes.

So is it time to recognize the defender? "Yes, as we celebrate offense with the Pwnie awards – which are hilarious – we need something like that for the blue teamers because so often the work of the blue team goes unrecognized.

"With red teaming, you need deep skills in one particular area, but with a blue team you need to have such a width of skills to be able to cover everything from PR to reverse engineering to everything else," Taylor says. "I've been a blue teamer for 18 years, and I still don't even think of myself as a blue teamer – it's time to recognize ourselves for what we are."

"Sifting through data and distinguishing a real incident from a false positive takes knowledge, skill and experience"

The blue team is the security team, those tasked with securing the network, defending and hardening it against attacks and remediating when something goes wrong. For every new attack method, there's a defender tasked with rolling out a patch or applying a rule or policy so their network is not vulnerable.

Blue Hats versus Red Hats

The blue team are now often being perceived as 'the good guys' who, whilst working tirelessly to defend networks in the face of attack, actually receive none of the praise they deserve. There is also an argument that blue teaming is, in fact, more skilled than red teaming, highlighted by the defense ethos of needing to be 'prepared all the time' in an era of vulnerability disclosure and bug bounties. Ultimately, the industry is often guilty of praising those on the offensive side without recognizing the work of those doing the defending and repairing.

James Jardine is CEO of Jardine Software and is a co-host of the *Down the Security Rabbithole* podcast.

"I have spent time working both sides of the fence on the red and the blue side," he tells *Infosecurity*. "There is much more status given to the ability to test or hack than there is for those that focus more on defensive techniques.

"Of course, one of those reasons is that offensive techniques are easily confirmed. If I find a SQL injection and exploit it to gain access to a cache of data, it is tough to dispute that. I know it happened, I have the data. This makes it easy to identify an accomplishment."

On the defense side, Jardine adds, it is not as easy as you can assume that defensive techniques are working, "but we cannot be 100% sure."

security is broken with no idea how to fix it and that "it is easy to break but harder to defend." Guest speaker Wendy Nather, director of advisory CISOs at Duo Security, said that it is all too easy to say "you missed a spot," but eventually it is time to grow up and do some defending.

Speaking to *Infosecurity*, Nather argues that it is time that those given the task of repairing the 'damage' are given more credit, adding it is actually about more than that, as running an enterprise security program requires much more than just blue teaming.

"The term blue team connotes a game or a match, one side against the other in a limited exercise, but most of the time, corporate security is not about attack and defense," she says.

"Corporate security is not football. It is the ongoing process of designing and building secure systems, processes and procedures; it's about helping the business do what it does in the most secure way possible without hampering its success," says Nather.

"Every so often, you have to drop what you're doing and respond to an incident, but most of the time you're having a discussion with a colleague about finding the best way to build something or make it better."

Are The Blues More Skilled?

The thing that seems to have tipped the balance in the favor of the blue team is the acknowledgement of the skills required to be a blue teamer. Nather points out that being a blue teamer "requires empathy, psychology, process re-engineering and a pragmatic understanding of how everything works, not just the best way to attack something." You also need "a broad technical knowledge far beyond what a

Nothing is Rosy on the Blue Side

Along with not being as recognized as those conducting offensive actions, another problem that blue teams face is in achieving a 'business as usual' baseline. Gemma Moore, director, information security consultant and penetration tester at Cyberis, thinks the blue team needs to understand "what normal activity looks like in order to be able to identify abnormalities," and this is a key weakness in detecting unusual activity within the network.

So why is this a weakness? Moore says that you need to consider the variety of indicators that might be present within a standard corporate network. On a purely technical level, the blue team needs to consider all kinds of events to baseline: user authentication events, the use of system privileges, patterns of network traffic internally, CPU and memory consumption, changes in DNS querying activity, users conducting unusual operations within the network, and many more.

"Any changes in these metrics could be a result of a compromise in progress," she says. "This is a lot of data to process and analyze, and it requires a really in-depth understanding of technical operations in an effective blue team."

That is why a skilled blue team is so important, she argues, and the challenge



for the blue team is to understand which indicators of compromise are more likely to provide a true positive in their particular business environment, so that these are properly monitored.

"Sifting through data and distinguishing a real incident from a false positive takes knowledge, skill and experience."

Are You Normal?

Understanding what is 'normal' is a challenge for the blue team, who need to determine what they expect normal to look like, and when dealing with a persistent attack or anomaly, need to know what the problem is and be able to respond immediately. Nather says that this is why cybersecurity practitioners need to be promoted as role models, as this sort of work comes with its own unique challenges.

April C. Wright is CEO of Architect Security, and she believes it is not a case of the red or blue team needing more skills but that they "definitely need different skills and they need a totally different mindset as default."

"I've been a blue teamer for 18 years, and I still don't even think of myself as a blue teamer – it's time to recognize ourselves for what we are"

She adds: "Defenders must be able to see big-picture trends, anticipate events before they happen, and understand known risks to focus efforts on high-risk areas. Offensive teams need to have more of a 'predator' mindset, be able to find the forgotten system, exploit human weakness and understand the nature of vulnerabilities."

"In other words, you need a blue team that can 'think like an attacker' and a red team/offense that can 'evade detection'. Without knowledge of both

sides, either team is going to be limited in effectiveness."

Taylor says that this is one of the common failings around red team reports; they do not take the time to explain findings to the blue team. "What frustrates me is a red team that doesn't understand that they need to educate," he adds. "If they get in they should sit down with the blue team and talk them through what they did and how to defend against it."

Time for Recognition

All of this acknowledgement of the challenges of blue teaming and the skills required suggests that it is time the blue teamer was seen as an equal to the red teamer. Wright says that a good day for a blue teamer can be when nothing happens. This can be "extremely relieving and knowing that you've defended data against attack for another day is, in my opinion, a more difficult struggle and a bigger win."

However, it does feel that there is more recognition growing about what blue teams do. Self-declared blue teamer and security technology lead at Entergy Keirsten Brager explains that the efforts to recognize blue teamers are very timely and if we're going to get more people interested in the cybersecurity career field "the public needs to understand that it entails more than hacking."

She agrees with the general consensus that while offensive skills are great for informing defensive strategies, the industry needs to move away from promoting the celebrity hacker as the de facto career choice because it is such a small subset of the industry.

"Companies need defensive talent, business acumen, communication skills, regulatory knowledge, incident response and a host of other overlooked capabilities that are required to run a successful security program," Brager says. "The better approach is to promote how offensive and defensive skills are equally important to continuously improving the discipline as a whole. We need fewer examples of the lone hacker and more illustrations of the collaborative nature of our work."



A red team is on the offensive side, typically employed by a company to find ways to break into a business or service. These are usually external third party services, although there are instances where a company will have its own red team.

A blue team is on the defensive side, and is your typical network security team or security operations team. Once employed to complete a task, the red team should inform the blue team of how they were able to succeed, so that the blue team is better informed about its vulnerabilities.

BARACK OBAMA

Identity management company Okta does not mess around when it comes to keynote speakers. At Oktane 2018, CEO Todd McKinnon welcomed former President Barack Obama onto the stage and the room positively erupted. *Eleanor Dallaway* reports on the highlights

What Identity Means in Washington DC

“We live in a culture today where everybody feels the crush of information and the collision of worlds, and it’s disruptive in a way that previous generations just didn’t experience for most of human history.

The great thing about the United States is that we have had a head start over the rest of the world in trying to figure out technology, social media and the new economy. By definition, we are a people that came from everywhere else and had to figure out how to join together, not based on a common race, a religious faith, or even initially a language, but based on a creed and essential principles.

The big challenge we have today is how we maintain that sense of common purpose and how we join together as opposed to splinter and divide.”

Technology: Be All and End All or Part of the Problem?

“The public sector has an extraordinary talent and does a lot of hard things really well that the private sector can’t or won’t do. The one area where there is this huge gap, however, is technology. The difference between the kinds of service responsiveness and nimbleness in government IT services, for example, versus what you see in the private sector, is vast. It’s partly to do with procurement. The way government rules have evolved around how you buy stuff is not well-equipped for things like software, and as a consequence, you get these huge systems, wildly expensive, [that often] don’t work, and we were trying to redesign them in a whole bunch of ways. We need to make data sets that we can aggregate and that researchers from all over the place can work with. The political system is not as responsive as it could be to unleash the opportunities with technology, but also in creating the regulatory

structures in areas where technology is moving so quickly.”

The Great Data Exchange

“There is the issue of data collection, how data is used, what happens to personal data, how it gets commercialized? Creating a framework that’s agreed upon, transparent and that people understand is a challenge that we should welcome and do in a structured, systematic way, as opposed to in a spasmodic way.

When there’s a data breach, people are outraged, they feel as if they don’t know that their data is being collected or used in a particular way and then scramble to catch up to the headwinds. What I’ve been driving for in this review is to be proactive and say to law-makers ahead of time, here are the questions we have to grapple with, and here’s our business model that we think makes sense. Here are the tools we have to protect the data and information, but we recognize that we are under some obligation to make sure that the consumers and the ordinary people understand what it is that they’re giving up and what they’re getting in return.”

Technology and the Tax System

“We under-invest in the IRS. Nobody likes the IRS, it’s always a good whipping boy, and so as a consequence, we discovered that the basic IT systems in place are held together by string and bubblegum.

You could make the interaction with the IRS much more efficient, transparent and user-friendly, but that requires some funding. It is in the interest of all of us for there to be a good conversation between the tech community and the people in Washington to create a structure of ongoing deliberation and exchange.

Technology is an area where we had one of our biggest recruitment problems, because frankly, companies like Okta pay better than the US government. It may be that we struggle to retain an outstanding computer scientist or coder

or engineer for 20 years because of some of the pay disparities that exist.”

Electronic Election Voting

“Three-quarters of this room knows more about the technical elements of online security and the dangers of identity theft in commerce than me. Obviously when you start thinking about the possibilities of hacking into election results, it’s deeply problematic. I will say that my bias is to make voting easier, not harder. We are the only developed country on earth that deliberately makes it hard to vote! I am always biased towards opening up the process to make it easier for citizens to participate and have their voices heard.

I think eventually, if we can secure the voting process, and if frankly there’s a paper record that is generated alongside the online voting, then it’s something that should be considered and tested and almost inevitably will come. It is important for people to understand that the reason we don’t vote is not simply because of the lack of technology, it’s that laws are structured to make it hard for people to vote.”

Convincing People to Innovate

“Change is hard. The starting point for me is always to spend time talking to the people that you want to change, or whose lives are going to be disrupted, so that you actually appreciate who they are, what they care about and what their values are. If they feel heard then potentially they can be partners, and together you can initiate the change.

Initiating change requires hearing enough voices and enough perspectives, particularly among the chief stakeholders, so that even when there are disruptions, you can anticipate some of those disruptions and address them.

Every leader has strengths and weaknesses, and one of the strengths I have is a good BS detector. No-one in my White House ever got in trouble for screwing up, as long as there wasn’t a



malicious intent behind it. There wasn't, which is why I didn't have any scandals! Which seems like it shouldn't be something you'd brag about, but if you look at the history of the modern presidency..."

The Best and Worst Advice

"The worst advice I got probably slowed us down and hurt some of our effectiveness early on. It was that once you are President, there are certain ways you should behave and certain ways you should do things. You walk into the Oval Office and you think, 'I need to wear a tie now, and I have to look serious'. I think that we corrected that towards the end of the first term.

The best advice I got was to maintain humanity. Michelle and I, partly because we wanted to make sure our girls didn't get weird because of a weird environment, thought it very important to make sure that we did not lose ourselves in this process. We wanted to stay intact in terms of our values and

what we believed in, how we treated people, the expectations we placed on ourselves, how we ran our household and how we ran our staff and the expectation of kindness and honesty. We came out intact."

No Longer Being the President

"You know, it's pretty good. I don't miss the trappings of the Presidency. We walked into our own house, and I had to figure out how the coffee maker works, and fight Michelle for closet space, [a fight] which I lost. I didn't have people saluting or all kinds of trumpets going off, and it didn't bother me one bit. I didn't think, 'oh man, I wish I still had those trumpets'.

I get much more sleep now than I used to. It's a grueling job. You have barely five hours' sleep a night for eight years. Now I have time to rest and read, all that stuff. Everything moves in slow motion outside the White House."

Closing Remarks

"Right now, there are competing narratives globally. How do we deal with globalization or technology, whether it's displacement or inequality, or migration? How do we deal with the big churn that's taking place? There are two ways to respond to this. One is the default position for most of human history – to feel threatened. We go tribal, we go ethnic, we hold in, we push off. There's a constant event, and alongside that, there's typically power and a zero sum gain, dominance and hierarchies and all that other stuff.

Then there's another narrative which is more fragile. It's newer, and it's the notion that we can think and reason and connect. We can set up institutions based on global law, a sense of principles and dignity in work for every individual. This narrative is based on a respect for freedom of speech and religion, and a whole host of values." ●●● END

SIEM: THE SECURITY MODEL THAT REFUSES TO DIE



Davey Winder explores whether the SIEM model is an endangered species or still an essential mainstay in the security posture puzzle

Security incident and event management (SIEM) has been a staple component of a mature security posture for the longest time; since the halcyon days when talk of a cyber-threat prompted debate about who was the best *Dr Who* foe. The truth is that all but the sagest of greybeard security veterans will be unable to recall a time when threats were infrequent, and uncomplicated, enough to be handled with ease by the nominated incident response techie.

These days the sheer volume and complexity of security event data demands a team of well-trained experts to deal with, and even with the help of an automated SIEM system, they are often fighting a losing battle in determining the real threats from the false positives. Yet SIEM systems remain at the heart of the enterprise incident response puzzle, despite the problems and despite having been written off as unfit for purpose by many for at least the last decade.

"When we look at the SIEM market, we observe multiples of vendors selling on the dream of an all-seeing, must-have silver bullet solution to the end user," says Professor John Walker, advisory board, Research Centre in Cyber Security (KirCCS) at University of Kent. "The success of any such implementation can vary from the over-engineered solution, which detected so much low-level information it provisioned the team with an almost impossible to deal with output, to those which accommodate a design based on a skilled mind where the human operator is still key."

Professor Walker recalls one outsourcing company with many government contracts that set up a security operations center where the managed security service provider was advised to detect every security event known to man, plus anything indicating any level of logical danger. Unsurprisingly, these rules produced an unmanageable forest of false-positives. "The SIEM solution implemented was reliant on one all-knowing, highly-trained operative who then left the organization," says Professor Walker, adding "it is the added-value of the skilled human who can bring an investment into the capacity of true SIEM productivity – the age of point-and-click security is still some time off."

Is SIEM Dead?

This doesn't mean that SIEM is dead as a security model, rather that it needs to evolve, and according to Richard Holmes, head of cybersecurity services at independent outsourcing consultancy CGI UK, that's just what it is doing. "SIEM is evolving, with the latest technology providing an opportunity to analyze increasing volumes of data via technologies such as elastic search and the use of data lakes," he explains. "Whilst the aggregation and correlation of data is still fundamental to good operational security monitoring, there has also been a drive to provide the necessary tools to assist in threat hunting, and the tools are starting to evolve into a single pane of glass for security monitoring and alerting."



“It is the added-value of the skilled human who can bring an investment into the capacity of true SIEM productivity”

This is where the likes of a security operations and analytics platform architecture (SOAPA), sometimes also known as security orchestration, automation and response (SOAR), comes into the evolutionary mix. Within the dynamic SOAPA model, SIEM is just one of the available tools to help the incident response team stay on top of the cyber-threat alongside endpoint detection and response (EDR), threat intelligence platforms (TIP) and network analytics. All designed with asynchronous cooperability built in to help skilled security analysts find actionable items in real time.

Into the Mid-Market

Ian Trump, cyber vulnerability and threat hunting lead at Ladbroke's Coral Group, and a founding member of the Canadian Cyber Defense Challenge (Cyber Titan), thinks the biggest move he has seen for SIEM technology has been into the mid-market via channel players.

Indeed, many MSPs, MSSPs and IT Service Providers have been looking to third-party outsourced solutions like Event Tracker, offerings by Black Stratus such as SIEMStorm and the recent big move by SolarWinds in acquiring Trusted Metrics to bring SIEM-like capability into mid-market.

“That comes as no surprise to me as security and compliance challenges impact small and medium size businesses just as much as enterprise, and SMBs just have a much tighter security budget,” Trump says. “The idea of security or compliance as-a-service from a third-party is attractive and a SIEM is still something that helps detect Indications of Compromise (IoC).”

What Trump finds interesting is how SIEM has evolved into SOAR – first at enterprise and then mid-market. “The recent TimeHop data breach really makes the case to have a security technology which could have automatically stopped the bad guy pivoting from dev workstation to hosted infrastructure and the stealing of 21 million records in slightly less than 2.5 hours of hang time,” he points out.

The Impact of AI


The eagle-eyed reader will no doubt have spotted that so far artificial intelligence has not been mentioned, which surely has the potential to be a game changer as far as SIEM transformation is concerned. So is AI, or more accurately machine learning (ML), making an impact in the SOC yet? “Having AI/ML algorithms hunting for anomalous behaviors in the streams of data a SIEM

(or end-point agent) is hooked into, is exactly what the next generation security companies like ZoneFox, DarkTrace and Intechnica are all doing to a certain extent,” Trump says.

However, whilst he admits that the marriage of SIEM and AI/ML will eventually lead to SOAR at some point, Trump doesn't think we are there yet. “Unless the basic and fundamental security controls are in place, the signal to ‘Danger! Danger!’ ratio may be too great,” he warns.

Professor Walker is also yet to be convinced that such models are fully fit for the robustness of the security purpose. “A recent example of this was a calculation based on learned ‘known knowns’, which predicted an output condition which was proven to be inaccurate by an ‘unknown unknown’ expected condition which sent the ML algorithm into a nose dive.”

The AI/ML calculation of which he speaks related to the 2018 World Cup when Germany were credited with an expected success, illustrating that machine learning still depends upon human algorithm adjustments for the calculation output to be robust enough when talking about automated ‘breach or no breach’ determinations.

Richard Holmes adds to the uncertainty when he suggests that much of what is described as operational monitoring AI is actually automation. However, Holmes agrees that there are some great tools coming into the market, such as network analysis tools doing interesting work in the area of AI. Moving forward, he says, “the operational security monitoring space is ripe for the development of AI, with a drive to automating the first line of SOC analysis, enabling operational security specialists to focus on level two and three analysis and response.”  **END**

Interview: Greg Fitzgerald, Chief Marketing Officer at JASK



JASK is a startup that's using AI to modernize the SIEM experience. “Since the foundation of data and security monitoring, IT has been aggregating disparate point technologies and their outputs. Now we are clearly seeing how a traditional infrastructure is being dramatically changed with the application of more current capabilities such as the use of AI and cloud storage. The challenge

with SIEM is that the traditional players are caught in their own financial business models, proprietary data structures and integration formats, and general inertia with little innovation.

This has hurt the IT security people who have built their monitoring models around these technologies, Fitzgerald adds.

“SOAPA systems are helping humans deal with the variety and volume of information processing, essentially augmenting existing SIEM or substituting it altogether: the information distilled by the SOAPA, like JASK, is sent into a SOAR to apply playbooks and help humans take action.

“The use of advanced math, be that AI or ML, is dramatically changing the world and the SIEM model is perfectly suited for updating. It's been a 30-year industry with two dominant players (Splunk and ArcSight) with a plethora of other log- and event-only aggregators with basic, static and manual correlation rules. By applying advanced math models, that have been proven to work with other cybersecurity technologies like Cylance Next Gen Anti-Virus, it's modernizing how IT security works to stay ahead of the hackers.”

In the SIEM world, he continues, the human analyst will be freed from the mundane, manual processes of data integration, collection, aggregation, parsing and analyses of raw and proprietary systems by the automation of this work, enabling them to do what humans do best: “subjectively analyze the results from the ‘machines’ for how those results apply to their organization. Over the next couple of years, I believe we will see security operations teams becoming leaner, more effective and more proactive in reducing the risk to the organization.”



01 Microsoft Seeks Your Hidden Treasures

Feeling the pinch after taking off on the high seas for your summer holiday? Well, fear not – Microsoft is giving you the opportunity to turn those buried treasures in your security expertise into solid gold.

The company has launched its new 'Identity Bounty' program, which along with explaining our terrible use of pirate puns, could make you a pretty penny.

Phillip Misner, who holds the catchy title of principal security group manager of the Microsoft Security Response Center, said: "Microsoft has invested heavily in the security and privacy of both our consumer (Microsoft Account) and enterprise (Azure Active Directory) identity solutions.

"We have strongly invested in the creation, implementation, and improvement of identity-related specifications that foster strong authentication, secure sign-on sessions, API security, and other critical infrastructure tasks, as part of the community of standards experts within official standards bodies such as IETF, W3C, or the OpenID Foundation.

"In recognition of that strong commitment to our customer's security we are launching the Microsoft Identity Bounty Program."

So where do you come in? Well, if you are a security researcher who discovers a security vulnerability in the Identity services, Microsoft wants you to tell them first and give them a chance to fix it, before spreading the news over the internet.

Of course, this means they can tweak and hone their products and make them more appealing, but it also saves them from a raft of embarrassment or legal costs if something goes awry in the meantime.

However, as we know, no pirate carries



out such a task without a little incentive. So what is Microsoft offering?

Well, a payout of between \$500 to \$100,000, depending on the vulnerability.

Misner wishes his new recruits "happy hunting," but will you become part of the crew?

SLACK SPACE

Grumbles / Groans / Gossip

02 Is Your Newspaper Secure?

In a world full of #Fakenews and alternative facts, it is understandable if you cling to your trusty *Infosecurity* for comfort and accuracy.

It's OK though, we understand you may occasionally venture into other pages or onto other websites to get your news. We won't hold it against you (too much)!

It seems however, that whilst we may be forgiving, you may be putting yourself at risk too.

In July, reports revealed that users of the latest version of Google's Chrome browser were getting security pop-ups if they went to one of the world's most visited newspaper sites – the *Daily Mail*.

OK, you may be at risk of seeing one too many Kim Kardashian stories or an insane amount of information about how the latest heatwave in the UK is shutting the whole country down, but are you secure?

What it really comes down to is that the website is not using the HTTPS protocol, switched to by so many companies in order to protect both themselves and their users.

The latest browser version – number 68 if you can believe it – has moved on from only flagging sites that collect passwords or credit card details, but now it is warning users of this extra level of security on any website.

Other massive websites in the UK have also not made the move yet, including *LADBible*, Sky Sports and National Rail.

It is also interesting to see how many internet service providers and mobile phone companies remain on the HTTP protocol – such as Virgin Media, Vodafone and Three.

The fact is other big browsers are likely to follow where Google leads, and nobody wants the first thing a user sees when they land on their website to be a security warning.

So, it is something they will have to think about very soon...(and yes, we use HTTPS).



1. Turn security expertise into solid gold



2. Who's lagging behind in HTTPS?



3. C-level security gaffes

03 CE-DOH!

We have all sat, listened and perhaps rolled our eyes as the biggest of bosses tell us what we already know about cybersecurity.

Perhaps you have even had that little niggles in the back of your mind wondering if they practice what they preach.

Good news for those doubters about you; it seems you were right! Do they heck! The bad news is this will just make your jobs infinitely harder...



According to a new survey from Code42, of the chief executive officers they questioned, a whopping 93% admitted to keeping work on a personal device outside of the office – and no, we aren't talking business-approved cloud services or security protected company laptops, just their own devices, shoved in their pockets for anyone to get their hands on.

Despite huge amounts of cash being spent on preventing the loss of data, especially when it is business sensitive or relating to clients, it is human error that still proves fatal.

Although this isn't just human error, its C-level boss error – not necessarily someone the security people can give a good telling off to. Oh, did we mention that 63% of CEOs also admitted to clicking on a link they weren't supposed to, whilst 59% said they downloaded software onto their devices that they knew they weren't allowed to?

What is even more galling about that is that 77% of them said they knew their IT teams would see it as a security risk, but they threw caution to the wind and carried along their merry way regardless.

Perhaps you could just leave this page open on their desk or next to the executive coffee machine so they get a glimpse – CEOs reading this...WE KNOW!

It seems they may need some subtle hints to make sure those security budgets aren't being wasted on foolish moves.



Parting Shots...

Michael Hill, Deputy Editor

Cybersecurity as a 'board issue' has recently emerged as one of those topics that seems noticeably commonplace in a lot of conversations in and around our industry. This is fair enough because protecting people's data should now be just as important for a business as anything else and boards are undoubtedly more aware and mindful of cyber-risk than they ever have been.

That is certainly a good thing, and it's indicative of just how much businesses rely on IT and the security of information to operate. However, the question of whether cybersecurity is *enough* of a board issue is still very much up for debate.

The reason I say that is because awareness is one thing and understanding is quite another. I believe a lot of corporate boards aren't much better at understanding security nuances and their full impact on a business, they're just more aware that cyber-threats pose a huge risk – there is still quite some way to go until that balance reaches the parity it needs.

Boards are in place to navigate businesses through risk, and there really aren't many more critical risks than that of cybersecurity in today's world. However, simply saying you are on top of information risk management because it's in your operations risk register doesn't really cut it, and a lot of boards are still failing to really get involved in cybersecurity strategies. This

is something that was highlighted in PwC's latest *The Global State of Information Security Survey 2018* which found that just 31% of corporate boards directly participate in a review of current security and privacy risks.

So how do you remedy this? Well, one argument that many in the

instead preferring to keep them on the periphery of boardroom discussions much like heads of other key business areas like HR or health and safety. The difference is that those are traditional business areas that people understand better and have a longer history with. To the contrary, cyber-risk has emerged

"A lot of corporate boards aren't really much better at understanding security nuances and their full impact on a business"

industry make is that boards need to be more open to regularly inviting security professionals into the boardroom, be that external consulting services or, in some people's ideal, the company CISO (any that currently do are very much in the minority). Boards are made up of business people that do not think like experienced security experts, so I think it makes absolute sense for boardroom discussions to include individuals who do.

The big problem is that boards have been – and by and large still are – very reluctant to invite cybersecurity experts into the boardroom. Everything from a lack of confidence in their ability to communicate technical jargon, concerns about their understanding of the company's business objectives and ability to articulate how information security aligns, right through to fears that they will be sold something they don't need or even anxiety that some horrific security issue will be brought to light, all play a part.

Therefore, it is certainly not a universally-held view that high-level security pros should have a seat or at least a voice on the board, with most

significantly in a far shorter time and is evolving at a much quicker rate.

Of course, any information security professional that steps through the boardroom doors needs to be able to quantify cyber-risk in a way that resonates with business leaders who don't speak XSS or SQL, but will connect with ROI, customer retention and how security affects the bottom line. So as much as boards still have work to do to really involve themselves in the wider picture of cybersecurity within a business, there is a need for security experts to become more business-minded people who can effectively communicate with enterprise hierarchy.

Awareness is the first step in the right direction, but deeper understanding needs to follow, because without it, boards are not well-positioned to exercise their responsibilities for data protection and privacy matters. If corporate boards aren't taking every step possible to fully educate themselves on the business ramifications of information security by engaging with the security professionals they have around them, they are setting themselves up for a monumental fall



» 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

Promo code:
IMIS10
10% off!

iStorage®



Without the **PIN**, there's no way **IN**.



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

To receive 10% off, please enter promo code 'IMIS10' online at www.istorage-uk.com. Promotion valid from 27.08.2018 - 30.09.2018.



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