STRATEGY / INSIGHT / TECHNOLOGY

infosecurity

Q2 2017 / Volume 14 / Issue 2

THE CISO OF THE FUTURE
Getting down to business

COUNTDOWN TO GDPR
Preparing for compliance as the May 2018 deadline looms

BLOCKCHAIN
Creating security problems, or solving them?

CONTENTS

ON THE COVER

14 How can CISOs of the future succeed in an increasingly demanding business role?

infosecurity® EUROPE

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, SIRB conference 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**
philmuncaster@gmail.com

Online US News Editor **Tara Seals**
sealstara@gmail.com

Proofreader **Clanci Miller**
clanci@nexusalliance.biz

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

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

Digital Marketing Co-ordinator
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

Locklizard

Protect your Documents against Leakage & Theft

Protect from piracy

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

Share securely

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

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

Control BYOD use and lock PDF documents to specific locations.

Dynamic control

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

Apply dynamic watermarks displaying individual user information.

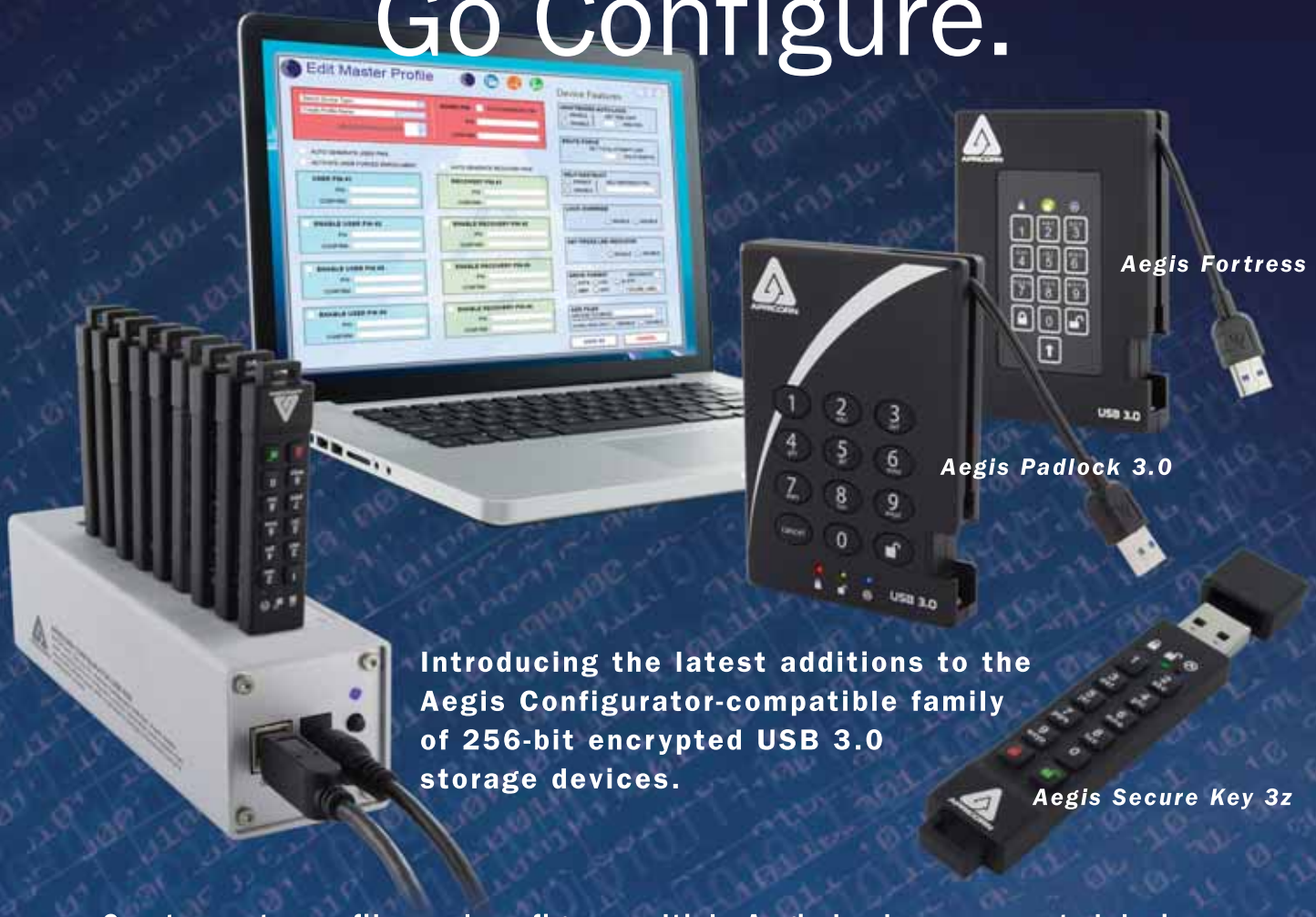
Revoke documents no matter where they reside.

Total protection

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

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

Go Configure.



Introducing the latest additions to the Aegis Configurator-compatible family of 256-bit encrypted USB 3.0 storage devices.

Create master profiles and configure multiple Aegis hardware-encrypted devices simultaneously and in a matter of seconds using the Aegis Configurator application.

- **Software-Free / 256-Bit Military-Grade XTS Onboard Hardware Encryption**
- **USB 3.1 (3.0) Connectivity**
- **FIPS 140-2 Validation**
- **Bootable**
- **Completely Cross-Platform Compatible; OS and platform independent**
- **Programmable Min / Max PIN Lengths**
- **Two Read-Only Modes**
- **Data Recovery PINs**

Take advantage of our free, no-obligation corporate evaluation programme on any of our USB 3.0 military-grade encrypted secure drives.

APRICORN

Come see our complete line of Encrypted Hard Drives and the Aegis Configurator in action at

InfoSec Europe 2017
London, 6-8 June
Stand T74

Apricorn.com/infosec

@InfosecurityMag

From the Editor...

Hand of Fate

We have serendipity to thank for most information security professionals

Rarely do I interview or talk to anyone in this industry who tells me that this is the career path they actively, and determinedly, pursued. Instead, I hear recurring tales of how people have "fallen into it by accident", and these fortuitous infosec pros are almost always delighted that this was their accidental vocation.

Whilst serendipity has been on our side to date, it's simply not good enough that we are relying on this as a means to staffing our profession. Nor is it even an option as we stand on the brink of a skills gap crisis that threatens to put the white hats well and truly on the losing side, as under-resourcing and lack of talent threatens the security of our data, our money and our privacy.

Imagine an infosec world without the James Lynes, or the Charlie Millers. It's unfathomable, right? Yet, this would be a reality if it wasn't for serendipity. James Lyne didn't go to university. Charlie Miller studied Mathematics. Without being in the right place at the right time, these industry stars would have been swallowed up by other industries. Whilst it makes for a great tale of fate, it's really not OK.

The career paths into information security are currently undefined, unpromoted and far too rigid. As the saying goes, beggars can't be choosers, yet despite projections that the world will face a shortfall of 1.8 million cybersecurity workers by 2022 (statistic taken from the (ISC)² workforce study), employers are still demanding unrealistic years of experience or specialized further education, thus excluding and alienating a huge potential pool of talent.

The good news is that there is growing recognition from industry that this is unsustainable and needs to change. The Cyber Retraining Academy is an HM Government program delivered in partnership with SANS. "The remit for applicants is to have no cyber experience and show an aptitude for cyber", Stephen Jones, managing director of the SANS Institute, told me, but that's where the requirements end. The 2017 Academy's 55 students included a bartender, a professional gamer, a journalist, a psychiatrist and police officers, to name a few.

After a 10-week intense program, graduates have the skills to be deployed into industry in entry-level information security roles. The Academy has many industry partners waiting in the wings to snap up the talent. I visited the Academy's career fair style event, connecting the students with industry partners, and spoke to representatives from a few of the supporting companies, including Huawei and the National Crime Agency about what they were looking for.

They all admitted a struggle with hiring talent and saw the Cyber Retraining Academy as a great opportunity to recruit. For Huawei, lack of specific further education or industry experience pales in comparison with natural talent and passion. Academy applicants take aptitude tests to "assess whether their brains work in the right way." In other words, it's doing what the rest of the industry should be: discarding experience and education in favor of natural talent, mindset and willingness.

The stats speak for themselves: upon graduation, all students got jobs, and every industry supporter of the inaugural Academy came back for its second helping of talent. "The guy we recruited from the first Academy is absolutely phenomenal", said a Huawei rep.

Employers would be wise to invest in passion and talent, not certificates

James Lyne, now a SANS instructor and advocate of the Cyber Retraining Academy, "got lucky" by landing in this industry

We shouldn't dismiss the importance of formal and specialist education. A degree in computer science isn't going to be in vain – there will always be a huge appetite for specialist graduates. They alone will not fill the talent pipeline though, nor should they.

Industry needs to open its eyes and mind to alternative talent, the people who code for fun, who look for exploits as a hobby, the people like James Lyne – our profile interviewee – who live and breathe cybersecurity despite never having stepped into a cybersecurity classroom (unless it's one he is teaching).

It's about changing the view of what a good cybersecurity professional looks like. Search for the skills and qualities that can't be learnt in the classroom. You can't teach passion, you can't teach aptitude. So, take a chance on these qualities and invest in the people, adding formal training as and when necessary.

At present, information security is an industry with many closed doors and the paths leading to those doors are ambiguous. Given the skills gap we face, this is catastrophic.

The Cyber Retraining Academy is a great start, but funding is limited and with the current scale, it's going to make a tiny (but wonderful) dent in a huge problem. Industry needs to rally to support and fund similar initiatives, opening doors and investing in talent, not certificates. Recruiters can practice this same methodology within their own organizations and reap the rewards.

For now, let's celebrate the accidental infosec pros who found their way into the industry by accident but continue to light it up every day. Thank-you, serendipity.

Enjoy the issue and take care,

Eleanor Dallaway,
Editor

TRUMP'S FIRST CYBERSECURITY SCORECARD

'C for effort – could try harder' seems to be the overall judgment of Trump's first quarter as President, reports *Danny Bradbury*

It has been one of the most disruptive presidencies so far. Donald Trump has rattled civil liberties advocates with a series of divisive executive orders in pursuit of his protectionist goals. The question is, how has this protectionism shown up in his cybersecurity policies, and how comprehensive are they?

Not very, according to cybersecurity lawyer and policy expert Jody Westby. The former PwC senior managing director now heads boutique legal firm Global Cyber Risk LLC. She advised the Department of Homeland Security on cybersecurity research and development for eight years.

"I found it all underwhelming," she says, arguing that so far the administration has focused on talks and reports. "We've had so many reports over so many years about cyber that what we really need is funding, action and new direction. What's proposed is old direction stuff."

Cybersecurity review was a big feature of an executive order dealing with cybersecurity scheduled for signing on January 31, but it was delayed with hours to spare.

The order, which was leaked ahead of time, promised a vulnerabilities review board, which would analyze the nation's cyber-exposure, and then make recommendations to plug the holes within 60 days of the order's enactment. A similar report would analyze US cyber-capabilities. Other reports called for in the executive order would list cyber-adversaries that threaten the US and an analysis of incentives to get private sector organizations adopting cybersecurity methods.

Time for Action

Westby argues that we have all the reports we need already, and that it's time for action. Most recently, the NIST-organized Commission on Enhancing National Security published a report in December, offering cybersecurity recommendations.

In any case, the order may look different if and when it finally sees the light of day. It hadn't been signed at the time of writing, but has gone through several drafts, say experts.

"Trump's failure to publish the executive order has been particularly disappointing as right now there are too many different groups claiming to be responsible for cybersecurity", warns Richard Stiennon, chief strategy officer at Blancco Technology. A former Gartner analyst and author of a best-selling book on cyberwarfare, Stiennon still has hopes that the order will help fix the problem.

"One draft of the executive order called for assigning responsibility for cybersecurity to the cabinet secretaries, which would be a great motivator and help to clear up much of the confusion", he says.

Industry watchers were hoping that the administration would announce the executive order at RSA, which took place February 13-17, two weeks later, but it didn't materialize. Neither did the administration; none of Trump's representatives attended the conference.

Trump has nevertheless made several cybersecurity appointments. He named Rudy Giuliani, the former New York City mayor and strong Trump campaign advocate, as his informal cybersecurity adviser on January 12.

Thomas Bossert, whom he appointed homeland security advisor on December 27, was deputy homeland security advisor under Bush. Trump has committed to elevating his position to independent status, and cybersecurity will play a big role in it. Bossert has said that he wants a cyber-doctrine that "reflects the wisdom of free markets, private competition and the important but limited role of government in establishing and enforcing the rule of law."

The other significant appointment at the time of writing – which Stiennon calls "the one reason for optimism" – is the appointment of Rob Joyce as White House cybersecurity co-ordinator. However, as the former head of the NSA's TAO cyber hacking team, Joyce's appointment could be considered a statement about Trump's view on surveillance policy in the US for the next four years.

Trump also made another statement that should worry privacy advocates. His blueprint budget

> ***"We've had so many reports over so many years about cyber that what we really need is funding, action and new direction"***

carved out $61m to help law enforcement agencies crack encryption. This was a talking point for Trump during his election campaign, when he sided against Apple in its FBI dispute over decrypting the San Bernardino attackers' iPhones.

The provision is "at odds with any attempts to strengthen data protections", Stiennon says.

The blueprint also includes $35m to help the FBI develop biometric identification technologies with the DoD, at a time when Congress has been grilling law enforcement agencies on their accountability when using facial recognition technology.

The other big recipient in the budget was the DHS, which gets $1.5bn. The document earmarks the money for "a suite of cybersecurity tools and more assertive defense of Government networks." It also promises to share more cybersecurity incident information with other federal agencies and the private sector to speed up responses.

A Long Way to Go

Westby is skeptical. For one thing, she says, the budget hasn't been accepted yet. Trump's stinging Congressional defeat over the revised healthcare act won't help his credibility when trying to push through the finalized budget later in the year.

"Why does DHS need $1.5bn? It looks to me like OPM needs some money", she argues, referring to the agency's massive data breach in 2015. With agencies required to turn their FISMA reports in to Congress each year, we know which ones need an extra cybersecurity focus, she explains. "Get the funding over to those agencies and say 'where do you have common problems?' Let's develop a solution", she recommends.

Incidentally, Obama's government issued a policy on sharing federal source code between agencies and releasing some of it as open source, although this policy has been deleted from the White House website by the current administration.

Amit Yoran, president and CEO at Tenable Network Security, was the national cybersecurity director at the DHS from 2003-4. Unlike Westby, he believes that cybersecurity is a top priority for this administration, and sees signs in the draft executive order that it will hold agencies accountable for it.

Nevertheless, he says, you can't just throw money at a problem to fix it.

"Prioritizing security needs to be set culturally at the very top of an organization and permeate across its entire culture," he says. "There's a huge difference between those that believe in the importance of their security program, and those that give it lip service and just meet their compliance minimums."

Let's be fair, says Westby: the Trump administration has only been in office for two months (at the time of writing). It takes time to organize these things, but his other cybersecurity-related distractions are not making it any easier.

Of note was a report by the *New York Times* in January that Trump was tweeting from an unsecured Android phone, and a later revelation that VP Mike Pence had used a personal AOL account to conduct state business while serving as Governor of Indiana. When it was hacked, Pence simply set up another account, the report said.

Most recently at the time of writing, Trump caused a rift with the UK government by accusing it of helping in an alleged wiretapping campaign against him, organized by the former administration.

Herb Lin, senior research scholar for cyber policy and security at Stanford's Center for International Security and Cooperation, worked on the *NIST Commission on Enhancing National Security* report. He says that such distractions take away from an already difficult job.

"Anybody has limited bandwidth. There's only 24 hours in a day," he says. "[If] they're distracted by a bunch of things, they won't be able to pay good attention to the things that they need to be paying attention to."

The chances are that things will have moved ahead dramatically by the time this article goes to print. The final executive order may be out, and there may be yet more scandals as a tempestuous President, prone to unpredictable public outbursts, muddies the waters further still. Let's just hope that his advisors keep him in check – and don't go off the rails themselves. Kellyanne Conway, current Counselor to the President, must be cringing over her suggestion that microwave ovens can turn into cameras. Or perhaps not. Honestly, with this shipful of loose cannons, it's difficult to imagine just what they're thinking END

Timeline

Date	Event
27 Dec	Appoints Tom Bossert as homeland security and counter-terrorism advisor
12 Jan	Appoints Rudy Giuliani informal cybersecurity advisor
25 Jan	Congression investigation into Russian hacking begins
31 Jan	Expected executive order on cybersecurity cancelled at last minute
14 Feb	Michael Flynn resigns as national security advisor following revelations that he communicated with Russian officials during the election campaign
16 Feb	RSA conference. No sign of Trump representatives
04 Mar	Trump accuses Obama of wiretapping on Twitter
14 Mar	Trump appoints NSA hacking chief Rob Joyce as White House cybersecurity co-ordinator
17 Mar	GCHQ dismisses White House claim that it helped Obama spy on Trump
22 Mar	House Intelligence Chairman Rep. Devin Nunes says that intelligence community 'incidentally collected' communications from Trump transition team

INTERVIEW: JAMES LYNE

James Lyne: Hacker. Uber geek. Insomniac. Cyclist. Gamer. SANS instructor. Public speaker...and, as *Eleanor Dallaway* discovers, that's just for starters

Despite both living in Oxfordshire, I meet James Lyne in San Francisco and spend more than two hours being thoroughly entertained by one of the most self-deprecating, intelligent and hyper human beings that I've had the pleasure of interviewing.

James is the most confident, bubbly 'introvert' (his description, not mine) that I have ever met. When he tells me that when he first started out in this industry he found any type of communication, let alone media or public speaking, excruciatingly difficult, it's almost inconceivable. Here's a guy who has built an impressive career on the exact notion of communication: translating technical security flaws in a comprehensible way.

Whilst you and I would call it 'an impressive career,' James refers to it as his "passion and hobby." I can't emphasize enough how much James loves what he does – it literally radiates out of everything he says and does. "My work is my hobby, I would do this stuff even if I didn't get paid, but don't tell anyone," he laughs, later admitting, "I do get tired sometimes. The saving grace is that I love it – I couldn't keep my schedule up if I didn't. There is so much cool stuff going on and I don't want to miss a second of it."

I wonder if that FOMO (fear of missing out) plays into James' self-confessed insomnia. Given that he gets four hours of sleep on a good night, he has many extra hours in his day to cram in additional reading, "playing with new tools" and gaming. "I love sitting there at two in the morning unpicking interesting malware samples, playing with cool exploits and reading new papers", he says.

A Hard Day's Night

It's not just his nights that are busy. James breaks down his days and work into three areas: research, dealing with the press and outreach.

Of the research part of his role, James says: "Trying to keep up with infosec and tech is like having a hose-pipe connected to your face." An analogy that doesn't do his love of it justice. "There's just so many smart people doing so much amazing work and whenever a new paper or tools comes out, I always want to sit down and spend a few hours reconstructing it until I have that 'a-ha' moment". Sometimes, he admits, he'll spend a week of his life playing with one tool.

Then there's "dealing with the press," which as I know only too well, "happens when it happens and it's not always at convenient times." James explains that his main objective in this part of his role is to "be the voice of reason." The public speaking part of his work requires a thick-skin, adds James. "As many people who think you are great, the same amount of people will call you a pillock. Maybe sometimes that's deserved; I've done plenty of things where I deserve to be called a pillock."

> ***"I had interventions of sorts that made me realize that these skills could actually be valuable and that I could hack stuff and help people at the same time"***

Finally, and an increasing focus for James, is the outreach piece and "trying to translate this industry into accessible, sometimes entertaining but at least watchable, presentations and talks that help people outside of our industry."

Balancing the three is definitely tiring, admits James, who has not been home for more than a day and a half in over two months. "I'm in the business of failing to keep up with all three but trying really hard, because I think it's important that you break those boundaries down."

So this is what James does now. What I'm really interested in, however, is how James' background and childhood have shaped who he is today.

As a child, James moved around a lot. His father designed cities so the Lyne family spent time living in Hong Kong, Australia and other countries, but their base was always in Oxfordshire. "I started travelling and I never really stopped," he reflects, "a constant theme of being a road warrior."

The young James Lyne was "a problem child. I'm quite a problem adult actually", he laughs. He describes his young self as "hyperactive, disrespectful, a total nightmare." The only part of this description that rings true to me is the hyperactive bit. I'll give him that. The rest seems implausible.

"It's true," he says seriously, "I really struggled with people. I remember being told I'd never amount to anything in a parent teacher review meeting." How wrong they were.

At the age of about nine or 10, the Lyne family got a computer, which,

although he didn't know it at the time, would shape the course of his life. "Something just flipped inside me", he explains. Within an hour, James had broken – and then fixed – it.

The Black Hat Crossroads

Lyne spent a lot of time as a teenager hanging out in hacking forums and taught himself a lot. His definition of ethics back then, was, in his own words, "fuzzy. I don't think many 14-year-olds have excellent judgment about the world or make the right decisions. I certainly didn't epitomize those traits."

Having developed the kind of hacking skills that could have been used for good or bad, James recalls a series of interventions. "I had interventions of sorts that made me realize that these skills could actually be valuable and that I could hack stuff and help people at the same time." This was a novel concept to James who admits he was "very close to potentially being on that boundary of going the wrong way and ending up on the path of no return."

There is one man in particular whom we can thank for convincing James to play for 'our team'. "In one of my first jobs, Mike Hobbs was a bit of a tech and business father figure to me. He put up with a lot of my BS and childish antics early on in life and put me on the straight and narrow. Sophos played a large part in that too, but it was Mike who was the seminal person catching me at the right time."

There's a wonderful serendipity around his chance encounter into the industry, but at the same time James finds it concerning that he just "got lucky by running into the right people at the right time. I lucked out on a path that got me into this industry when I demonstrably had the skills.

"I don't want other people in the same situation to have to luck out. There's a really undefined fuzzy path of how you become a security practitioner." This, says James, is a real problem.

"It's important that companies reconsider what good talent looks like. If employers continue to demand five years of experience or computer science degrees, they will miss out on amazing talent," he says. "That could have been my story", says James, who skipped university all together. "Granted, I've worked damned hard in my career to build myself to where I am today, but I can't say that I got into this industry because I worked harder than others. I was lucky."

What do Paxman, Snoop Dogg & Cameron Diaz Have in Common?

Had fate seen him down a different path, he may not have had the opportunity to meet the host of famous people he has. "Jeremy Paxman was actually really cool, a media legend", he says casually when talking about his appearances on *Newsnight* and subsequent pints at the pub with Paxman.

"Being on Bill Maher with Snoop Dogg was pretty strange. It was a seven or eight minute interview talking about the state of security and after, the producer said they were surprised they'd found a geek that could talk." I'm still laughing at the thought of James perched next to Snoop Dogg when he drops his next bombshell: "I met Cameron Diaz at the TED conference. I was standing next to her for a few hours, speaking about security, watching Bono. That was kind of weird." Kind of weird, James? I am speechless.

I ask him who he'd like to meet if he could meet any living person, and without hesitation, he cheats. "I'd build a time machine to meet Alan Turing, Aristotle or Newton." Trust a hacker to find a way around a challenge.

"Of course, according to Twitter, I need to go and meet Peter Capaldi because everyone's proposing I should replace him. That was a good compliment – that I'm the bastard step-child of Michael McIntyre and Doctor Who", James laughs. The time machine answer makes more sense now.

It seems the perfect time to ask him about his appearance on *Late Night with John Oliver*, where they use a clip of James talking about encryption. A huge fan of the show, I'm totally star-struck by this. "You know when John Oliver wants to use your clip, you're in for a ridiculing. Let's be honest, with hair like this, as ginger as I am and the things that I tend to do on stage, I deserve a good ribbing."

A Nerdy Introverted Upstart

James joined the support team at Sophos nearly 12 years ago. "Before Sophos, I was very introverted, I had the technical skills but I actually had to learn to talk to people and communicate." For that reason, James considers it one of the most valuable experiences of his career.

> ***"I'd build a time machine to meet Alan Turing, Aristotle or Newton"***

"I joined Sophos very young, and they provided me with a huge number of different opportunities and put their faith in me to develop my career both technically and as a business professional. They coached me through many screw-ups and my many lapses of judgments through the years. I was very fortunate to land in a company that had a set of managers that would put up with a nerdy introverted upstart and helped me grow into what I've become today."

The loyalty that Sophos has shown James has, of course, been reciprocated. It's no exaggeration to say that James could probably land a job in any infosec company he wanted. So why Sophos? "I've been extremely fortunate that they value me unrelentingly questioning 'how and why'. It's special because they always try and do the right thing. Yes, we're a company that wants to make money, but we care about quality and we want to do this right."

James is also a certified instructor at the SANS Institute and has been working with them to get children interested in cybersecurity while simultaneously changing the hiring mind-set of government and employers.

James has a passion for cycling and does so around the world, including Amsterdam (pictured) and a recent 936 kilometer cycling tour of Sardinia.

> ***"Let's be honest, with hair like this, as ginger as I am and the things that I tend to do on stage, I deserve a good ribbing"***

As part of this objective, they have created a hacking game for 11-18-year-olds. "It has been a monumental undertaking with a really bizarre 'A team' of people working on it," he says. "We brought together a mix of security people and wildcards who are in no way related to our industry, and the result has been unbelievable.

"It's about 300 hours of hacking challenges, hundreds of thousands of lines of code, it has been a monumental undertaking," James explains. "We took security problems, things that we do as security professionals, and took the skill, the tool and boiled it down to the thought process behind it. We want them to get the fun of the industry, the thrill, and we want their brains to go in a way that can have an adverse impact on the system. If we embed that context earlier, we build better security people, developers and more rounded technologists."

The first program was run with 5000 children in the Middle East. "The government there are really progressive on wanting to do something about the cyber-skills gap so we started there. We've been doing a lot in the UK as well, and now we're trying for bigger deployment."

The hacking game asks players to register to play as an agent at the Cyber Protection Agency, the fictitious online virtual agency created. The game gives players an emulation – James' character, Agent J, has a monocle. Of course.

"There are multiple levels, and players start at headquarters on the basic levels 'in training'. There's a field manual where we teach them various training models. Players get badges for finishing them, then they go into the challenges. Some of the scenarios can get quite bizarre – kids love it", he gushes.

"By the time kids get to level six, they're actually using a real Linux terminal to run various parts, they're doing real stuff that security practitioners would do." He calls it one of the coolest projects he has ever worked on. Perhaps he sees himself in so many of the children that are finding their sparkle in front of a computer.

His advice to anyone starting out in the industry is to be passionate about one part of security and be hands on. "Just learn – there's so many amazing conferences you can go to, so many cool presentations, so many things to watch. Throw yourself into it, absorb it, master the skills and in parallel just keep applying for those roles, keep talking about your practical experience and show your passion."

Study More, Suck Less

Don't be mistaken in thinking that James' sparkle is limited just to tech. His list of passions include skiing, running, cycling, pulling bikes apart, reading and travel. He recently did a cycle tour of Sardinia, cycling 936 kilometers in six days. "I love exploring and seeing interesting places, but after a patch of doing that, I'm ready for my computer, to look at some malware and see what's going on."

The Cyber Retraining Academy: Himself an example of "getting lucky" and falling into the industry, James now works with SANS to create paths into the industry for anyone with passion and talent.

When we talk about the future, James says he wants to "study more and suck less", considering himself a perennial student whose thirst for knowledge is insatiable. He's keen to throw himself more into the development aspect of bringing up the next generation to the industry and enjoys his work at SANS greatly. "At some point I'll probably have to re-write the IT GCSE too", he says grinning.

One thing he's sure of is that he is on the right 'side' of the industry, "having the opportunity to research, reverse engineer and have an impact on the industry both in technical research and as a communicator."

When I ask if he can see himself as an end-user, he's adamant that he can't. "It's not me, I love my keyboard time doing stuff and endlessly breaking things. I think my temptation to get my hands dirty constantly might be challenging with the busy and generally overloaded CISO role."

In a parallel universe, James can see himself as (predictably) a video games programer, or (less predictably) a librarian "at a really awesome library and on the condition that I get enough time to borrow the books myself." I'm sure you won't be surprised to learn that his favorite genre is non-fiction, he's currently enjoying tomes on quantum physics and mathematics.

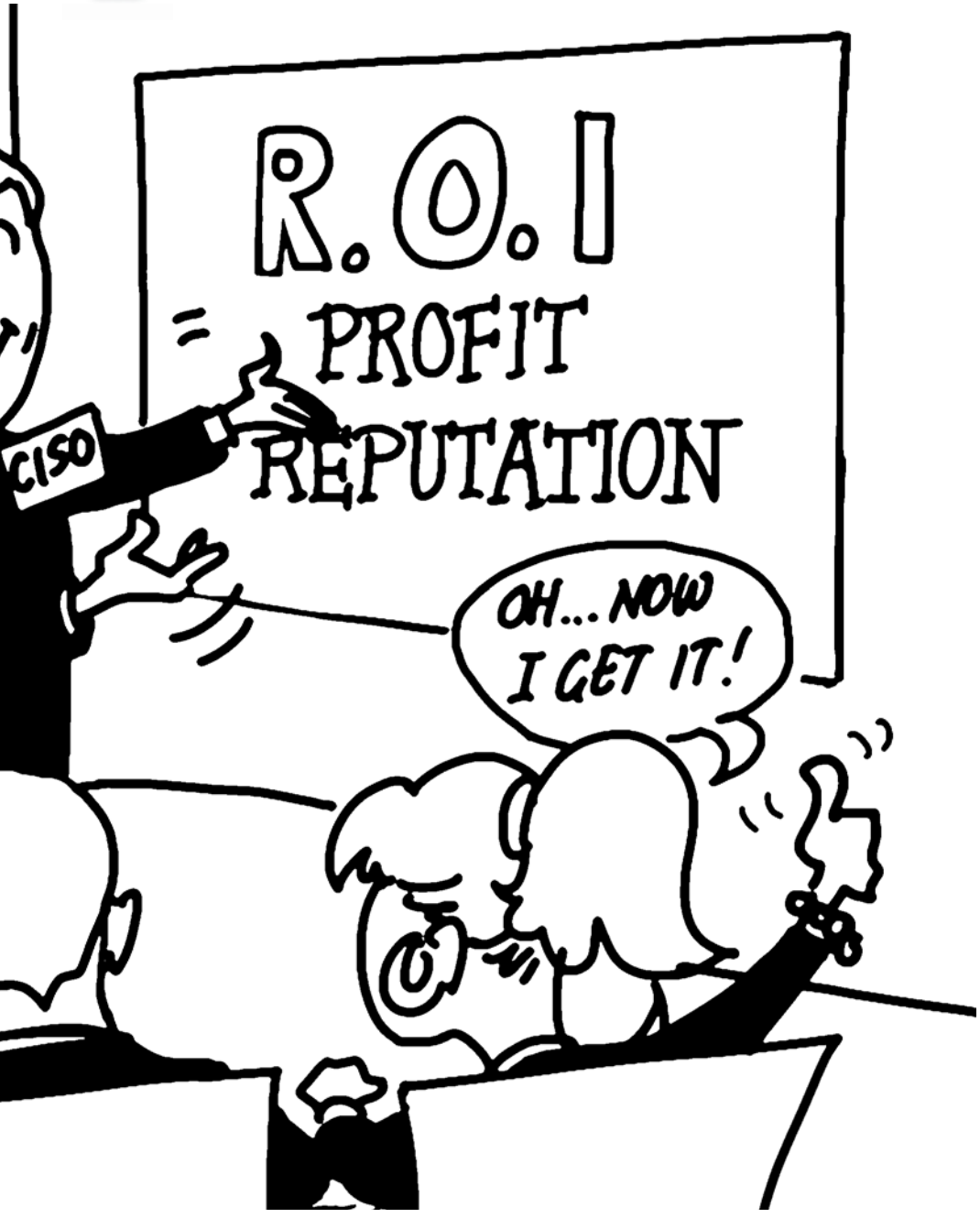
Alternatively, he says, he'd like to be a hipster bike builder and "grow a cool hipster beard." Almost as random as his recent obsession with growing a bonsai collection or interest in hydroponics to grow tomatoes and peppers six-times their normal size. No wonder he doesn't sleep much – he doesn't have the time.

Generally, as long as James is being "a massive geek", he's a happy man. "If I could just geek out all the time arbitrarily, that would be superb", he grins, but he's totally serious.

I want to end by sharing something that James says to me during the interview when explaining why computers are so amazing: "There's this orchestra of tiny mathematical operations of great simplicity that occur at such speed that they go up to that screen with the keyboard function, and the network and wireless, and the clock moving with beautiful graphics and amazing features, but all of it boils down to such simplistic transformation, and such a believable and comprehensive velocity. That is not only technologically remarkable but it's beautiful, I mean it's incredible." This strikes me as so very poignant, not just because it's an incredible way of articulating something so scientific, but because I imagine James' brain works in a similarly extraordinary way. James Lyne, you are truly one of a kind END

THE CISO OF THE GETTING DOWN TO

As the role that cybersecurity plays in the business environment grows, *Michael Hill* investigates how the job of the CISO will change from one which once solely oversaw technical solutions to one that will be ever-more business-orientated



FUTURE: BUSINESS

The profile of the Chief Information Security Officer (CISO) has evolved significantly over the last decade or so. With more and more organizations realizing just how important and big the task of protecting their data really is, the need for a lot of businesses to have a skilled, dedicated information security leader has changed from a convenient nicety to a critical element in the success and sustained well-being of a company.

In fact, as Andrew Hay, security expert and CISO, tells *Infosecurity*, the role of the CISO (or its equivalent) has become as close to an enterprise requirement as we can expect without a government mandate.

"The largest organizations in the world know that having a CISO is a required cost of doing business if they hope to retain customers' hearts, minds and dollars. This sentiment is beginning to trickle down from the biggest of the big to the mid-market organizations fighting tooth and nail to compete with incumbent firms, protect their intellectual property, and secure the transactional and analytical data generated by their customers", he says.

A maturing threat landscape coupled with the enhanced profile of the CISO is having a notable impact on the role itself. More than just increased pressure to protect and deliver in a demanding environment, the anatomy of the job is changing, most poignantly moving from one which once solely oversaw technical solutions for particular cybersecurity problems to one that is becoming far more business-orientated.

"The role of the CISO has always – and will always be – changing and evolving and the CISO will need to adapt to new demands and levels of accountability", explains Amanda Finch, general manager of the Institute of Information Security Professionals (IISP).

This trend will continue into the future, adds Dr Adrian Davis, EMEA managing director, (ISC)², with the role becoming ever more business-defined. "The challenge [for future CISOs] will be to have enough technical awareness and knowledge to be able to turn the business requirements into working security processes, procedures and technologies", he says.

Whether they originate from a traditional cyber-tech background or not, for future security leaders, being able to constantly understand, learn and adopt the various technological aspects of cybersecurity will always be important. However, what's evident is that this will not be the only thing keeping them busy.

As the role cybersecurity plays in the business environment grows, it will be just as – if not more – imperative for CISOs of the future to have the ability

> *"If the CISO learns to communicate in the language of business, their peers within the organization will likely be more receptive to future requests as they arise"*

to align cybersecurity with various elements of the wider business, and deal with the challenges that presents. This, as Hay argues, will be the greater test: "Technical aspects of technology are relatively easy [to learn]. Understanding the broader application to the business world, however, takes exposure and experience."

Well, there's no better place to start than at the top.

Getting on Board

As the prevalence of the CISO increases, so will their influence in the one place where key business decisions are made: the boardroom. "CISOs will increasingly be board members or similar," Finch explains. "This again comes back to the expected increase in desire for accountability."

This presents CISOs of the future with a real opportunity to become one of the key business leaders in the company, but having a seat on the board is one thing, using it to address key cybersecurity matters is quite another.

"CISO's have got to be able to express themselves and get the right outcome in the boardroom," Simon Hember, group business development director at Acumin Consulting, tells *Infosecurity*. "They have to be able to quantify cyber-risk, and also be able to monetize that risk so it is easily digestible for the board."

They will need to translate cybersecurity in a way that resonates with business leaders who don't speak XSS or SQL, but will connect with ROI, customer retention, company reputation and how security affects the bottom line. A strong understanding of those business matters along with the right business communication skills are therefore key. For too long, businesses have suffered from a disconnect between the C-suite and the realities faced by the IT security team, and it will be the responsibility of the CISO to change that.

"Technical jargon might impress but the presentation of a firm business case combined with a detailed risk or threat assessment will be much more impactful," Hay adds. "If the CISO learns to communicate in the language of business, their peers within the organization will likely be more receptive to future requests as they arise."

The Awareness Leader

Stepping into the wider echelons of a business, another significant challenge awaits the CISO: the issue of security awareness amongst staff and users.

In a survey at the Financial Services Information Security Network in 2016, the Network Group Events found that 82% of CISOs who attended were planning to invest in security awareness in the near future.

"Over the past few years, we have seen a radical shift in attitudes amongst CISOs towards user awareness training," Jake Summerfield, managing director of The Network Group Events, explains. "Whereas this practice has historically been seen as an inefficient and unproductive exercise in the workplace, user awareness training is now viewed as the most effective method of protecting corporate assets."

This paints an encouraging picture of what future security leaders will have within their remit. Historically, security awareness is an area that has drastically let companies down. As attacks become ever-more human-targeted, a greater focus on addressing insecure behavior to make the 'human firewall' a company's strongest security asset instead of its weakest link can only be a positive thing. However, to get it right, CISOs of the future must learn from mistakes of the past and, in many ways, the present.

The key is to realize that the people who make up a company's workforce are very diverse, with differing understandings of, and attitudes

> *"Technical security people would do well to invest in courses, training or books that help them grow in key business areas"*

Time for Tech

Although a CISO requires a lot more than just technology expertise, this does not mean that tech will not still have its place in the life of the CISO of the future – far from it!

Along with needing to communicate and understand technical issues to retain credibility with their subject matter experts (IT security team), future security leaders will need all the help that they can get to secure the massive amounts of customer data generated and aggregated in a safe, secure and transparent manner, which will inevitably include adopting and exploring new types of technology such as next-gen anti-virus, automated services/AI, blockchain and analytics platforms.

"The CISO needs to help the business understand the risks and exposure of new technology adoption from every angle", says Acumin's Hember.

However, as Andrew Hay explains: "Being a CISO in this day and age is not a static education role. One does not simply become a CISO and decide to not learn how to secure new technology. Unfortunately, with the lack of funds (and time), CISOs will be forced to self-educate through blogs, presentations, webinars and books – perhaps even paying for these resources out of their own pockets."

> *"The CISO and his/her reports will be more like project managers, managing resources to accomplish goals "*

towards, cyber-threats. Whilst the board will often share common goals for business success, the wider workforce is a far bigger, more varied pool of individuals to manage.

"You have to look at how people learn, and why they learn, and give them a reason to care," Chris Pogue, CISO at Nuix, explains. "Whether that's marketing, or sales, or administrative staff, they're not focused on security day in, day out, so you have to provide a reason for them to care. You need to give them an emotional hook, and once they are emotionally invested they will do just about anything."

Mind the Resource Gap

That's a strategy for managing the people already on board though, but what about dealing with what many consider to be the future CISO's biggest hurdle – the ever-widening cybersecurity skills gap?

With so many unfulfilled jobs in cybersecurity already, and a plethora of research suggesting the number is set to grow over the next five years, it would be naïve to think that a shortage of skilled staff isn't going to dramatically impact security leaders of the future.

Businesses have been guilty of chasing the 'five-year experience hires', deferring to experience to get the people they need. "Clearly, companies can no longer follow this policy and it will fall to the CISO to show leadership in resetting a talent strategy that includes investment in newcomers", argues Davis, whilst Finch adds that CISOs will also need to give more thought to "growing talent internally, either through apprentice schemes, graduate programs and cross training people from within the business."

However, the reality is that we have already moved beyond the point where creativity in recruitment alone can help CISOs and their companies meet the needs of the future. For example, businesses will not be spared the rod of regulatory fines (most notably those of the GDPR) if they fall foul of data privacy laws, and the excuse of 'we are under resourced' will not wash.

Therefore, as Morey Haber, VP of technology at BeyondTrust, argues, it will also fall on CISOs of the future to bring in and manage specialist services to help them meet demands, outsourcing certain aspects of the operation to service providers who deliver on scale to multiple organizations.

"The shortage of security professionals will warrant using partners, MSSPs, consultants and other shared resources to accomplish goals verses bringing the entire expertise in house", he says. "This means The CISO and his/her reports will be more like project managers, managing resources to accomplish goals verses reactive tactile responses."

A Learning Curve

As the future CISO embarks on a journey to become a business leader, and dealing with the business challenges that includes, the strongest quality they can demonstrate will be a willingness to constantly learn, grow and develop their skillset.

"Technical security people would do well to invest in courses, training or books that help them grow in key business areas," Hay advises. "This includes negotiating, leadership, conflict resolution, communications, business writing and human resource management. Not only will these skills be invaluable for their career progression, but it will also help them better understand the business as a whole."

If they get this right, adds Finch, the world can be their oyster and the role could have a lot of kudos and the opportunity to really influence at senior levels.

What's inescapably clear is that for CISOs of the future, the volume will be turned up on all levels providing a high-profile, high-pressure role for gifted people, but while the challenges will be vast, so will be the opportunities to succeed END

Q&A

CHARLIE MILLER

Charlie Miller has a PhD in mathematics, a CV that includes working at the NSA and is recognized as one of the best hackers in the world. Despite that, his dream to be an astronaut remains just that after NASA ignored his many job applications after grad school. Their loss. The former state champion cyclist now focuses on making autonomous vehicles resistant to cyber-attack.

What's the best thing about your job?

Securing things that affect people's physical safety. I've been writing computer exploits for over a decade and for the most part, these exploits could typically steal emails or photos or something. Once I wrote an exploit that could control a driving automobile, I realized that things were getting serious. This led me to switch to securing things rather than breaking them. Now I get to put all of my energy into trying to keep people physically safe from hackers, which is pretty cool.

What are you most proud of?

The after-effect of the Jeep hack we presented. It led to a recall of 1.4 million Fiat Chrysler vehicles and due to the changes they made to the way the cars communicate, they are much safer for everyone now.

Who do you really admire in the industry?

I really admired Barnaby Jack. He was the researcher who did the ATM hack and some of the first medical device hacking. He inspired me to work on high-profile targets and really led the way into thinking that lots of interesting things have computers (and vulnerabilities) besides just laptops or phones. If I could create an 'all-star' project team to work on a really tough but exciting project, I'd pick my buddy Chris Valasek, Mark Dowd – who is probably the best bug hunter in the world – and Joe Grand, an expert in all things hardware.

Tell me about a time when a hack went wrong

There are plenty of projects I've started and not been successful with. One that comes to mind is when I tried to hack laptop batteries (which I did) in order to make them catch fire (which I couldn't do). When I tried hacking a Palm Pre, I wasn't able to do it, despite later finding out there were some very serious and easy to find vulnerabilities in the product. I regret not learning more. I tend to be project-focused and learn [only] what I need to accomplish my goals. I wish I'd have spent more time learning about topics that I didn't necessarily need to know right away.

If you could change one thing about the information security sector, what would it be?

I'd love to see more women and minorities in the field. I'm not sure how to get there, but it is a goal our sector should push towards.

BIO

@0xcharlie

Dr Charlie Miller is a world-class white hat hacker. He was the first to hack both the iPhone and the first Android phone. Charlie won the Pwn2Own computer hacking contest four times. He found a vulnerability that would allow hacking into 1.4 million vehicles. He has worked for many high-tech companies including Twitter and Uber and is currently distinguished engineer, lead of Autonomous Transportation Security at Didi Chuxing.

infosecurity® EUROPE
06-08 JUNE 2017 OLYMPIA. LONDON.

Infosecurity Europe 2017

EVENT PREVIEW

Plan Your Time at Europe's Premier Information Security Conference and Expo

Guest speakers include:

Dame Stella Rimington
Former Director General of MI5
Opening Keynote. Day 1

Jeremy Paxman Broadcaster, journalist and author
Opening Keynote. Day 2

Featuring:

- Full Conference Programme
- Keynote Speakers
- Workshops and Training
- Floorplans
- A-Z Exhibitor List

Dame Stella Rimington

REGISTER NOW AT
www.infosecurityeurope.com

Jeremy Paxman

DOWNLOAD INFOSEC APP FOR FULL DETAILS

@infosecurity
#infosec

DOWNLOAD INFOSEC APP FOR FULL DETAILS

DOWNLOAD THE INFOSECURITY EUROPE APP

Everyone and everything you need to know about information security at your fingertips

Our NEW app features include:

- Full **conference agenda**
- Create and synchronise your **personal schedule**
- Speaker, exhibitor and sponsor **profiles**
- Interactive **floorplan**
- Activity feed featuring **p s** and **onsite discussions**
- Discover other participants and **connect**
- **Contact exhibitors** before, during and after the show
- **Live Q&A** during key conference sessions

@infosecurity
#infosec17

MAKE THE MOST OF YOUR VISIT

DOWNLOAD BEFORE YOU ARRIVE

infosecurity® EUROPE

06-08 JUNE 2017 OLYMPIA. LONDON.

Cybersecurity at the Speed of Business

With allegations of Russia hacking the democratic process in the USA, Yahoo revealing it had been the victim of the biggest data breach in history (twice) and a massive DDoS attack on Dyn via connected devices threatening to take down the internet, the events of 2016 served to highlight the increasing vulnerability of digitalised, connected systems, processes, devices and organisations.

At the same time, global economic and political uncertainty is rife with a new US administration, the fall-out from the UK's vote to exit the EU and the international rise of populism and armed conflicts around the world. All of these happenings raise questions about the future of national security and the role of cyber in it.

Against this backdrop, agile organisations are transforming, taking advantage of new technologies such as the cloud, mobile and IoT and adopting new working practices to achieve business objectives, efficiency and profitability. As organisations digitalise, the challenge for information security professionals is to keep pace and manage risk at the speed of business. Their role needs to be that of proactive enabler of the adoption of innovative technologies, rather than hinderer of digital business. As more infrastructure and applications fall outside the organisation's perimeter and out of the direct control of security teams as a result of business transformation, the need for effective governance and assurance over third party partners and suppliers has never been greater.

The pressure of regulatory oversight is also increasing with organisations ramping up their privacy and security policies and operations to ensure they are well positioned to comply with the EU GDPR and the NIS (Network and Information Security) Directive, both due to be implemented in 2018. However, according to research by Veritas Technologies, more than half of organisations are behind in their preparation to meet the demands of EU GDPR. With organisations facing potentially huge financial penalties, along with reputational damage in the event of a breach, the pressure really is on information security professionals to ensure that they protect their enterprise's sensitive data and are compliant with the regulation.

With innovative attackers and the boundaries blurring between physical and digital systems, the stakes are getting higher when it comes to the potential impact of a cyber-attack. The risk landscape continues to evolve rapidly and the role of cybersecurity is changing with risks being carried over into the real world, potentially impacting human safety. Whilst cyber-defenders try to keep pace with business transformation, they are also grappling with the challenge of keeping up with the professional cyber-criminal and responding to attacks. New technologies and innovations such as AI and Blockchain offer potential solutions, but their true value to cybersecurity is not yet known.

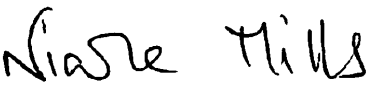
The theme of this year's Infosecurity Europe is **Cybersecurity at the speed of business.** The event will provide you with knowledge, insight and solutions you need to keep up with business transformation and is your opportunity to meet the information security community all under one roof. Providing tools, strategies and techniques to enhance the security maturity of your organisation, Infosecurity Europe brings together everyone and everything you need to know about information security.

As the highlight of the European information security event calendar, Infosecurity Europe offers you an unmissable chance to keep up with the strategic direction of the industry, catch-up with your peers, connect with vendors and service providers, find out about the latest technological solutions and develop your career.

This year, Infosecurity Europe will offer even more opportunities to discover something different, be that at a networking event or in our new Talking Tactics theatre. Our new Infosecurity Week portal is also here to support the industry. Featuring all the activities in and around London during the week of the event, make the most of your visit by checking out what's going on or list your own event to tell others what you're up to.

With so much on offer I hope you will join us at this inspiring annual gathering of the community.

I look forward to welcoming you to Olympia London in June.



Nicole Mills,
Portfolio Director

WHAT'S ON AND WHERE: MONDAY-TUESDAY WEDNESDAY-THURSDAY FRIDAY...

Infosecurity Week is a city-wide landmark event bringing Infosecurity professionals together to learn, explore and have fun in and around London during the week of 5-11th June 2017.

Check out what's on during this busy week and sign up to attend anything from specialist conferences, training courses, networking events, vendor parties, awards ceremonies and much more. There's a whole host of reasons to make your way to London in June 2017.

You can get involved by partnering, sponsoring, participating or simply listing your event. Full details at www.infosecurityeurope.com/infosecurityweek.

BROWSE THE FULL LINE UP OF EVENTS

BUY YOUR TICKETS

LIST YOUR EVENT FOR FREE

With more events added every day, make sure to check regularly for the latest announcements.

Visit www.infosecurityeurope.com/infosecurityweek

infosecurity® WEEK

Recommended for You

With so much happening at Infosecurity Europe 2017, it's hard to know where to start. We've highlighted below some of the key features not to miss depending on your role and experience. Login to **My Event** at **www.infosecurityeurope.com** to create your own personal schedule

Are you new to the industry?

- **Login and plan your visit:** Use My Event before the show to plan which conference sessions to attend and build an agenda that suits your needs. Connect with your peers and set-up meetings using the mobile app.
- **Learn and earn CPE/CPD credits:** With eight theatres onsite, plus workshops and training, there's something for everyone. All sessions are accredited for CPE/CPD credits by (ISC)², ISACA and EC-Council.
- **Exhibitor recommendations:** All visitors will receive personalised recommendations of exhibitors matching their product interests. Keep an eye out for these just before the show and contact exhibitors to set up meetings or request information.
- **Hear about new technologies:** As well as taking in the main exhibition floor, don't miss the Discovery Zone and Cyber Innovation Zone on the upstairs Gallery, featuring 100+ companies showcasing the latest innovations. The Tech Talks theatre is also a good place to drop in, with top-quality curated content featuring the latest technical insight.

Are you in a technical role?

- **Get in-depth technical know-how:** For technical insight, attend the Tech Talks and Intelligent Defence sessions and speak to technical experts on the exhibitor stands.
- **Post questions & start discussions:** Download the Infosec mobile app to start engaging with the whole community. Our Activity Feed is one of the most popular features - find out why on our brand new mobile app, available from early May 2017.
- **Find out what's new:** Head upstairs to the Discovery Zone and Cyber Innovation Zones. To hear about the latest technologies, catch presentations in Cyber Innovation Showcase and Technology Showcase.
- **Make sure you see the right people:** Use My Event to set up meetings with target exhibitors and your peers, and make sure to talk to technical experts in information security.

Are you in a business role?

- **Network with peers & vendors:** With two networking bars and brand new features on our mobile app, there are now more ways to connect with the community than ever. Download the new mobile app or login to My Event online and start to create your perfect personalised tour of Infosecurity Europe.
- **Discover new innovation:** If you're looking for something new at Infosec, head upstairs to visit the Discovery Zone and Cyber Innovation Zone. Featuring 100+ companies, you'll get a view of the latest industry talent.
- **Catch a Conference session:** This year's programme has been carefully curated to offer the latest, most relevant content on eight stages. Plus, new for 2017, is Talking Tactics, a whole day of case studies and 'how to' sessions where you can learn from real life experiences on Thursday 8th June.
- **Meet & Seat:** Set up meetings with guaranteed space whenever you need it. Book a Meet & Seat table with dedicated wifi and refreshments so you can easily meet with peers, suppliers and clients. With everyone and everything under one roof, it's easy to make valuable connections.

infosecurity® EUROPE LEADERS PROGRAMME

As an Infosecurity Leader, you'll be first in the queue at Infosecurity Europe and enjoy a host of benefits onsite including:

1. Exclusive access to the Infosecurity Leaders Lounge with wifi and concierge service
2. Invitations to peer-to-peer networking opportunities
3. Fast-track entry and reserved seating in the conference sessions
4. A seat at the 'off-the-record' members-only roundtable programme
5. Dedicated contact person to ensure you have everything you need before, during and after the show
7. Tours of our Discovery and Cyber Innovation Zones featuring 100+ next generation cybersecurity companies

Apply to join our Leaders Programme at www.infosecurityeurope.com/leaders

Please note: The Infosecurity Leaders Programme has strict membership criteria and the organisers reserve the right to decline your application

Make the most of your time

Reserve Your Seat

Guarantee your seat at sessions in the Keynote Stage, Information Security Exchange, Strategy Talks and Tech Talks.

Plan Your Visit

Check out the full agendas and start creating your schedule ahead of time to ensure you make the most of your time away from the office. Login to My Event at **www.infosecurityeurope.com** to shortlist your favourite exhibitors and conference sessions to your personal calendar.

Network & Engage

Download the mobile app to set-up meetings in advance and network and engage with your peers and vendors on the day.

TREND MICRO™

Go Beyond Next-Gen

Smart, optimised and connected security for your hybrid cloud environments, network and endpoints.

IDC
Analyze the Future

Global server security market leader 7 years in a row

NSS Labs
RECOMMENDED

Top score in breach detection 3 years in a row

www.trendmicro.co.uk/xgen


POWERED BY
XGen™
SECURITY


17
SITS
THE SERVICE DESK
& IT SUPPORT SHOW
7-8 JUNE 2017
OLYMPIA, LONDON
DON'T MISS IT
TRANSFORM YOUR
IT SERVICE DELIVERY
The UK's leading event for
IT Service Management
& Support Professionals
FREE
to attend
Sponsored by:
SDI Service Desk Institute
Supported by:
itSMF UK
The IT Service Management Forum
FREE SEMINARS | FREE KEYNOTES | 75+ ITSM SUPPLIERS | 3500 IT PROS
ORDER FREE TICKETS TODAY
www.servicedeskshow.com

@InfosecurityMag

INSPIRATIONAL KEYNOTE SPEAKERS

The Keynote Stage once again brings you a host of diverse sessions addressing the biggest industry challenges. Take some time to hear fresh perspectives and see your infosecurity heroes in action; the line-up is hand-picked after extensive research with the infosec community, to make sure we address the topics that are important to you.

Opening Keynote: Day 1
Dame Stella Rimington,
Former Director General of MI5

Opening Keynote: Day 2
Jeremy Paxman,
Broadcaster and Journalist

Below are just a few of the inspirational thought-leaders and expert practitioners who will be sharing their expertise on the Keynote Stage across all three days.

To reserve a seat visit:
www.infosecurityeurope.com

Dame Stella presents **Open Secret.** Drawing on her experience as the first female Director General of MI5, a position she held until 1996, Dame Stella will discuss her fascinating career in the security service and her work in counter-subversion, counter-espionage and counter-terrorism.

Jeremy presents **Governments, Businesses & Other Scoundrels: Why Trust Anyone?** Drawing on his expertise in current affairs, politics and history he shares his perspective on the notion of trust in the modern world. Can we and indeed, should we trust anyone?

Bruce Schneier, Security Technologist, Infosecurity Europe Hall of Fame Alumnus

Keynote speaker: **Spotlight on Disruptive Technologies: Artificial Intelligence & Machine Learning: Cybersecurity Risk vs Opportunity?**

- Wednesday 7th June: 11.05-11.45

Professor Angela Sasse, Director, UK Research Institute in Science of Cyber Security (RISCS), **UCL**

Keynote speaker & panellist: **Psychologist Insight - Understanding User Behaviour & Motivations**

- Tuesday 6th June: 12.15-13.40

Bret Arsenault, CISO, **Microsoft**

Keynote speaker: **How Microsoft Secures Data & Protects User Privacy**

- Tuesday 6th June: 15.40-16.20

James Lyne, Security Researcher

Keynote speaker & panellist: **Countering Ransomware – When Should you Pay the Ransom?**

- Tuesday 6th June: 13.55-15.25

Jaya Baloo, CISO, **KPN Telecom**

Keynote speaker: **Spotlight on Disruptive Technologies: What does Blockchain Mean for Cybersecurity?**

- Wednesday 7th June: 12.00-12.40

Helen Rabe, Head of Information Security - Strategy, Risk & Compliance, **Costa Coffee**

Panellist: **Privacy, Security and EU GDPR: Practitioners' Guide to Compliance**

- Wednesday 7 June: 14.10-15.30

Stuart Hirst, Head of IT Security, **Skyscanner**

Panellist: **Building an Agile Security Team for the Future**

- Tuesday 6th June: 11.05-12.00

Dr Jessica Barker, Cybersecurity Consultant

Panellist: **Practical Tactics to Change User Behaviour & Create a Secure Culture**

Tuesday 6th June: 12.15-13.40

Peter Brown, Senior Technology Officer, **Information Commissioner's Office (ICO)**

Speaker & Panellist: **EU GDPR Benchmark - Where Should Your Organisation be Now?**

- Wednesday 7 June: 14.10-15.30

Adrian Asher, CISO, **LSEG**

Panellist: **Securing the Code: Building Resilience, Security & Agile into Coding, Design & Development**

- Wednesday 7 June: 16.35-17.25

Senior Speaker, NCSC

Keynote speaker & panellist: **Getting to Know the Cyber Adversary**

- Tuesday 6th June: 13.55-15.25

Cameron Craig, Deputy General Counsel, Group Head of Data Privacy, **HSBC**

Panellist: **Privacy, Security and EU GDPR: Practitioners' Guide to Compliance**

- Wednesday 7 June: 14.10-15.30

Emma Smith, Group Technology Security Director, **Vodafone**

Panellist: **SOC 2020: Building a Robust SOC Capability to Detect & Respond**

- Thursday 8 June: 10.55-11.45

Infosecurity Europe Hall of Fame

The Infosecurity Europe Hall of Fame celebrates the achievements of internationally recognised information security visionaries, luminaries, practitioners and advocates.

Join **Professor Mary Aiken, 2017 Infosecurity Europe Hall of Fame inductee** in conversation with Eleanor Dallaway, Editor & Publisher of Infosecurity Magazine. During this session Professor Aiken will discuss her career as a forensic cyberpsychologist, her current research projects, share insights on future threats and the importance of human factors in information security.

- Thursday 8th June, 13.45-15.25

Visit www.infosecurityeurope.com to start building your personalised programme using My Event. From conference sessions, exhibitors to meet or to check out other attendees, it's all online!

RESERVE YOUR SEATS NOW

KEYNOTESTAGE

Cybersecurity at the Speed of Business

For the latest programme and speaker updates visit **www.infosecurityeurope.com/keynote**

Against a backdrop of global economic and political uncertainty, organisations are transforming, taking advantage of new technologies and working practices to enhance business agility, efficiency and profitability. As organisations connect, evolve and digitize, new attack vectors are emerging, ready to be exploited by the sophisticated cyber-criminal. The challenge for information security professionals is to keep pace with the speed of business change, enabling the business whilst enhancing the maturity of its information security.

The Keynote Stage will analyse the challenges of developing an agile security strategy that can keep pace with business transformation and the evolving threat landscape. The sessions will provide strategic and tactical advice on how to address these challenges.

Actionable, practical takeaways

By attending the Keynote Stage sessions you will gain practical, actionable takeaways that can be applied directly to your business.

Insight, ideas and inspiration

Get direct access to information security knowledge and expertise presented by some of the industry's leading end-user practitioners, policy-makers, analysts and thought-leaders. Acquire new ideas, insight and inspiration to enable you to streamline your information security strategy, accelerate the effectiveness of your security tactics and reinforce the critical position of the information security function.

Themes to be addressed in the 2017 Keynote Stage agenda include:

- **Managing the human risk:** Analyse user behaviour and discover how to change it
- **Building an agile security team:** Understand the skills required for an effective team, how to attract and retain staff and which skills you need to be developing to enhance your career
- **Securing critical information assets and achieving compliance:** Benchmark your organisation's compliance to EU GDPR; discover how to secure your organisation's critical data both on-premise and in the cloud; analyse the evolution of privacy and security functions
- **Disruptive technologies:** Get to grips with Blockchain and AI and understand what they mean for information security
- **Building a cyber-resilient enterprise:** Discover how to build an effective SOC capability and identify new approaches to cyber incident response

Day One: Tuesday 6 June

10.00-10.50
Opening Keynote Presentation
Open Secret
Dame Stella Rimington

11.05-12.00
Panel Discussion
Building an Agile Security Team for the Future

Panellists:
Vicki Gavin, *Compliance Director, Head of Business Continuity and Information Security, The Economist Group*
Stuart Hirst, *Head of IT Security, Skyscanner*
Mahbubul Islam, *Head of Secure Design, Department of Work & Pensions (DWP)*
Paul Watts, *CISO, Network Rail*

Moderator:
Adrian Davis, *Managing Director EMEA, (ISC)²*

This session will include the White Hat Charity Cheque Presentation.

12.15-13.40
Securing the User Special Focus – Extended Session
This specially extended session will get to grips with the challenges of driving security culture within an organisation. The session will begin with a psychologist's presentation which will analyse the behaviour of users and their motivations. It will be followed by a panel discussion sharing practical techniques to change user behaviour and create a security culture.

Psychologist Insight
Understanding User Behaviour & Motivations
Professor **Angela Sasse**, *Director, UK Research Institute in Science of Cyber Security (RISCS), UCL*

Panel Discussion
Practical Tactics to Change User Behaviour & Create a Secure Culture

Panellists:
Dr Jessica Barker, *Cybersecurity Consultant*
Jonathan Kidd, *CISO, Hargreaves Lansdown*
Professor Angela Sasse, *Director, UK Research Institute in Science of Cyber Security (RISCS), UCL*
Additional panellist to be announced

Moderator:
Stephen Bonner, *Partner, Deloitte, Inosecurity Europe Hall of Fame Alumnus*

13.55-15.25
Risks, Threats & Adversaries: What (or Who) Should You Be Worried About? - Extended Session
This specially extended session will delve into the threat landscape and provide you with different perspectives on some of the latest threats and challenges and how to overcome them.

Presentation 1: **Getting to Know the Cyber Adversary**
Senior Speaker, NCSC

Presentation 2: **Attack Vectors: Latest Trends & Implications for Cyber Defence Strategies**
Rik Ferguson, *Special Advisor, Europol EC3, Infosecurity Europe Hall of Fame Alumnus*
Presentation 3: **Countering Ransomware – When Should You Pay the Ransom?**
James Lyne, *Security Researcher*

Moderator:
Peter Wood, *Security Advisory Group, ISACA*

15.40-16.20
Keynote Presentation
How Microsoft Protects Data and User Privacy
Bret Arsenault, CISO, Microsoft

16.35-17.25
Panel Discussion
Securing the Code: Building Resilience, Security & Agile into Coding, Design & Development

Panellists:
Adrian Asher, *CISO, LSEG*
Lee Barney, *Head of Information Security, Marks & Spencer*
Additional panellists to be announced

Moderator:
To be announced

Day Two: Wednesday 7 June

10.00-10.50
Opening Keynote Presentation
Governments, Businesses & Other Scoundrels: Why Trust Anyone?
Jeremy Paxman, *Journalist & Broadcaster*

11.05-11.45
Keynote Presentation
Spotlight on Disruptive Technologies: Artificial Intelligence & Machine Learning: Cybersecurity Risk vs Opportunity?
Bruce Schneier, *Security Technologist, Infosecurity Europe Hall of Fame Alumnus*

12.00-12.40
Keynote Presentation
Spotlight on Disruptive Technologies: What does Blockchain Mean for Cybersecurity?
Jaya Baloo, *CISO, KPN Telecom*

12.55-13.55
UK's Most Innovative Small Cybersecurity Company of the Year: Competition Final
During this session the finalists from the national competition supported by the Department for Culture, Media & Sport, will pitch their technology/service to the Keynote Stage audience and an expert judging panel. The judging panel will select the winner and award the title of 'UK's Most Innovative Small Cybersecurity Company of the Year'.

Judges:
David A. Cass, *Vice President & CISO, Cloud & SaaS Operational Services, IBM*
Additional judges to be confirmed

14.10-15.30
EU GDPR Special Focus – Extended Session
This specially extended practical session will examine the EU GDPR, providing the opportunity to benchmark your organisation and learn best practice tips from a panel of practitioners.

Regulatory Briefing
EU GDPR Benchmark - Where Should Your Organisation be Now?
Peter Brown, *Senior Technology Officer, ICO*

Panel Discussion
Privacy, Security and EU GDPR: Practitioners' Guide to Compliance

Panellists:
Helen Rabe, *Head of Information Security - Strategy, Risk & Compliance, Costa Coffee*
Cameron Craig, *Deputy General Counsel - Data Privacy & Digital - Group Head of Data Privacy, HSBC*
Peter Brown, *Senior Technology Officer, ICO*

Moderator: **Brian Honan**, *CEO, BH Consulting, Infosecurity Europe Hall of Fame Alumnus*

15.45-16.35
Panel Discussion
Securing Cloud 4.0: New Approaches to Protect Data in the Cloud

Panellists:
Daniele Catteddu, *CTO, Cloud Security Alliance*
Mark Jones, *CISO, Allen & Overy*
Anton Karpov, *CISO, Yandex*

Moderator:
Bob Tarzey, *Analyst 7 Director, Quocirca*

16.50-17.25
Case Study Presentation
How to Manage Critical Data Assets Through Risk Prioritisation, Without Forgetting Compliance

Asim Fareeduddin, *Vice President, IT Security & Regulatory Controls Assurance, RELX Group*
Jason Miller, *Information Security Assurance Manager, RELX Group*

Day Three: Thursday 8 June

10.00-10.40
Opening Keynote Presentation
Details to be Announced

10.55-11.45
Panel Discussion
SOC 2020: Building a Robust SOC Capability to Detect & Respond

Panellists:
Chris Gibson, *CISO, Close Brothers*
Adrian Gorham, *Director of Business Operations, Telefónica UK*
Russell Wing, *Head of Information Security, LME*
Emma Smith, *Group Technology Security Director, Vodafone*

Moderator:
Dan Raywood, *Contributing Editor, Infosecurity Magazine*

12.00-13.30
Live Incident Scenario
Cyber Attack Survival Guide: Fostering Cyber Resilience Within the Organisation

Panellists:
David Boda, *Head of Information Security, Camelot*
Andrew Gould, *Detective Chief Inspector, Falcon – SCO7 Organised Crime Command (OCC), Metropolitan Police Service*
Joseph da Silva, *Director of Information Security, Centrica*
Duncan Gallagher, *Europe & CIS Crisis Practice, Edelman*
Additional panellists to be confirmed

Facilitator:
Richard Horne, *Partner. PwC*

13.45-14.30
Infosecurity Europe Hall of Fame 2017
Professor Mary Aiken is recognised for her long-term contribution to the information security sector as the world's leading expert in Forensic Cyberpsychology, her work as an advocate and educator in information security and her role in raising the profile of the information security sector. Join Eleanor Dallaway, Editor & Publisher of *Infosecurity* Magazine in conversation with Professor Aiken.

2017 Infosecurity Europe Hall of Fame inductee:
Professor Mary Aiken

Interviewer:
Eleanor Dallaway, *Editor & Publisher, Infosecurity* Magazine

Infosecurity Europe Hall of Fame 2017

Keynote Stage, Thursday 8th June, 13.45-14.30

Join Professor Mary Aiken, 2017 Infosecurity Europe Hall of Fame inductee in conversation with Eleanor Dallaway, Editor & Publisher of *Infosecurity* Magazine on the Keynote Stage on Thursday 8th June at 13.45-14.30.

During this session, Professor Aiken will discuss her career as a forensic cyberpsychologist, her current research projects, and will share insights on future threats, and the importance of human factors in information security.

The Infosecurity Europe Hall of Fame celebrates the achievements of internationally recognised information security visionaries, luminaries, practitioners and advocates.

Industry luminaries who have been recognised in the Infosecurity Europe Hall of Fame include Mikko Hypponen, Bruce Schneier, Shlomo Kramer, Professor Fred Piper, Whitfield Diffie, Dan Kaminsky, Eugene Kaspersky, the late Professor Howard Schmidt and Phil Zimmerman.

RESERVE YOUR SEATS NOW

STRATEGYTALKS

Discover how to develop a robust security strategy to secure the transforming business

For the latest programme and speaker updates visit www.infosecurityeurope.com/strategytalks

Strategy Talks sponsor

Symantec.

Day One: Tuesday 6 June

10.00 – 10.25
Financial Institutions on High Alert for Cyber-Attacks - How Effective IT Security Monitoring Fosters Resilient Financial Institutions
Harald Reisinger, *Managing Director, RadarServices Smart IT-Security*

10.40- 11.05
Building an IR Capability to Meet Modern Threats & Comply with GDPR
Steve Armstrong, *Technical Security Director, Logically Secure*

11.20 – 11.45
Re-Centring the Value of Security (or The Law of Unintended Consequences)
Darren Thomson, *CTO and Vice-President of Technology, EMEA, Symantec*

12.00 – 12.25
Managing Security Risk at the Speed of Business, Not the Speed of Spreadsheets
Nik Whitfield, *CEO, Panaseer*

12.40 – 13.05
Achieving Cyber Resilience in 2017
Paul Ayers, *GM, EMEA, IBM Resilient*

13.20 – 13.45
Empowering the Entire Enterprise via Threat Hunting
Rick McElroy, *Security Strategist, Carbon Black*

14.00 – 14.25
Securely Connecting a Global Workforce to the Cloud - an Inside View
Sébastien Huet, *CTO, Rémy Cointreau*
Xavier Leschaeve, *Global CISO, Rémy Cointreau*

14.40 – 15.05
Skyscanner Case Study - How to Build a Robust and Flexible IAM Strategy
Michael Newman, *CEO, My1Login*
Stuart Hirst, *Head of IT Security, Skyscanner*

15.20 – 15.45
The Communications Disconnect: What Separates You From Your Boss?
Jonathan Draper, *Head of Cyber Defence Strategy, BAE Systems Applied Intelligence*

16.00 – 16.25
How to Effectively Manage Your Risk in an Era of Cyber Extortion
Stephen Gates, *Chief Research Intelligence Analyst, NSFOCUS*

16.40 – 17.05
How to Embrace the Internet Of Things (IoT) Opportunity, Whilst Controlling the Expanding IT Security Attack Surface
Bob Tarzey, *Analyst & Director, Quocirca, speaking on behalf of ForeScout Technologies*

Day Two: Wednesday 7 June

10.00 – 10.25
Information Security Compliance Training - the Good, Bad & Indifferent
Darren Hockley, *Managing Director, DeltaNet International*

10.40 – 11.05
People: The Strongest Link
Emma W, *People-Centred Security Team Lead, National Cyber Security Centre*

11.20 – 11.45
GDPR, Brexit & Security: Making it All Work
Ilias Chantzos, *Senior Director EMEA & APJ Government Affairs, Symantec*

12.00 – 12.25
Connecting the Dots: The Four Dimensions of Data Breaches
Stuart Clarke, *Chief Technical Officer, Nuix Technology UK*

12.40 – 13.05
DevSecOps – Building Continuous Security into IT & App Infrastructures
Chris Carlson, *Vice President, Cloud Agent Platform, Qualys*

13.20 – 13.45
So, You Think You're Ready for the EU GDPR? Three Tips to Make Sure You've Future-Proofed Your Approach
Tony Pepper, *CEO, Egress Software Technologies*

14.00 – 14.25
CISO Confessions: Security Lessons Learned from Modern Day Cyber-Attacks
David Meltzer, *CTO, Tripwire*
Martin Whitworth, *Research Director, IDC*
Stephen Khan, *Head of information Security Strategy & Architecture, RBS*
Thom Langford, *CISO, Publicis Groupe*

14.40 – 15.05
Artificial Intelligence and Smart Devices – The New Frontier of Cyber Warfare
Dave Palmer, *Director of Technology, Darktrace*

15.20 – 15.45
Cloud-Ready Security: 3 Steps to Optimise Your Cloud Environment
Hatem Naguib, *SVP & Head of Security, Barracuda Networks*

16.00 – 16.25
The Security Supply Chain for IoT Devices
Ralf Huuck, *Director & Senior Architect, Synopsys*

16.40 – 17.05
How to be Employed at the SOC of Tomorrow… Today
Ryan Kovar, *Staff Security Strategist, Splunk*

Day Three: Thursday 8 June

10.00 – 10.25
Shadow Admins: Underground Accounts That Undermine The Network
Lavi Lazarovitz, *CyberArk Research Lab Team Leader, CyberArk*
Asaf Hecht, *Cyber Security Researcher, CyberArk*

10.40 – 11:05
Business Process Compromise Attacks – The Next Generation Threat to Your Organisation
Morton Swimmer, *Senior Threat Researcher, Trend Micro*

11.20 – 11.45
Security for the Cloud Generation
Michael Mauch, *Global Solutions CTO, Symantec*

12.00 – 12.25
Being the Fly on the Wall – Experience from (ISC)² Members' GDPR Task Force
Yves Le Roux, *Co-Chair and Policy Workgroup Lead, (ISC)² EMEA Advisory Council*
Adrian Davis, *Managing Director EMEA, (ISC)²*

12.40 – 13.05
Session details to be announced, visit www.infosecurity.com/strategytalks

13.20 – 13.45
3 Greatest Threats to Cyber Resiliance & How to Overcome Them
Andy Norton, *Risk Officer, SentinelOne*

14.00 – 14.25
Why the Commercialisation of Crimeware Demands a New, Threat-Centric Approach to Vulnerability Management
Ravid Circus, *VP Products, Skybox Security*

14.40 – 15.05
Covering Your Assets
Andy Burston, *Security Specialist, Huntsman Security*

15.20 – 15.45
Achieving Enhanced Security While Driving Business Growth with the Power of Identity
Darran Rolls, *CTO & CISO, SailPoint*

TECHTALKS

RESERVE YOUR SEATS NOW

Gain the technical tools, techniques & skills to protect your organisation

Tech Talks sponsor

CISCO

For the latest programme and speaker updates visit www.infosecurityeurope.com/techtalks

Day One: Tuesday 6 June

10.00 – 10.25
Biometric Analysis: A New Dimension to Continuous Authentication
Balázs Scheidler, *Co-founder & CTO, Balabit*

10.40- 11.05
Two-factor Authentication in Android, iOS & Windows 10 Mobile Devices
Oleg Afonin, *Researcher, ElcomSoft*

11.20 – 11.45
Ways to Make Your Security Management Simple
Presented by Cisco

12.00 – 12.25
The All Encompassing World of Botnets
Mark James, *Security Specialist, ESET*

12.40 – 13.05
Hybrid Cloud Secure Network Integration: Tips & Techniques
Gur Shatz, *CTO & Co-Founder, Cato Networks*

13.20 – 13.45
Scaling-Up and Automating Web Application Security
Ferruh Mavituna, *CEO & Founder, Netsparker*

14.00 – 14.25
The Top 4 Ways Vulnerabilities Creep Into Your Software
Maria Loughlin, *SVP of Engineering, Veracode*

14.40 – 15.05
Threats of Tomorrow: Using AI to Predict Malicious Infrastructure Activity
Staffan Truvé, *CTO, Recorded Future*

15.20 – 15.45
IoT - The Consumer Skynet, a Corporate Liability, or the Best Thing Since Free Wi-Fi?
John Stock, *Senior Cyber Security Analyst, Outpost24*

16.00 – 16.25
DDoS on the Frontline: How to Plan & Prepare for a DDoS Attack – with Three Real-Life Customer Case Studies
Raza Rizvi, *Technical Director, activereach*

16.40 – 17.05
How to Build a Secure, Enterprise-class Containers' Architecture
Ghaleb Zerki, *NSX Senior Systems Engineer, EMEA Technology Practices NSX Specialist Team, VMware*

Day Two: Wednesday 7 June

10.00 – 10.25
Defeating & Abusing Machine Learning-based Detection Technologies
Oliver Tavaholi, *CTO, Vectra Networks*

10.40 – 11.05
The Malicious Network of Things
Snorre Fagerland, *Principal Senior Security Researcher, Symantec*
Waylon Grange, *Senior Threat Researcher, Symantec*

11.20 – 11.45
Insights into the Mind of a Hacker
Presented by Cisco

12.00 – 12.25
Making Sense of Web Attacks: From Alerts to Narratives
Amichai Shulman, *CTO, Imperva*

12.40 – 13.05
Hacking Exposed: Real-World Tradecraft of Bears, Pandas & Kittens
Adam Meyers, *Vice President, Intelligence, Crowdstrike*

13.20 – 13.45
Malware Red Alert: The First 24 Hours
Steve Shepherd MBE, *CSIR Senior Consultant, 7Safe*

14.00 – 14.25
The Magnificent FIN7: Revealing a Cyber-criminal Threat Group
John Miller, *Manager for Cyber Crime Intelligence, FireEye*
Barry Vengerik, *Principal Threat Analyst, FireEye*

14.40 – 15.05
On the Hunt for Advanced Attacks? Command & Control Channels are a Good Place to Start
Moshe Zioni, *Security Research Manager, Verint*

15.20 – 15.45
Stop Chasing Ephemeral IOCs & Increase the Lifetime of your Threat Intelligence
Dhia Mahjoub, *Principal Engineer, Cisco Umbrella*

16.00 – 16.25
Cyber Reasoning Systems – A New Era of Automated Defence
Neil Thacker, *Deputy CISO, Forcepoint UK*

16.40 – 17.05
A Leak in the Dike is all it Takes to Break the Dam
Brandon Hoffman, *CTO, Lumeta Corporation*

Day Three: Thursday 8 June

10.00 – 10.25
Protecting Your Mobile Apps Across the App Store Ecosystem
Terry Bishop, *Solutions Architect, EMEA, RiskIQ*

10.40 – 11:05
The DDoS Consideration for SDN Deployments
Sean Newman, *Director, Product Management, Corero Network Security*

11.20 – 11.45
Defending Against the Threats You Currently Can't Address
Presented by Cisco

12.00 – 12.25
The Truth About What's on Your Network Using Threat Correlation
Marc Laliberte, *Information Security Threat Analyst, WatchGuard Technologies*

12.40 – 13.05
Could a Few Lines of Code <F!#ck> it All Up?
Amit Ashbel, *Cyber Security Evangelist, Checkmarx*

13.20 – 13.45
Hurricanes, Earthquakes & Threat Intelligence
Jonathan Couch, *SVP Strategy, ThreatQuotient*

14.00 – 14.25
Incident Responder's Field Guide - Lessons From an F100 Incident Responder
Tim Bandos, *Director of Cybersecurity, Digital Guardian*

14.40 – 15.05
How to Explain Cryptography Without Using Any Big Words
Paul Ducklin, *Senior Technologist, Sophos*

15.20 – 15.45
Are you at the Office? An Analysis of CEO Scams in the Wild
Davide Canali, *Senior Threat Analyst, Proofpoint*

ADVERTORIAL

Steps to Solving the IoT Security Problem

Steve Mulhearn

Director Business Development, Fortinet
@Fortinet

According to research from Strategy Analytics, by 2020 there will be 4.3 internet-connected devices for every human on the planet. Most Internet of Things (IoT) devices were never designed with security in mind, and thus include a multitude of vulnerabilities such as weak authentication and authorization protocols, insecure software and firmware, poorly designed connectivity and communications and very little security configurability.

The sheer volume of IoT devices and the ease by which they can be weaponized now makes them a serious threat to any organization trying to protect sensitive data. The issue is only aggravated by the growing landscape of devices, as more everyday devices are upgraded to smart devices and more people are bringing multiple personal devices into the workplace in order to increase efficiency. As these devices are deployed more widely, securing them requires visibility and control across highly distributed ecosystems.

How exactly are these devices being compromised? Nearly every new device being added to the internet now has its own operating system (OS). Unlike PCs and other computing hardware, these devices are not being regulated and controlled by standardized OSs. We are already seeing these vulnerabilities being exploited by criminals, with printers and routers topping the list of the most exploited devices in Fortinet's latest *Global Threat Report*.

A network of compromised IoT devices can be misused for a number of malicious activities, including DDoS attacks, cyber-warfare, spying, reconnaissance, spreading malware, coordinating advance persistent threats and more. Also, as seen in the recent high-profile IoT-based Mirai DDoS attack, vulnerabilities in the operating systems of CCTV cameras and DVRs can be exploited to carry out these attacks.

Many IoT devices are currently being manufactured as 'headless' which means they cannot be patched, so other security measures will have to be developed, especially in lieu of an established regulatory environment. Whilst legislative bodies in Europe and the US have begun to take the issue seriously and propose new laws and standards, they have yet to fully mature.

Such security measures present a major challenge for today's enterprises and data that traverses many different types of devices and environments from tablets to cloud applications. The challenge with current point products and platform security solutions is that they often lack the visibility and wider network integration necessary to see and then secure the IoT.

To successfully defend against the threats faced by the expansive scope of IoT and the cloud, organizations will need to implement a security fabric which can protect the entire infrastructure and offer comprehensive visibility, segmentation and end-to-end protection. Such a fabric must include three strategic network security capabilities in order to ensure maximum protection for the infrastructure against evolving IoT threats.

1. Firstly, businesses should seek to establish strong access controls to identify and inspect IoT devices and traffic which is connecting to the network. Enterprise security solutions can provide real-time discovery and classification of devices and allows the network to build up risk profiles which can be automatically assigned to IoT device groups along with the appropriate policies.
2. Once armed with complete visibility and management abilities, it is pivotal to understand and control the potential attack surface from IoT. With that in mind, the next priority should be to segment your network to isolate IoT traffic, which can control the proliferation of attacks and quarantine infected devices. The network can then automatically grant and enforce baseline privileges suitable for a specific IoT device risk profile.
3. Finally, policy-driven IoT groups combined with internal network segmentation enables multi-layered monitoring, inspection and enforcement of device policies based on activity anywhere across the distributed enterprise infrastructure. An integrated and automated security framework allows the association of intelligence between different network and security devices, in addition to the automatic application of advanced security functions to IIoT (Industrial Internet of Things) devices and traffic anywhere across the network, including at access points, cross-segment network traffic locations and in the cloud.

Fortinet is committed to driving the development of IoT security. Our dedication to innovation helps ensure that we are well-equipped against the evolving threat landscape threatening the success of our emerging digital economy

INTELLIGENT DEFENCE

DOWNLOAD INFOSEC APP FOR FULL DETAILS

Access the latest technical research & defensive tools and techniques

Taking place on Tuesday 6th June, the Intelligent Defence sessions take a deep-dive into the latest risks, trends, cyber-attack methodologies and intelligence-based defence strategies to detect, contain and respond.

The programme features the following presentations:

Internet Banking Safeguards Vulnerabilities - Wojciech Dworakowski

Barbarians in the Throne Room - Dave Lewis

Adversarial Machine Learning: The Pitfalls of Artificial Intelligence-based Security - Giovanni Vigna

Behavioural Analysis Using DNS & Network Traffic – Joshua Pyorre

Learning from Mistakes - They Will Happen - Adam Compton

So Many Ducks, so Little Time - Michel Coene

IoT Security – Executing an Effective Security Testing Process - Deral Heiland

The IP Address Black Market - A Primer – Security Researcher

To view the full agenda and latest speaker and session updates please visit **www.infosecurityeurope.com/intelligentdefence**

INFORMATION SECURITY EXCHANGE

RESERVE YOUR SEATS NOW

Trade insight and experience with infosecurity experts

Attend in-depth presentations and panel discussions to gain new techniques and actionable insight to enable you to enhance your organisation's information security strategy and tactics.

Sessions include:

App-to-Cloud Security: Three Problems You Don't Know You Have - MobileIron

Securing Digital Cohesion with SDSN - Juniper Networks

Enabling Secure Access for the Next Generation of Workers, Apps, Networks and Things - Pulse Secure

Elections, Deceptions & Political Breaches - What High Profile Attacks can Teach us About Enterprise Security - Fidelis Cybersecurity

Navigating Infosecurity's Role in GDPR Compliance – Qualys

The Rise of IoT Botnets – Radware

Yesterday's Email Security Systems Can't Stop Today's Email-borne Threats – Mimecast

A Laptop is Stolen Every 53 Seconds. Are You Ready? – OneLogin

How to Become Cyber Resilient in an Ever-Changing Threat Landscape - Cognosec

Other organisations making presentations in the Information Security Exchange include **Arxan Technologies, Fortinet, SSH Communications Security, SonicWall** and **RedOwl.**

To view the full agenda and latest speaker and session updates please visit **www.infosecurityeurope.com/ise**

TALKING TACTICS

DOWNLOAD INFOSEC APP FOR FULL DETAILS

New for 2017

Learn real-life lessons from practical case studies

The Talking Tactics sessions, taking place on **Thursday 8th June,** are a series of 'how to' and 'case study' presentations offering practical guidance and actionable information on how to address specific challenges and issues.

Learn how others have addressed these challenges through presentations by exhibitors and their clients sharing real-life experiences.

Companies presenting 'case studies' and 'how to' sessions include **Proofpoint** and **Veracode.**

To view the full agenda and latest speaker and session updates please visit **www.infosecurityeurope.com/tt**

SECURITY WORKSHOPS

Build your skills and understanding during practical workshops

Join in-depth, extended workshop sessions and gain practical know-how and learning that can be applied directly to your business. Engage with your peers during interactive sessions and learn from leading security experts how to address the latest challenges.

Organisations offering workshops include **(ISC)², Bitdefender, Cisco, Crowdstrike, Efficient IP, IAPP, Neustar, Osirium, Security Culture Framework Community, Splunk** and **Wombat Security.**

Topics to be addressed include:

- **Mature Your Security Capabilities with a SOC & a CERT** - Splunk
- **CISSP Preview: Security & Risk Management** - (ISC)²
- **CISSP Preview: Business Continuity & Awareness Programme Requirements** - (ISC)²
- **Cure VM Blindness: How the Hypervisor Can Find Attacks an Agent Can't See** - Bitdefender
- **Security Culture Workshop on Metrics** - Security Culture Framework Community
- **Taking Back the Upper Hand from DDoS Attackers** – Neustar
- **The Major Security Vulnerabilities of 2017 and Beyond** – Cisco
- **The Art of a Data Breach, and the Best Way to Prevent One** – Cisco
- **Hand-to-Hand Combat With an Advanced Attacker** – Crowdstrike
- **Protecting Your Business & Data from New DNS-Based Exploits** – EfficientIP
- **Top Privacy Issues Encountered by Infosecurity Professionals** - IAPP

To register your interest in attending and view the full agenda visit **www.infosecurityeurope.com/workshops**

SECURITY TRAINING

cloud CSA security alliance℠

Infosecurity Europe is delighted to be working with the Cloud Security Alliance to deliver two in-depth training courses

Certificate of Cloud Security Knowledge (CCSK)

Discover how to optimise cloud security within your organisation

- Access strategic and technical know-how to overcome cloud security challenges
- Discover how to protect and control sensitive data in the cloud
- Understand how to implement robust security controls to optimise cloud security

Date: **Thursday 8th June 9.00-17.00**
Price: **£649+VAT**

Register and find out more at **www.infosecurityeurope.com/ccsk-training**

Cloud Controls Matrix (CCM) Foundation Training

For cloud vendors:

- Discover how to comply with fundamental cloud security principles and requirements
- Learn how to assess the security posture of your offering
- Compare yourself with competitors and industry benchmark

For a cloud customer or cloud auditor:

- Find out how to assess the overall level of security offered by cloud provider
- Determine how to build the necessary assessment processes for engaging with cloud providers
- Leverage the mapping with other industry-accepted security standards, regulations, and controls frameworks to reduce audit complexity
- Normalise security expectations, cloud taxonomy and terminology, and security measures implemented in the cloud

Date: **Thursday 8th June 9.00-17.00**
Price: **£649+VAT**

Register and find out more at **www.infosecurityeurope.com/ccm-training**

infosecurity EUROPE

06 June - 08 June 2017
Olympia, London, UK

Visit
NUVIAS
Incorporating WICK HILL
on stand
D100

Find out more and book an appointment

01483 227600 | www.nuvias.com/infosec | cybersecurity@nuvias.com

CYBER INNOVATION SHOWCASE

Hear about new innovations in cybersecurity

Take this chance to hear about the newest innovations in cybersecurity. The agenda includes presentations by the 14 shortlisted companies from the competition funded by **Department for Culture, Media & Sport (DCMS)** sponsored by Atkins to find the **UK's Most Innovative Small Cyber Security Company.**

They will be joined by organisations including **Balabit, Beame.io, Cymulate, Cyphort, Ericom Software, HP, Imperva, Kaymera Technologies, Logtrust, Secgate** and **Waratek.**

The sessions will demo and showcase the products and services offered by these organisations.

To view the full agenda and latest speaker and session updates please visit **www.infosecurityeurope.com/CIS**

Live Incident Response Scenario

Cyber-Attack Survival Guide: Fostering Cyber Resilience within the Organisation

New for 2017

When: **Thursday 8th June, 12.00-13.30**
Where: **Keynote Stage**

Take this chance to join stakeholders from information security, legal, communications and law enforcement as they form an incident management team to respond to a cyber-attack scenario. The panel will share their perspective on how to respond as the scenario unfolds.

What would you do in their shoes?

Facilitated by **Richard Horne**, Partner, PwC, the session will address the steps to take to remediate a breach, how to engage stakeholders across the enterprise, how to involve law enforcement and the steps an organisation needs to take to ensure it is resilient to cyber-risks.

Panellists include: **David Boda**, *Head of Information Security at Camelot,* **Andrew Gould**, *DCI, Falcon at the Metropolitan Police Service* and **Joseph da Silva**, *Director of Information Security at Centrica.*

TECHNOLOGY SHOWCASE

Keep up-to-date with the latest infosec technologies & solutions

Exhibitors will take to the stage to demonstrate the capabilities of their products and technologies. Gain the insight you need to maximise ROI on your solution purchases.

Don't miss this chance to hear about the latest technological developments and breakthroughs and pose your questions directly to the vendors. Presenting companies include: **Cyberark, Cyberbit, Cyren, Duo Security, Ivanti, GB&SMITH, Indegy, Panaseer, Picus Security, Pulse Secure, Satisnet, SecuLution, Splunk, SSH Communications Security, Varonis, Verint Systems, Wandera** and **ZoneFox.**

To view the full agenda and latest speaker and session updates please visit **www.infosecurityeurope.com/techshowcase**

SITS 17
THE SERVICE DESK & IT SUPPORT SHOW
7-8 JUNE 2017
OLYMPIA, LONDON

SITS – The Service Desk & IT Support Show, the annual exhibition for the UK's IT Service Management community, returns to Olympia London on 7-8 June

With an extensive free seminar programme, big name keynotes, hot topic roundtables and an array of new products and services – the show will provide service desk professionals with an unrivalled opportunity to discover the latest research and ideas that they need to meet the unique challenges of their rapidly evolving industry.

The two-day show will feature 80 leading specialist vendors, integrators, consultancies and service providers, demonstrating top quality IT solutions – from self-service IT portals and live chat software to transformational service management tools.

Among the 80 exhibitors, returning companies include Hornbill Service Management, TeamUltra, Cherwell Software, Webroot, ServiceNow, Atlassian, Freshdesk, TOPdesk UK and Bomgar.

Visitors to the show will also benefit from a packed free seminar programme, featuring over 50 sessions covering topics such as DevOps, BRM, enterprise service management, digital transformation, ITIL and the new General Data Protection Regulations coming into place in May 2018.

SITS takes place next door to Infosecurity Europe, meaning that with one badge you get access to two great shows. For further information please visit **www.servicedeskshow.com**

Detection Alone is Not Enough

Network Traffic Analytics from Scrutinizer

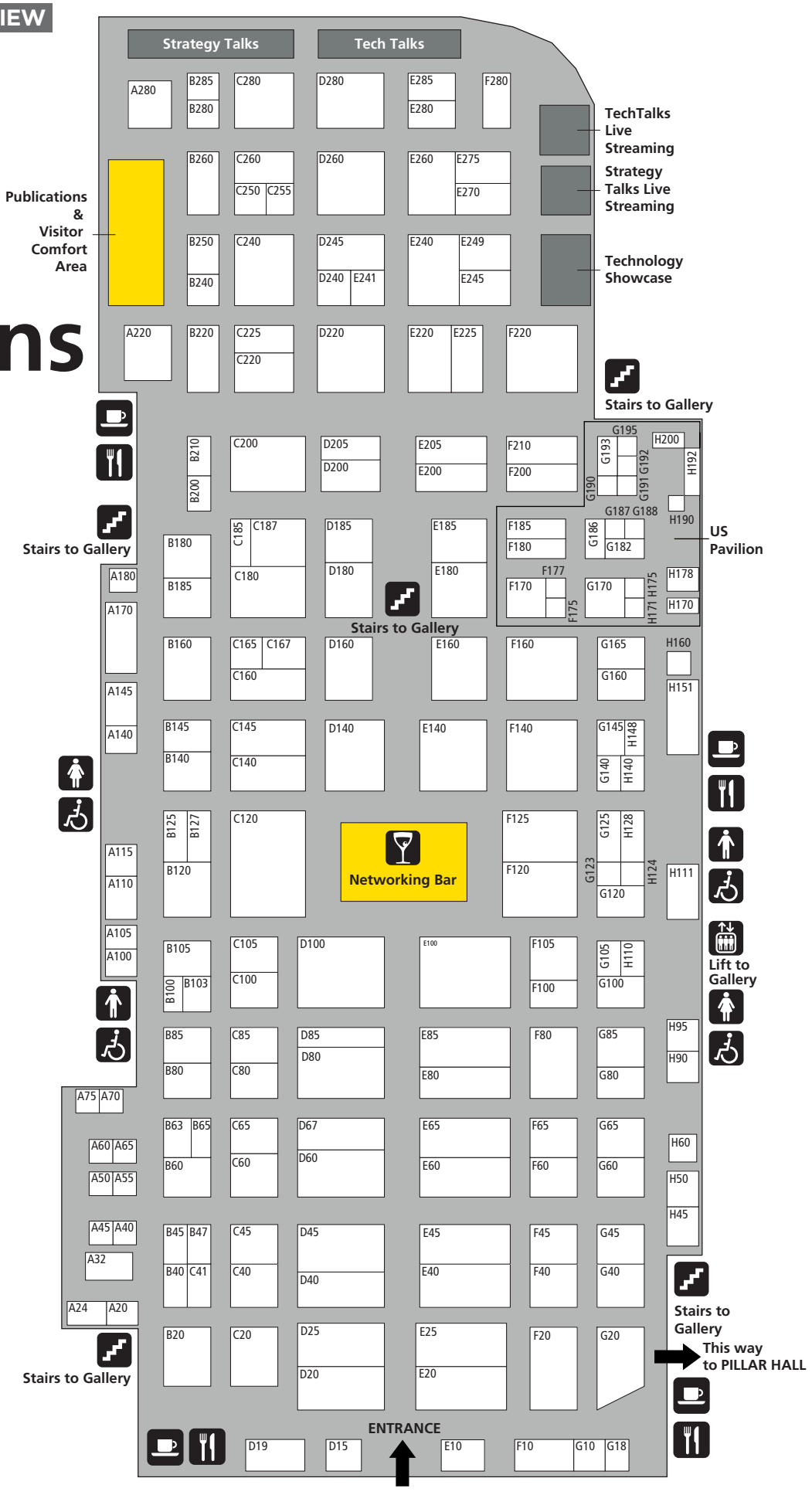
Stand E220

Infosecurity Europe 2017

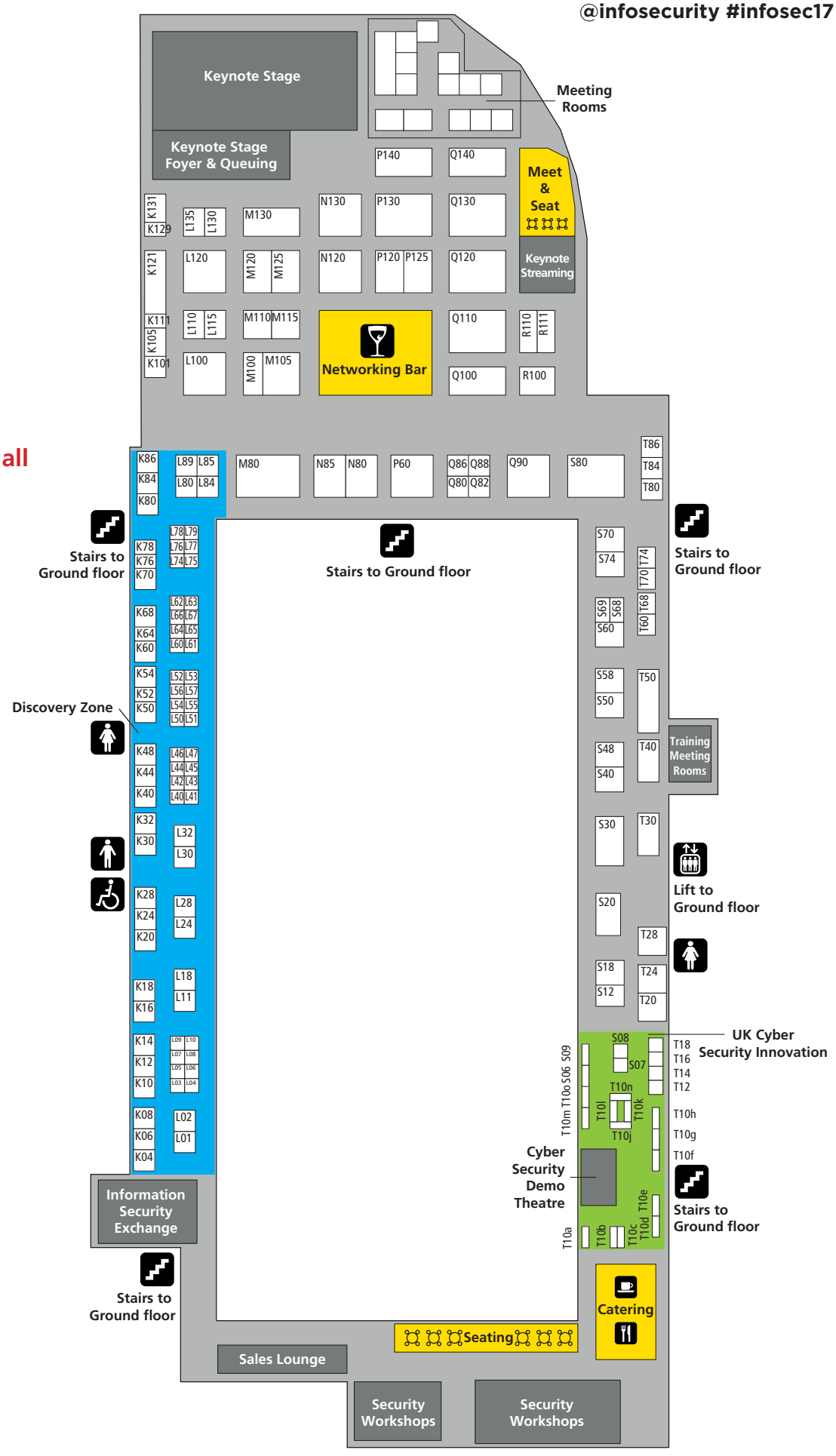
plixer

Floorplans

Ground Floor, Olympia Grand Hall



Upstairs Gallery, Olympia Grand Hall



A-Z Exhibitor List

Logtrust	S58
Looking Glass	K60
Lumeta Corporation	H190

M

Malwarebytes Limited	E45
ManageEngine	B103
Metacompliance Ltd	E249
Midlands Engine	S60
Mimecast Services Ltd	G100
Missing the Linq	L45
Mobile Iron International	H111
My1login	B210

N

Netcope Technologies, a.s	K64
Netsparker	H110
Netwrix Corporation	B85
Neustar Inc	B20
Niagara Networks	L85
Nominet UK	L77
NSFOCUS Information Technology Co. Ltd	D180
NUIX TECHNOLOGY UK LTD	E185
Nyotron	L120

O

OneLogin Inc	B65
OPSWAT	G195
OracleUK	P60
Origone	L79
Osirium	F210
Outpost24 UK	D45

P

PA Consulting Services Ltd	A170
Palo Alto Networks UK	C200
Panaseer	A140
PCI Security Standards Council	A115
Pen Test Partners	E85
PeopleNet Security Technology Co., Ltd.	G60
Performanta Ltd	P120
Pervade Software Ltd	S74
phishd by MWR	A220
PhishMe Inc	E180
Picus Security	L74
Pinnacle Office Equipment Ltd	L44
Plixer	E220
Portnox	B63
Positive Technologies	H160
PRIORITY	K18
Privasee AB	L06
Proofpoint	C260
Prosoft Systems	L18
Pulse Secure	E200

Q

Q-East Software (Smart Investigator)	L10
Qualys Ltd	E20
Quest Software International Ltd.	K105

R

Rackmount.IT	L52
RadarServices	F60
Radware	E260
Rafael Advanced Defense Systems Ltd.	K131
Rapid7	D40
Rebasoft Limited	K68
Recorded Future	F10
RedOwl Analytics	G187
Redscan	G125
Resilient, an IBM Company	E245
Resolve Systems	L40
RiskIQ UK Limited	F177
Risk-X	E10
Rohde & Schwarz Cybersecurity	C41
Royal Holloway, University of London	A180

S

SafeDNS	L47
SailPoint Technologies, Inc.	C45
Satisnet	D245
Savvius	D15
Scram Software Pty Ltd	L56
Secgate	L100
Seclore Technology Pvt. Ltd	F175
Secudrive	Q82
SecuLution GmbH Deutschland	L84
SecurityDAM	L130
Securonix	G170
SentinelOne	B180
Sepio Systems	L57
ServerChoice	D200
Serverius	L08
ServiceNow UK Ltd	B45
Silensec Limited	L30
Silent Circle	L04
Silobreaker Ltd	R100
Sixgill	L66
Skybox Security Inc.	F200
Skyhigh Networks	C80
SolarWinds MSP UK Limited	G10
Soliton Systems	G120
Sonatype/Nexus Lifecycle	H192
Sonicwall	C280
Sophos Limited	C120
Splunk Services UK Ltd	C20
SSH Communications Security	D240
SSL247	L110
Stormshield	A280
Sumologic	Q135
SureCloud	C85
Symantec	E25
Synopsys NE	G80

T

TechWeek Europe	A50
Tempest SI	K48
Tenable Network Security Limited	F160
Teramind Inc	F280
Thales	C140
The Eastern Trade Council	Q110
The National Cyber Security Centre (NCSC)	F100
Thinkst Applied Research	K12
ThreatQuotient, Inc.	F180
Titania	G40
TrapX Security	G85
Trend Micro	D25
Tripwire International	D20
Tufin Software Technologies Ltd	P125
TypingDNA	K52

U

UBITECH	K18
University of Surrey	L51
UNLOQ Systems LTD	K76
Utimaco IS GmbH	A70

V

Varonis UK Ltd	C40
Vasco Data Security SA	E240
Vectra Networks	E225
Veracode ltd	B120
Verint Systems Ltd.	G160
VERISIGN	E205
Viavi Solutions UK Ltd	L24
VÍNTEGRIS SL	B47
VMware International Limited	E140

W

Wallix	B127
Wandera	G105
Waratek	B240
WatchGuard Technologies	E65
Weblife	L05
Welsh Government	T24
WhiteSource	B285
Wick Hill Ltd	D100
Wombat Security Technologies, Inc.	F185

Y

Yellow Room Learning Ltd	L61
Yoh Solutions Limited	A20
Yubico Ltd	M110

Z

Zenedge, Inc	E270
ZeroFOX	G188
Zimperium	G190
Zonefox	S12
Zscaler Inc	D260

The floorplans and exhibitor list were correct at the time of printing. For the latest exhibitor list, please visit: **www.infosecurityeurope.com/exhibitor-directory**

Media Partners and Associations

WHAT NEXT

FOR THE INFORMATION SECURITY WORLD?

NETHERLANDS
Infosecurity Netherlands
01-02 Nov 2017
www.infosecurity.nl

LONDON
Infosecurity Europe
05-07 June 2018
www.infosecurityeurope.com

RUSSIA
Infosecurity Russia
19-21 September 2017
www.infosecurityrussia.ru

NORTH AMERICA
Infosecurity North America
04-05 October 2017
www.infosecuritynorthamerica.com

MEXICO
Infosecurity Mexico
23-24 May 2018
www.infosecuritymexico.com

BELGIUM
Infosecurity Belgium
14-15 March 2018
www.infosecurity.be

MIDDLE EAST
Infosecurity Middle East
06-08 March 2018
www.infosecurityme.com

Infosecurity Group is here to help the information security community share, meet, discuss, network all around the world. Our magazine, webinar series and global events provide all you need to keep up-to-date with the latest news, understand emerging issues, learn from each other, inspire solutions and hear from global thought-leaders and innovators.

infosecurity® GROUP

@infosecurity

info security
STRATEGY | INSIGHT | TECHNOLOGY

www.infosecurity-magazine.com

Q&A

NEIRA JONES

Neira Jones has so many roles and titles that we can't fit them all on the page. Let's just say she's an independent advisor and international speaker with various board positions. All of these things give her the freedom to choose who she works with and just be herself, which is why even when pitted against working with performance cars, shoes, travel or being a Michelin restaurant reviewer (all passions of hers), she still considers her current role her dream job.

Who do you really admire in the industry?

Those that continue to strive to make our world a safer place, and there are many. To pick out a few: I bow to Prof Fred Piper for being such an inspiration and making cryptography sexy; Elizabeth Denham for doing such a fabulous job at the UK ICO in the short period she's been in position; Brian Honan and Prof John Walker for their indomitable stamina; Troels Oerting for finding the time to be involved in very worthwhile initiatives whilst being CISO at Barclays; Jenny Radcliffe for telling it like it is and making it her business to eradicate that scourge that is social engineering; and Lee Munson for not giving up on his dream.

Tell me about a time you screwed up

I remained in a job much longer than I should have, causing myself – and those around me – a lot of angst. In fact, I failed to follow my own advice in a timely manner, which is "If you can't change the people, *change the people*. Sometimes it's you." So I extracted myself, albeit late, and that was a good lesson.

How do you feel about the 'women in tech' conversation?

I'm definitely in the camp of favoring the conversation about 'people in tech' more generally. Whilst the gender imbalance is undeniable (not just for cybersecurity but for STEM in general), I think the root of the problem happens much earlier in the education system. With 'women in tech', we're trying to fix a symptom and whilst there are many worthwhile initiatives, on their own, they can only achieve so much.

What's the most misunderstood thing about information security?

That it's about technology only and should be left to the IT guys. If I could change one thing about the sector, I would want it to be more open and stop the fear-mongering.

What advice would you give to someone starting out in the industry today?

Keep informed, interact and build a network and really understand that it's about people, process and technology. Don't be scared, we don't all wear foil hats…(well, unless they're Philip Treacy's).

Tell me something that will surprise our readers

I collect antiques and I'm really interested in Tudor history. My favorite management book is Macchiaveli's *The Prince*.

BIO

@NeiraJones

Neira has more than 20 years of experience in financial services and technology. She advises organizations of all sizes and addresses global audiences on payments, fintech, information security, regulations and digital innovation. Neira has won numerous industry awards and holds a number of board positions with security and payments organizations.

TOP TEN DDoS Attacks

01
Attack on DYN – 1.2 Tbps

The attack on the DNS provider took websites such as Spotify, Airbnb, Starbucks and *The Guardian* offline.
Source: Mashable, Wikipedia

02
Attack on OVH – 1 Tbps

Hosting company OVH was hit by a 1 Tbps attack in September 2016, the largest ever seen at that time.
Source: Security Affairs

03
Attack from Leet botnet – 650 Gbps

The botnet conducted 17-minute attacks with huge power originating from spoofed IPs.
Source: Imperva

04
Takedown of Krebs on Security – 620 Gbps

Among the biggest assaults the internet has ever witnessed, this was nearly double the size of the largest attack seen previously.
Source: Krebs on Security

DAN RAYWOOD

The Problem with Measuring DDoS

The DDoS attack has moved from a sign of cyber-protest to something tactically used to bring websites, applications and even DNS providers offline.

***Infosecurity* presents the top ten DDoS attacks (in terms of size) of all time. The problem with measuring DDoS attacks is that traffic figures are sometimes hard to measure, and in collating this list, some noted attacks could not be included as the actual attack size was unquantified.**

Yet what's particularly evident is that the size of attack has increased dramatically over the course of 2015 and 2016, and while there have been more devices appearing online, more computing power has arrived to enable greater and stronger attacks, evolving from megabytes to gigabytes right up to terabytes of packet data being delivered at any one time.

05 Attack on BBC by the NWH – 602 Gbps

The BBC's websites were offline for several hours on New Year's Eve 2016, after Islamic State-linked New World Hacking carried out the attack as a "test of its capabilities."
Source: BBC

06 Attack During Hong Kong Elections – 500 Gbps

PopVote, an online poll platform managed by The University of Hong Kong's Public Opinion Program, was hit by a 500 Gbps attack in 2015.
Source: SecurityAffairs

07 Attack on Gambling Company – 470 Gbps

The attack in June 2016 targeted a Chinese gambling company and lasted for over four hours before it was mitigated.
Source: Imperva

08 Attack on Spamhaus – 300 Gbps

Described as "The DDoS That Almost Broke the Internet", the attack peaked at 300 Gbps of traffic in March 2013.
Source: Cloudflare

09 Attacks on Hong Kong – 300 Gbps

DDoS attacks measured at 300 Gbps were targeted at PopVote and Apple Daily in March 2014.
Source: Forbes

10 Attack on Church of Scientology – 220 Mbps

Hacktivists Anonymous hit the Church of Scientology in 2008 in an attempt to gain media attention away from the church.
Source: PC World

BLOCKCHAIN: WHAT IT MEANS FOR CYBERSECURITY

Are Blockchains redefining cybersecurity or do they pose more security challenges than they solve? *Sooraj Shah* investigates

Many have compared the seismic impact the internet has had on the world with the potential effect blockchain will have over the next decade. The same has been said about cloud computing, artificial intelligence and numerous other IT buzzwords and should therefore be taken with a pinch of salt.

Indeed, Blockchain's very own senior vice-president of growth, Liana M. Douillet Guzman, tells *Infosecurity* that she "doesn't think blockchain is a panacea."

However, it is clearly an area which is likely to see growth in the coming years. One report, by Grand View Research, suggests that the blockchain marketplace will grow to almost $7.74bn in value by 2024.

So What Exactly Is It?

"Blockchains are transaction networks. A blockchain is a globally replicated, secure database. You can think of it as an immutable, permanent and secure spreadsheet in the cloud which de-risks liability thanks to its distributed nature," Guzman explains.

"If one of these nodes goes offline, the rest of the network can continue to confirm transactions without skipping a beat", she adds, before emphasizing that the only blockchain protocol in widespread use today (Bitcoin) has been running every day for eight years without a major interruption.

However, there are numerous other blockchain trials ongoing. For example, international shipping company Maersk is working with IBM on a project which would help to manage the global supply chain and track the paper trail of tens of millions of shipping containers across the world. Charity Save the Children UK wants to create a 'humanitarian passport' using blockchain and retailer Walmart is using blockchain in China to track the supply chain record of food to improve health and safety standards.

The technology seems to be on every large organization's radar, particularly those in the financial services space. Metro Bank, the UK's newest retail bank, is keeping tabs on developments in the technology, its chief technology officer David Young tells *Infosecurity*, with security seen as the key benefit of the technology.

Yet John Palfreyman, director of blockchain at IBM's cloud division, emphasizes that the blockchain structure itself isn't any more or less secure than any other technological structure. For him, the main attraction towards blockchain is the applications that it enables, rather than the security benefits it may have.

There Are Security Benefits

As cybersecurity becomes a focal point for businesses, many IT departments will be looking at if – and how – blockchain can help them to beef up security.

> ***"The code which supports Blockchain is relatively new and largely untested"***

Dr Joao Ferreira, a cybersecurity expert at Teeside University in the UK, states that there are two key benefits, the first of which is the immutability of data.

"It is impossible in theory to tamper with the data; you can't just change a record in the blockchain because it's a hash chain structure that is distributed. Many attacks occur because of the criminals' ability to change information, blockchain can be used to prevent that from happening", he says.

Blockchain uses a consensus algorithm and therefore any changes need to be verified by the network, and this comes at a cost.

"There is a cost to make a change, so any attack on a service based on blockchain becomes more difficult because it will be more expensive if there is a cost associated with changing that information", he says.

The second IT security benefit is a lower risk of being impacted by DDoS because the attack surface is distributed rather than centralized.

Combining the difficulty of changing data to the distributed nature of blockchain gives businesses a more resilient backbone to rely on.

"It means that even if a criminal takes my copy of the blockchain down, I may lose the services but everyone else can still use it", Ferreira states, thereby nullifying the threat of DDoS.

As blockchain is a decentralized system, it has an advantage over existing trust architectures that have a single point of failure such as Certificate Authorities (CA) and DNS providers, Garrett Bekker, principal analyst at IT advisory firm 451 Research, explains.

"We've seen CAs that have been compromised and also what can happen when a DNS provider goes down, as with the impact of the recent Mirai botnet attack on Dyn; I suspect blockchain could deal better with this, and also simplify the use of public key infrastructure (PKI) by eliminating dependence on a CA as the single anchor of trust", he says.

Blockchain Versus IoT

There is one organization that is hoping that blockchain can be used to solve one of the biggest headaches for the IT industry at present – securing the Internet of Things (IoT).

The Isle of Man government is working with members of the blockchain community on an experiment to see if the technology can keep IoT devices from being hacked.

"We want to prove that by adding a layer around that device, that any data that comes out of it can immediately be hashed into the mesh [network] that surrounds it", Brian Donegan, head of operations, fintech and development at the Isle of Man government, tells *Infosecurity*.

"If this can be demonstrated unequivocally, then you can do it to the next device it is connected to and so on – using blockchain repeatedly to get to a situation where you end up with networks of devices that have blockchain armory around them", he adds.

Donegan's team is still several months away from being able to report back its findings on the trial.

With Great Power Comes Great Responsibility

The law has always struggled to keep pace with developments in technology, and those that are providing the blockchain technology and services to organizations will need to be wary of who owns the risk, and how it is transferred.

> ***"Many attacks occur because of the criminals' ability to change information, blockchain can be used to prevent that from happening"***

"They need to make sure they understand the pressure that customers are under from a regulatory perspective and do everything they can to alleviate that risk; the worst situation is for organizations to not be able to move

forward with new technology because the providers can't give them assurance about the technology", says Luke Scanlon, senior technology lawyer at Pinsent Masons.

This is important because there are risks associated with blockchain. As Dr Ferreira emphasizes, there is "no system that is 100% secure."

He gives some examples of security issues that blockchain-related technology could run into – such as the theft of Bitcoin from cryptowallets. He says a key danger with blockchain – like many other technologies – is the human aspect.

"The cryptowallet means you have some files that encode your address and your balance. If you lose that, you lose your identity and your money and all of your cryptocurrency. If we expect users to manage their cryptowallets there could be many problems because it is easy to exploit people with social engineering", Dr Ferreira states.

However, even those humans behind the technology can be at fault for security breaches.

Last year, a smart contract called DAO, based on Etherium (a blockchain technology) was hacked, leading to $50m being taken from a virtual hedge fund. Dr Ferreira explains that it is incredibly easy to make little mistakes in writing smart contracts, and that attackers are ready to pounce on vulnerabilities.

"[In the DAO case], they hired very good people, professional programmers, but it still had a bug and an attacker was able to benefit from it", he says.

It's also worth bearing in mind that some of these benefits of blockchain – such as anonymity – can be used against organizations, as criminals seek to hide illegal transactions such as ransomware payments. Using blockchain-based identities to control access to services would give users comfort in knowing that their data is pseudo-anonymized, but if the blockchain was breached and the data was exposed, the company in question would face irreparable reputational damage. The more sophisticated the technology, the bigger the potential of a disaster.

The Future of Blockchain and Cybersecurity

It is the implementation stage where blockchain and cybersecurity really intersect; if a blockchain is incorrectly implemented, it opens up huge risks to the organization and to its partners.

According to Florian Malecki of IT security company SonicWall, the technology is not yet secure or mature enough to quell concerns around security and inspire wider adoption.

"The code which supports blockchain is relatively new and largely untested against the full potential of the global hacker community and at present there is no way to know what bugs remain and how large the resulting vulnerabilities are", he says.

For Karl Hoods, chief information officer of Save the Children UK, blockchain isn't redefining cybersecurity but is an enabling platform for it.

By combining it with existing IT security practices, it offers increased security. As organizations develop their understanding of how to implement the technology, it is likely that it will solve many more security challenges than it poses END


2013
Microsoft founder Bill Gates calls Blockchain 'a technical tour de force' and suggests that governments will maintain a dominant role in the area.
2014
Apple removes Blockchain, the last remaining Bitcoin wallet on iOS from its App Store. It later updated its rules on cryptocurrency apps and added Blockchain back to its App Store. Mainstream websites began accepting Bitcoins including WordPress, Expedia and Microsoft.
2015
Ethereum, an open-source, public, blockchain-based distributed computing platform goes live. One of its features would be for 'smart contracts' – another use of Blockchain.
2016 JUNE
A thief steals $50m of virtual currency from a fund called the Decentralized Autonomous Organization (DAO). The DAO had poured more than $150m worth of Ether into the project.
2016 JULY
Ethereum executes a 'blockchain hard fork' to return $40m of the DAO's funds to an account available to its original investors. The decision to use a hard fork was controversial as it undermined the perception that blockchain was immutable, and that contract agreements would be final.
2016 NOVEMBER
EY Switzerland announces that it would accept Bitcoin from clients to pay off their auditing and advisory invoices from January 2017, it would also install a Bitcoin ATM in its Swiss office.
2017 MARCH
47 Japanese banks completed a money transfer pilot using Ripple's blockchain technology. IBM announces enterprise-ready Blockchain-as-a-Service based on open source Hyperledger Fabric.
2017 MAY
A smart contract capability via 2-way peg (2WP) from RSK RootStock will allow smart contracts to run on Bitcoin's blockchain for the first time rather than just Ethereum.
2017 JULY
Isle of Man government aims to publish whitepaper about its trial to use blockchain to beef up security on IoT devices.
2020
66% of banks will have adopted blockchain – according to an IBM Institue of Business Value Survey.
2024
The market is set to reach $7.74bn by this point, according to a report by Grand View Research.
2025
A January 2017 World Economic Forum report predicts that 10% of global GDP will be based on blockchain and related technologies.

Does the UK Need an Information Security Royal Charter?

Ian Glover

President, CREST

Working in information security for 36 years, Ian has been instrumental in a significant number of major initiatives in the industry, including the Cyber Essentials scheme and the UK government CIR. Ian has also worked on a number of social responsibility research projects.

@CRESTadvocate

To have a Royal Charter and the ability to award Chartered status to 'professionals' working in the information security industry is a natural progression and has significant benefits for the industry and also for individuals.

To justify professional status, it must be done through industry and internationally recognized professional examinations or other agreed demonstrable assessment. The industry has made very good progress in the establishment of individual certification, however, none of the existing certificates identify individuals operating at the highest level of the profession.

There needs to be something for people working at senior levels in the information security industry to aspire to that provides them with a maintained recognized status, and Chartered status will provide this. It will add significant credibility to the industry and will help identify a 'senior professional' in the market.

This will not be an easy pathway because the industry is very diverse, ranging from very deeply technical people, through policies and standards setting or auditing people to senior management with direct links to other more established areas of risk management. Information security is an emerging industry and does not, or isn't even close to, having an agreed body of knowledge that encompasses all the roles.

If a Royal Charter is implemented, it must recognize the existing career pathways but be flexible enough to reflect new roles and jobs that do not yet exist. It is not clear in my mind how all of the aspects necessary to build Chartered status can encompass all roles and all jobs in the industry, so we must start with career pathways that are understood and established and work from there, providing a process that allows for considered expansion.

Information security is an international business so we must talk to equivalent issuing bodies in established and emerging regions to obtain consistency. A UK-only recognized award without equivalence will be of limited value.

The diverse range of roles also makes it difficult to establish what existing professional institution should make the award. Some of these already have a Chartered status, but have a limited number of new awards they can issue. Others are attempting to obtain Chartered status but have not achieved it yet. Interestingly, obtaining Chartered status in information security will probably require demonstrable expertise that would fall into multiple existing professional institutions.

The industry must start to work together on this. If particular industries or government contract any single body it will be difficult to develop and implement a process that will be widely accepted and sustainable. If specific sectors or government want to help this to happen, they should encourage collaboration. If seed funding is available it should be oriented towards helping to coordinate this collaboration, not to introduce competition in the 'institution' marketplace END

Amanda Finch

General Manager, IISP
Amanda has specialized in information security management since 1991 when she established the function within Marks & Spencer. In addition to her role at the IISP, she works with the Information Security Forum (ISF) and the British Computer Society (BCS) and has a Master's degree in Information Security.
@IISP

Protecting the systems that underpin the current technology transformation gets ever more complex, and there simply aren't enough security professionals to meet the challenges. As an information security profession, we are acutely aware of these issues but we need to address the issues more formally.

The UK Government has recognized the seriousness of the problem and in its National Cyber Security Strategy (2016-2021), stated that "the UK requires a sustainable supply of home-grown cyber skilled professionals to meet the growing demands of an increasing digital economy, in both the public and private sectors and defense." The intention is to develop clear entry and development routes for the profession, attractive to a diverse range of people. Part of this is to ensure that cybersecurity becomes "widely acknowledged as an established profession with clear career pathways, and has (a national body of) Royal Charter status."

Having a Chartered status will significantly raise the profile of our professionals and a Chartered Institute will provide clarity on the disciplines and bring us in step with other chartered professions.

We need recognized skills frameworks developed by professional bodies. Through definition and standardization, professionals wanting to demonstrate their capabilities can be measured against

> ***"Having a Chartered status will significantly raise the profile of our professionals"***

defined criteria. Such definition will give us the ability to cultivate skills on a greater scale and provide our professionals with clear signposting for development.

Professionalization is a way to demonstrate the mastery of certain skill sets essential for success, and show that those skills and knowledge can be refreshed through continuing education. To do this, we must identify the body of knowledge and skills that professionals need to have, supported by appropriate education and training programs and finally have a way to accredit this process.

It is often overlooked that employers place enormous trust in their information security specialists, who often have privileged access to highly sensitive information as well as critical business systems and processes. Such trust necessitates that individuals meet the highest professional, working and ethical standards.

The IISP argues that an effective alternative to today's ad hoc, decentralized approach is needed and that professionalization requires a nationally recognized, independent organization to act as a professional body and clearinghouse for the profession. The process would unfold over several years and involve stakeholders from government, academic institutions, profit and non-profit organizations, public and private sector entities, formal and informal groups. Its responsibility would include coordinating standardized core curricula for educational institutions at all levels and encourage collaboration with both intra-university and intra-professional bodies.

Chartered status would allow entitled members to stand proudly with a clear indication of meeting the highest professional standards of knowledge, skills, abilities and ethical behavior. The IISP has been applying these principles for 10 years since its formation and is keen to formalize these as institutional protocols END

Robin Smith

IT Security Manager, West Yorkshire Police
Robin is IT security manager at West Yorkshire Police. He has 15 years' experience as a privacy and compliance specialist, working across health, local government and law enforcement.

In our world where data is a currency, the information security professional becomes an essential broker. The protection of information and data is essential, and the information security industry must mobilize to support the recent application for Royal Charter status.

The recent application (submitted by the IISP) for a Royal Charter status to the Privy Council demonstrates how the profession is maturing and information professionals should support this move in a number of ways. The profession is dealing with risks that threaten the entire conduct of our digital societies.

Chartership is the level of professional registration for those working in the information professions who wish to be recognized for their skills, knowledge and application of these in the form of reflective practice.

The benefits of Chartership are myriad, ranging from the recognition of the profession as a key part of society to ensuring that individual professionals can plan his/her career path.

One of the key concerns regarding the application for Royal Charter will be the need to fuse experience with accreditation. Simply achieving Chartership should not be an objective; it should be part of a dedication to

> ***"It should be part of a dedication to developing skills and experience"***

developing skills and experience within a professional industry. Evidence from other professions highlights that many individuals fail to go beyond Chartership to push the boundaries of current professional practice and orthodoxy. The information security profession must avoid this risk.

The financial costs of Chartership in other industries can also be exorbitant. A number of engineers note that the process for an individual to become Chartered can be both expensive and time consuming, with few benefits aside from the title provided by authorized organizations.

Successful applications for Royal Charter have been based around mobilizing potential senior professionals and the emerging young stars in the industry to outline the value and impact made by granting the application. The information security industry is blessed with a number of highly influential individuals who can speak with fluency regarding the present and near-term threats that are being battled. The Institute of Information Security Professionals (IISP) deserves credit for conducting an excellent initial campaign to lobby for recognition. Its membership is key to the success of this endeavor and can take action to aid the application.

The new paradigm of the digital economy requires the information security profession to be clearly identified as a key broker for all information and data assets. With the rapid development of the industry in the last decade and the array of emerging issues that shape our entire society, information security professionals should mobilize to support this campaign to ensure success. As we approach 2020, individuals working in this key sphere need to decide whether they want to shape our digital nation or simply respond to its demands. It's really up to every individual information security professional. What do you want to do with the rest of your career? END


12
1
2
3
4
5
6
7
8
9
10
11

KEEP CALM AND COMPLY: ONE YEAR AND COUNTING UNTIL GDPR

With the May 2018 deadline fast approaching for Europe's new data protection laws, *Phil Muncaster* outlines practical tips from the experts on how to get in shape ahead of the big date

In April 2016, three senior European Commission policymakers issued a landmark joint statement. It signaled the final adoption of new EU rules designed to enshrine in law the right of personal data protection for all citizens. For organizations around the world, it also signaled the beginning of a two-year countdown to enforcement of the European General Data Protection Regulation (GDPR), which is also intended to foster "trust in online services by consumers and legal certainty for businesses based on clear and uniform rules." That May 25 2018 deadline now looms even larger – spelling trouble for some organizations.

Veritas claimed last December that over half (54%) of global firms had still not advanced their compliance plans, while a DLA Piper estimate from January claimed organizations are only currently complying with around 40% of GDPR principles. Meanwhile, Netskope claimed three-quarters of the 22,000 cloud apps it tracked fail to pass muster, according to the new regulation. That could be costly for firms, according to new rules which will levy fines of up to €20m ($21m) or 4% of global annual turnover for serious infractions. It could cost global firms $320bn if they fail to get compliance sorted, according to Capgemini. The Payment Card Industry Security Standards Council (PCI SSC) reckons that could amount to over £120bn ($150bn) for UK firms alone.

> ***"Is your customer-facing privacy communication ready for GDPR and able to address growing customers' expectations and demands for privacy?"***

This may sound like a lot, but be warned: the GDPR will make it much easier for individuals to bring private claims against firms. They won't need to prove financial loss, just 'distress' or hurt feelings. They'll also have the right to ask a consumer protection group to bring claims on their behalf, according to DLA Piper. What's more, the new law will apply both to data controllers and the suppliers they engage to process that data – bringing a whole sweep of new firms under the compliance microscope.

What Does it Cover?

It's worth mentioning that the GDPR covers all 'personal data' but that the definition of this is broader and will apply to more details, including a "wide range of personal identifiers" such as IP addresses, according to the UK's privacy watchdog, the ICO. Even pseudonymized data could fall under the scope of the new regulation, depending on how easy or difficult it is to tie it back to the original individual. It will also mandate that firms be more explicit when obtaining consent to use individuals' personal data: the use of straightforward language will be essential and firms will not be able to interpret a lack of response as consent.

One of the new rules with the biggest impact on firms will be 72-hour mandatory breach notification to the local data protection authority – i.e. the ICO for UK firms. Also high up on the list will be the mandatory appointment

Brexit Implications

The GDPR will automatically come into force in the UK on May 25 2018. With the process of Brexit likely to take at least two years, UK organizations will need to comply from that date. Beyond that, the government has hinted at a harmonization of laws following Brexit. There remains one potential conflict: the Investigatory Powers Act's bulk data retention requirements, which run counter to EU law. Still, in the meantime, there's no way out of GDPR compliance for UK firms.

of data protection officers (DPOs) for any firms which undertake "regular and systematic monitoring of data subjects on a large scale" or those who process special categories of data "on a large scale."

The GDPR introduces the idea of privacy by design, and for that reason, any firm judged to represent a major risk to user privacy must conduct a Privacy Impact Assessment (PIA) before undertaking any work. The regulation also introduces new consumer rights, notably the right to be forgotten and the right to data portability.

Where Should You Be by Now?

All organizations should have finished an initial assessment phase by now, designed to help them understand where their compliance gaps are, according to Forrester analyst Enza Iannopollo. Next should come budget approval, and implementing the necessary changes, before reviews and continuous monitoring.

Those complying with current European privacy laws will see the process more as an "evolution", while for others it will be a "deep, radical change", she tells *Infosecurity*.

"First of all, you need to find out where your data is and map its flow, including third parties and business partners, and this analysis should also include an evaluation of the technologies, processes and oversight mechanisms in place," she explains.

"Last, but certainly not the least, we need to look at the people: including employees' awareness and preparedness, but also customers. Is your customer-facing privacy communication ready for GDPR and able to address growing customers' expectations and demands for privacy?"

To ease the process, firms should have put together an internal privacy team in charge of GDPR compliance by now. However, the hardest part of the compliance puzzle is the necessary cultural change, according to PwC US privacy leader, Jay Cline.

"A common view of the privacy office in Europe up until now has been a lawyer sitting behind a computer screen writing policies and dispensing advice," he tells *Infosecurity*. "Yet for privacy programs to withstand the impending, heightened scrutiny of European regulators, the focus of activity needs to shift from the legal department to the IT, marketing and HR departments, as well as procurement, finance and product design."

Quick Compliance Wins

Although all the experts agree that firms should be far down the road to compliance by now, there are still some quick wins which could accelerate efforts.

"Look to the existing information security management and privacy controls, then determine which controls are already sufficient or near sufficient to meet the needs of the legislation", advises Capgemini's chief security strategist for NEU, Richard Starnes.

"Should a company not have sufficiently robust controls for a quick win, it is late in the game, but not too late. Partner with a trusted advisor and have your program ready to meet these new challenges. Companies don't have to go it alone."

Even pseudonymized data could fall under the scope of the new regulation

> *"Look to the existing information security management and privacy controls, then determine which controls are already sufficient or near sufficient to meet the needs of the legislation"*

For Canon's EMEA information security director, Quentyn Taylor, formalizing the role of the DPO can also give an early boost to efforts, as can data mapping – understanding what you have and how it is used.

"For any company that is a data processor, the changes are even more significant and we would urge them to talk to their customers who are the data controllers to understand how this change will impact their business relationship and working practices", he adds.

Alexandra Leonidou, senior associate at law firm Foot Anstey, claims some firms will need to create a number of new processes from scratch.

"Examples of this may include processes related to new rights for individuals, the new mandatory breach notification requirements, or in relation to the roll-out of new data protection impact assessments," she says. "You may wish to develop these new business processes simultaneously to conduct your mapping and audit to make sure that you get engagement and input from key parts of the organization as you go along. Leaving this until the very end may result in processes that are less tailored or workable for your business and your data."

The Global Picture

The GDPR is not just about European organizations. It applies to all those which store, process or share the data of European citizens, meaning UK firms post-Brexit and those in the US and elsewhere will need to comply. In fact, PwC recently claimed US firms will spend an average of $1m on compliance efforts.

There could be bumps in the road ahead though, both for those in the US and UK, which will require careful monitoring by IT leaders and DPOs.

Given the strict rules governing data transfers outside the region, global organizations would be advised to "keep it local" with European datacenters, according to KPMG global privacy advisory lead, Mark Thompson. Emily Taylor, CEO of Oxford Innovation Labs and associate fellow of Chatham House, agrees, adding that Donald Trump's 'America First' policies could undermine the EU-US Privacy Shield agreement.

"Although the previous US administration made substantial concessions such as limiting access to bulk data unless strictly necessary, legal challenges are already in motion, arguing that the protections are insufficient," she explains. "A more aggressive stance on security issues by the US may well topple an already wobbly compromise."

Is it Too Late?

There's certainly still time to get your compliance house in order, but depending on the size of your organization, it will be a challenge. Some are more optimistic than others.

"No one wants to admit it but the reality is that the vast majority of organizations are unlikely to have done anything close to what is needed by the May deadline. GDPR compliance is a massive task, it requires significant business change, winning hearts and minds as well as transforming business processes and systems", says KPMG's Thompson.

"In the event that your organization is behind, it is important that you take a risk-based approach."

The good news is that there are plenty of sources of high-quality advice for firms. The Article 29 Working Party and ICO are good places to start. Industry bodies like techUK can also help out, as can consultancies such as PwC, Capgemini and law firms. However, the focus should always be on "long-term sustainability," according to Thompson.

"Covering the gaps right now, only for them to emerge again in 12 months' time, is not what regulators are looking for", he concludes END

Timeline

24 October 1995 – Data Protection Directive 95/46/EC created to regulate the processing of personal data

25 January 2012 – European Commission proposes an update to the region's data protection regulations

15 December 2015 – Parliament and Council agree final text

8 April 2016 – Adopted by Council of EU

16 April 2016 – Adopted by European Parliament

25 May 2018 – GDPR will come into force

TWO EXPERTS GO HEAD TO HEAD

Point

Protecting the Large Enterprise

Paul Watts

CISO, Network Rail

Paul has worked in information security for over 10 years as part of a 22-year career in IT. He is currently working to enable Network Rail to embrace modern, business-enabling interconnected technologies whilst protecting this essential piece of UK Critical National Infrastructure from both current and future cyber-risk.

@PaulWattsUK

I'll be honest; I do look at CISOs of small-but-perfectly-formed organizations from time to time, and wish I could wrap my arms around my own 'as easily as *they* must be able to.' Of course, I have no scientific basis for that assertion, but permit me to elaborate on a few areas of challenge that face larger, more diverse organizations such as mine.

My organization is diverse, and it is certainly large. Network Rail consists of over 35,000 staff and contractors, 5500 suppliers, hundreds of properties and one of the largest private telecommunications networks in the UK. It also encompasses thousands of information and operational technology platforms and an infrastructure comprising more moving parts than is humanly possible to count, scattered liberally across the UK. All of this, coupled with our devolved operating model, makes the challenge of maintaining effective oversight of our security posture exciting and challenging in equal measure.

So *can* one CISO realistically wrap their arms around something of this scale? In our case, it wasn't practical and we therefore have two – one for the corporate and IT interests of our organization (me), and one for our telecommunications organization and Digital Railway transformation program. We also have an operations security manager and a professional head of cybersecurity. Between us and our teams, we just about cover all the bases.

Most large organizations will struggle to keep a low profile. In providing a key transport infrastructure for 4.5 million passenger journeys per day, our high public profile is inevitable. Depending on who you are, your public profile in some small way can influence threat opportunities and thus create potential headaches for the organization's CISO.

In the era of social media, it pays to have an ear listening out for who is talking about you and why. As well as identifying and defeating potential opportunities for business disruption, you are also taking steps to actively manage your brand's digital footprint and reputation. It gets you on the front foot far quicker than waiting for the first DDoS attack or *that* call from your media relations team, certainly a plus when you consider the saying "the bigger they are, the harder they fall."

> ***"Extend the traditional security team with a crowdsourced community"***

An effective security management plan starts with the right organizational culture and it fails spectacularly without one. However, building an effective security culture that reaches all four corners of a large and diverse organization is a massive challenge. From experience, I have concluded that one size simply does not fit all.

I often labor the point about security being a journey, and never a destination. However, in order to take everybody on the journey, it has to personally resonate in a way that compels people to *want* to be on it. Personally resonating with 35,000 people without culture change is insurmountable unless you enforce and edict, which is hardly conducive to winning hearts and minds and will ensure CISOs retain their traditional 'business blocker' moniker.

So, what is the solution to building an effective culture in a large organization? You must *listen* to your business. All of it. Recognize that within a vast organization lie subtle demographic differences. On the railway, an office worker has different needs and wants to a member of our trackside teams of engineers. Once you have agreed your core messages, subtly adapt them to relate to those different groups. By taking this approach we observed notable changes in behaviors; in our last culture assessment we measured improvements right across the board.

What about determining the reality of your security posture? They say the best way to eat an elephant is 'in small pieces' and this is *critical* in a large organization; you simply cannot expect your HQ-based security team to know-all, see-all. They can't, and they won't. If security is a collective responsibility, how can the organization play its part if you are 'invisible' to them, and they are 'invisible' to you?

One solution that works is to extend the traditional security team with a crowdsourced community of interest, advocates or 'champions'. Equip them with tools, materials and training. Incentivize, engage and empower them; if they feel they are making a difference, they will continue to champion the cause for you.

To conclude, whilst the rationale and outcomes of CISOs are broadly similar in objective, I do believe the depth and complexity of certain aspects of the role differs between large and small organizations. My advice to CISOs in large organizations is this: don't try and eat the elephant yourself. Instead of a CISO and their team trying to be one set of very long arms, one should instead seek an organizational culture that allows many arms to form one long chain around your business, letting the business own the problem with you, and collectively celebrate the success of managing it together END

Counter-Point

vs Securing the Smaller Business

It is natural to think that it is more difficult for smaller firms to implement security as the perception is that it's a specialist area and it can cost a lot of money to get the best technology to give you protection.

Traditionally, security was only implemented if it was a prerequisite to doing business with big companies. However, things have changed and technology that was once only available in high-end devices is now a standard on our home routers.

If you have never been involved in security and start looking at what is out there, you will find massive amounts of data. What is right for your business? What is cost effective? What does this all mean? This can all be overwhelming for a subject which most people feel adds no value and is just an unnecessary cost.

Cyber-criminals are working together and even franchising their services to work against victims of all sizes, but the reality is, they don't always look at big targets but rather the easy targets, which all-too-often are proving to be the smaller companies whose security setups are less mature, under-resourced and possibly not tried and tested.

For smaller business owners, security can often feel like a mammoth task, and for some, a variety of daunting challenges can actually make it seem like an impossible one.

Often for smaller companies the big challenge is surviving and growing the business with limited available budget, and security can be viewed as an inhibitor to that.

How do you assign the correct amount of money for security when funds are tight? The reality, however, is that for smaller companies fighting tooth and nail to be successful, it can be much more expensive **not** to address security because of the risk of:

- Damage to reputation
- Financial penalties
- Business interruption

Another significant hurdle to overcome is the issue of resource management. Even the biggest companies in the world, with their reputation, all of their finances and pulling power, can suffer from being under-resourced when it comes to skilled security workers. This is amplified for smaller companies whose security teams can be as small as a couple of members of staff.

> ***"Often for smaller companies the big challenge is surviving and growing the business with limited available budget, and security can be viewed as an inhibitor to that"***

Therefore, if you do not have the in-house expertise (which a lot of smaller companies don't) then you have to either hire, outsource or educate, but that comes at a cost and additionally, it can be a real challenge to judge whether you are getting value for money and quantify what you need them to do.

Having spent the money to get the basics in, the security landscape and criminals are moving fast and companies need to stay ahead whilst being cost effective.

The fact is, security *can* be as cheap or expensive as you want it to be. It is about identifying risk and assessing and mitigating based on your risk appetite. As a leader in a small company, you might say 'I don't have time to do this', but look to make it part of your business instead of seeing it as an additional thing to do. When designing a new product, or procuring a new service, make security part of the process. Just like you would evaluate suppliers against each other for value and requirements, this is just another consideration you need to make.

Luckily, there is a lot of information out there to assist you. Government initiatives like Cyber Essentials are a great, easy and cost effective way to make a start with protecting your business. There is also a site that provides free cybersecurity training for small businesses (https://www.gov.uk/government/collections/cyber-security-training-for-business).

Security can be a scary subject for anyone, but particularly for smaller companies who have to deal with challenges that the big players don't. However, you can educate yourself and make informed decisions, and the worst thing you can do is to ignore the problem and hope nothing goes wrong END

Johan Pieterse

Head of IT and Security, Racing Post

Johan has 17 years' experience in the industry and is the head of IT and security at *Racing Post*. Prior to that, Johan oversaw a contract for Siemens looking after a part of the Road User Charging scheme for TfL where security was paramount.

@JohanPieterse_


s.send("GET /" + sys.argv
s.send("Host: " + sys.arg
s.close()
for i in range(1, 1000):
attack()
import socket, sys, os
print "][Remote DDOS Addr
print "injecting " + sys.
def attack():
pid = os.fork()
s = socket.socket(socket.
s.connect((sys.argv[1], 8
print ">> GET /" + sys.ar
s.send("GET /" + sys.argv
s.send("Host: " + sys.arg
s.close()

MINIMIZING THE LOSS OF DDoS

As DDoS attacks grow in prevalence and size, *Dan Raywood* explores whether protection is keeping pace with a threat that has already trapped some of the biggest targets across the globe

The distributed denial of service (DDoS) attack is a modern capability to silence an opponent. If that opponent is a government, a business, a journalist or even a rival, the provision is there to stop the other entity from existing, even just for a short while.

From the beginnings of DDoS, with the 1996 attack on the Public Access Networks Corporation (Panix) ISP, the 2007 DDoS attacks that hit Estonia and the Anonymous campaigns against those who would not provide financial support to Julian Assange and WikiLeaks, DDoS is a weapon of choice for the modern activist who chooses to silence those who do not support the same cause.

For some time, the DDoS attack was about megabytes of traffic. The turning point was the attack on Spamhaus in 2013, which reportedly measured 300 Gbps. Described as the "attack that almost broke the internet" by CloudFlare, it changed the face of DDoS to what we know now in terms of size and capability. Now, according to Akamai's Fourth Quarter, *2016 State of the Internet Report*, attacks greater than 100 Gbps increased 140% year-on-year from Q4 2015.

It also reported that the largest DDoS attack in Q4 2016, which peaked at 517 Gbps, came from Spike, a traditional botnet that has been around for more than two years. Add to this the attack on DNS provider Dyn in September that was measured at 1.2 Tbps, and the attack a day earlier on the website of security journalist Brian Krebs which was measured at 620 Gbps.

Putting aside the Spamhaus attack, which was an anomaly for its time, the sudden rise in size of DDoS attacks has come as a surprise. Krebs claimed that the attack that took his website offline was "according to Akamai, nearly double the size of the largest attack they'd seen previously, and was among the biggest assaults the internet has ever witnessed."

In the case of the attack on Dyn, this was a Name Server DDoS attack, where attackers focused on name servers to prevent web addresses from resolving. According to Igal Zeifman, security evangelist at Imperva for the Incapsula product line, this is accomplished by using DNS floods against servers, or by attacking the network infrastructure of DNS service providers. He claims that the "significant increase in attack sizes over the past 18 months" has seen them swell to half a terabit per second.

> ***"DDoS attacks are more frequent and more damaging each year"***

Are We Keeping Up?

If attacks have suddenly increased, is the protection keeping pace? Neustar's Barrett Lyon, who previously founded 'always-on' DDoS protection vendor Prolexic, says the problem is not with technology, as that generally remains the same, but more about how high you can push the defenses.

Speaking to *Infosecurity*, Sean Newman, director of product management for Corero Network Security, explains that DDoS has been driven by amplification attacks from when attackers realized that they could abuse the protocols that make the internet work, and turn a small amount of traffic into a large amount of traffic.

"Apart from Mirai, pretty much all of the big attacks have been driven by amplification and reflection techniques, which were using and abusing protocols like DNS, or NTP", he says.

Newman said that DDoS attacks abusing network time protocol (NTP) can deliver an attack up to 1000-times of the traffic being sent to the target, if the attacker can find an open server with that sort of capability. "We still see DNS get used and it is a 50+ multiplier, but nothing like with NTP."

Asked whether he feels there has been a sudden increase in the size of attacks and if the capability has always been there, he says he is not convinced that there has been an increase in capacity, but just that DDoS "came back into fashion.

"Over time bandwidth has gone up so you need more power for the attack in the first place," he argues. "Go back 20 years and computers were much less powerful, so it would be hard to generate enough power."

Protection is Key

Claudio Neiva, Gartner security and privacy research director, says that "DDoS attacks are more frequent and more damaging each year" and protecting against these attacks, without breaking the budget, is critical to your website's performance and reliability.

Pointing out that an average attack can range from four to 10 Gbps, and last anything from 15 minutes to a whole day, Neiva adds that if the attacker is making a political point the attack can be more sustained. In terms of protection, it's

important to think about what makes sense to be protected in your environment. "Prices can go from $2500 a month, or $14,000 a month, but it depends on the size of your bandwidth."

In the case of a volumetric attack, Neiva explains that the attacker is intending to fill up 'your internet pipe'; this will mean that you cannot use your intrusion prevention technology or firewall, or even a dedicated anti-DDoS appliance "as the attack comes from the outside and there is no way to control it." A scrubbing center can offer a lot of bandwidth while a dedicated appliance comes as a service.

The second option is an 'always on' technology, where you do not have to call the provider to redirect the traffic as it will pass through the service center all of the time. The drawback here is that it does cost a lot more.

"On demand means that you need a good communication plan to find out who is responsible for making the call to either do a redirection with the push of a button or a call", Neiva said. This is enabled by either redirecting through DNS, or via a BGP routing protocol, but you need Slash24 on the website.

BGP helps with routing the internet, Neiva explains, but like Slash24, it allows you to own the IP address independent of the ISP, and it is possible to redirect traffic to another place.

However, the biggest failing, Neiva adds, is when people struggle to decide when to redirect traffic and often wait until it is too late, so it is important to plan which is the best way.

Another option is to use your ISP who could offer a 'clean pipe' service, a premium service with specialty scrubbing services dedicated to DDoS. However, contracts are often for minutes, and a certain number of mitigations and attacks cannot be higher than 100 Gbps. "I don't like the idea of negotiating a contact linked to the size of the attack as you don't have the ability to negotiate with the attacker", says Neiva.

The Best Option

Neiva recommends a combination of a dedicated on-premise DDoS appliance and a cloud-based service as it will not always be a volumetric attack, but many will be based on floods and are not filling up the pipe, but can be noisy enough to stop your IPS from working.

Garry Sidaway, SVP security strategy and alliance at NTT Security, says that most businesses are failing to realize the potential impact of DDoS attacks, which is why they are not budgeting for them or implementing the right controls and response plans to stop them.

"Recent high-profile incidents like the attacks on US company Dyn and [Brian] Krebs, will help push it up the corporate security agenda," he says. "Yet increasingly these will be driven by extortion, with ransom-based attacks becoming more common and companies prepared to pay off cyber-criminals to avoid customer attrition and financial loss."

According to Maxine Holt, principal analyst at the Information Security Forum, the key is preparation, and to include DDoS attacks when profiling threats to your organization, implementing the necessary level of protection. "Organize your infrastructure so that critical services are separated. This means that DDoS attacks shouldn't affect other critical services."

Preparation and having the right technology fit for your business is one thing, but ensuring it works is another. Eoin Keary, founder and CEO of cloud-based MSSP Edgescan, says he has found that many DDoS protection services are broken and not tested frequently enough.

Keary adds that despite spikes in traffic at unusual times, organizations do not see them and are often not aware it is going on until someone complains. "Often the DDoS protection kicks in too late, as if it kicks in at 300 Mbps, the servers are out of business when you get to 100 Mbps."

The need for protection "can be less or more depending on what it is protecting", Keary explains, and from the companies he has worked with, three out of five have DDoS protection, but only one in those three have it working.

Where there is no DDoS protection, Keary points out that many organizations rely on their ISP, but it is increasingly hard to block as the source of the attack is a moving target.

DDoS prevention is not an under-served part of the industry, and as has been uncovered in this article, there are plentiful options to protect yourself. However, as the size of attacks normalizes at a high level and protection services remain expensive and untested (meaning that businesses are unaware of when things are going awry) maybe the information security industry needs a better solution.

With a 20-year history, and 17 years between the attacks on Panix and Spamhaus which both involved email filtering targets, DDoS has rapidy matured and as the attacks on Dyn and Krebs showed, anyone can be a victim, and if you are the chosen target, even the best protection may not save you if you are unprepared END

Timeline

1996 Attack on the Public Access Networks Corporation (Panix) ISP

2007 DDoS attacks hit Estonia

2008 Anonymous attacks on Church of Scientology

2010 Anonymous 'Operation Payback' against those who would not provide financial support for WikiLeaks

2011 LulzSec 'Titanic Takeover Tuesday' campaign of attacks, including attacks against the servers of Minecraft and surveillance software provider FinFisher

2013 Takedown of Spamhaus

2014 Lizard Squad DDoS the PlayStation Network and Xbox Live on Christmas Day

2016 The IoT-enabled botnet Mirai takes down the website of Brian Krebs and DNS provider Dyn

@InfosecurityMag

SLACK SPACE

Grumbles / Groans / Gossip

01 McDonald's Goes Rogue on Twitter

One of the best things about social media account hacking? Plausible deniability.

In the age of the Donald, there have been several instances of Twitter being used in the US as a platform for "goin' rogue" (as the Sarah Palin-originated saying goes), to voice certain opinions or statements about President Trump which are often controversial.

In that spirit, we saw an official McDonald's company Twitter account goin' rogue in March this year, tweeting directly at President Trump in no uncertain terms: "@RealDonaldTrump You are actually a disgusting excuse of a President and we would love to have @BarackObama back, also you have tiny hands." Even better, the tweet was pinned to the top of the account.

It was since deleted, and the plausible deniability that we all knew was coming floated out into the public socialverse. In a statement, McDonald's apologized for the tweet, and suggested it had been hacked.

"Based on our investigation, we have determined that our Twitter account was hacked by an external source. We took swift action to secure it, and we apologize this tweet was sent through our corporate McDonald's account", the statement read.

Did an employee at the burger empire mistakenly tweet something personal from the wrong account? Was it an intentional, defiant act of Fight the Power? Was McDonald's actually hacked?

The Guardian pointed out that the tweet had been sent from Twitter web, "while every other tweet on the McDonald's account had been sent using a social media management platform." Good backup for the 'hacked' theory. Then again – why would the attacker send only the one lone tweet, and then retreat? It seems more of an act of scrambled desperation, a protest tweet from within that was quickly thrown up in an opportunistic manner before the supervisor returned from his smoke break.

It *seems* that way, but again – plausible deniability. Are there people working at Golden Arches HQ that are willing to do their small part to protest the chaos that is the Donald?

We'll likely never know, but if there are, they've shown how social media – and the culture of hacking – can be manipulated to cover their tracks.

In any event, McDonald's may have curried favor with a whole new set of potential customers: Liberals.

02 Beware the Squirrels, Not the Hackers

The doomsayers seem to announce it from every corner: Catastrophe. Blackouts. Chaos. Riots. These are the end times, for hackers will soon destroy our energy grid, plunging us into a darkened, if not downright benighted state in which our baser natures will take over and finish off civilization as we know it.

On the other hand, it seems the energy grid is actually more at risk from gnawing rodents than hoodie-wearing cyber-terrorists. Apparently, squirrels are our greatest enemy.

That's according to Marcus Sachs, CSO with the North American Electric Reliability Corporation (NERC), who said critters are Public Enemy No. 1 when it comes to knocking power offline. Squirrels (and, lest we be too squirrel-ist, snakes and birds are worrisome too) will tend to nest in substations, chewing on cables or creating fire threats from their gathered materials.

"Security is extremely important to us. There are multiple threats. Cyber is one and physical is another," said Sachs when addressing RSA Conference attendees earlier this year. "Yes, we have a few mouse clicks here and there – but the real threat is Mother Nature and humans doing stupid stuff."

It's not as though there's no cyber-danger at all, as the attack on the Ukrainian power grid demonstrated last year.

However, Sachs said that it's important to keep in mind that the lack of streamlining and general modernization/efficiency across the 55,000 power substations in the US is actually a plus. Outages tend to stay localized, and hackers can't really pivot and move throughout the system.

It's likely just a matter of when, not if, a nation-state successfully attacks the electric grid. So it's good to stay vigilant, but in the meantime, mind the squirrels: they're the real enemy.

1. Ronald got Donald?

2. Beware the squirrel

3. It wasn't me!

03 Playing the Blame Game

Social media trolling. Phishing emails. Hackers hacking. It's a lot for businesses to cope with.

So what do you do? Educate employees on recognizing threats? Hire a social media strategist? Beef up one's multi-layered security defenses?

No, no and no. The real answer is simple: find someone to blame – anyone but yourself.

Gary Spence, owner of digital marketing company HSC Media, offers a blueprint in this area: he found a good target in Action Fraud, the UK's national reporting center for fraud and internet crime.

He told the *Stoke Sentinel*: "We started to have trolling on our company's Twitter account. Then we had mysterious emails requesting work for potential clients which weren't grammatically correct, unlike any normal request. People were trying to access our website from the back end, not the public way."

Spence reported the situation to Action Fraud, but never heard back – and he called his dealings with Staffordshire Police "an uphill battle." He wasn't saying what the business could do to protect the crown jewels, he was just angry the perpetrators weren't thrown in jail.

He added, "Action Fraud is just there for lip services and collating data – they don't do anything."

Welcome to the real world, Mr Spence. Do for oneself – a bit of a hallmark for successful companies regarding security posture.

In stark contrast, we have 22-year-old Michael Hicks, who shows that school really does rule – at least when it comes to staving off a cyber-attack.

Thanks to the information he learned on a free online course, he avoided becoming a victim of unscrupulous cyber-criminals.

"I had a phone which I decided to sell via eBay," he said. "I was going to sell it for around £350 but then I was contacted by someone directly who said they would give me £500 if I took it off the auction and they would buy it straight away."

However, online safety awareness came to the rescue!

"I remembered what I'd been taught on the course and I realized that this was a phishing email and that it would have given them access to my bank account", he said.

What can we say. It's simple, really – stop blaming overloaded governmental resources for your own lack of security preparedness and *carpe diem*. Bottom line: Be like Mike.

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

Parting Shots...

Michael Hill, Deputy Editor

Behavioral analytics has become a real buzz topic in information security over the last few years and, in many ways, with good reason. As organizations grow ever-more connected, data-driven and open to attack, the pressure on companies to keep their information protected from a variety of threats increases. Of these risks, insider threats are some of the more difficult to identify and defend against.

As a result, you wouldn't be hard-pressed to find a business security leader ready to talk openly about the importance of having detailed, intrinsic data on the behavior of users and systems. Similarly, the benefits of being able to synthesize and understand that data to give a more holistic, detailed and intelligent view of what is going on inside the environment is well understood.

"User accounts are critical attack vectors for hackers intent on stealing valuable data or inflicting crippling damage", Ross Brewer, VP and MD of EMEA at LogRhythm, told *Infosecurity*.

"Organizations should know by now that it's no longer a matter of if they'll be breached but rather when. Without deep visibility into insider threats and risks, and behavioral analytics in place to analyze the potential threats, companies will be blind to breaches happening right under their noses."

> ***"You wouldn't be hard-pressed to find a business security leader ready to talk openly about the importance of having detailed, intrinsic data on the behavior of users and systems"***

From a security standpoint, the potential of behavior analytics is quite impressive. By connecting technology with individual data points, it narrows the scope of handling large amounts of information to not only detect and neutralize threats within the network, but also predict and determine errors and future trends. It's therefore no surprise that more and more companies are turning to behavior analytics technology as part of their cybersecurity strategies to defend against insider threats.

"Having the ability to analyze the vast and diverse data on a network to expose insider threats, compromised accounts and privilege abuse is becoming a necessity and organizations are realizing that threats can come from within and appear legitimate," Brewer continued. "It's time that we stop looking solely at *who* the network users are, but *what* they are doing once inside."

However, as is often the case when embarking on any new concept, there are some significant considerations that organizations need to bear in mind to ensure they are doing so effectively, legitimately and, in some cases, legally. Behavioral analytics does indeed appear to be one of the developments in technology that really can aid security, but if companies don't approach its use with care, they risk it having the opposite effect.

Firstly, as Danny Maher, CTO at HANDD Business Solutions explained, an organization's main obligation when handling any large amount of sensitive customer information and IP is to ensure it is sufficiently protected from both external and internal threats.

"With the arrival of EU GDPR in 2018, organizations are set to face stiffer penalties for data leaks and several well-documented breaches in the last 12 months have proved they can ill afford the reputational damage."

What's more, behavioral analytics is only one piece of the security puzzle and an overreliance on it can leave businesses lacking in other areas. Dave Polton, chief technology architect at NTT Security, said that in order to make the most improvement to data security, organizations must have a response plan in place alongside their behavior analytics technology, which can be invoked by validated and qualified incidents raised by their chosen behavioral analytics platform.

"Organizations that are considering behavior analytics should have an incident response plan and part of that plan will be to use other detection and response capabilities. These may capture a great deal more than odd behavior. In fact, some tools can collect and reconstruct all communication flows to and from any device."

Lastly, but no less importantly, is the delicate issue of transparency. It is important that companies ensure their reasons for implementing behavioral analytics are well communicated to the workforce.

"Without an effective communication plan and transparency, end users will naturally become suspicious about the organization's real intentions," argued Maher. "A suspicious and disengaged workforce can lead to lack of care and complacency which in turn leads to a frustrated workforce. Providing education allows the end users to see that such tools are put in place to protect the interests of the individual as well as the organization by keeping their job safe and the business profitable." END

How quickly can your organisation detect and respond to a cyber threat?

Do it faster with Threat Lifecycle Management

We can help. LogRhythm's Threat Lifecycle Management (TLM) platform empowers your team to detect and respond to cyber attacks – fast.

See LogRhythm in action, book a demo at Infosecurity Europe 2017 today: logrhythm-emea.com/demo

LogRhythm®
The Security Intelligence Company

THE FORTINET SECURITY FABRIC

COUNTERING THE EVOLVING CYBERSECURITY CHALLENGE FROM IOT TO CLOUD

Securing the enterprise network is a greater challenge than it has ever been before due to changes in both technology as well as the threat landscape. This challenge is compounded by the fact that most enterprise networks are also suffering from any one or all three of the below conditions – a deteriorating perimeter, their current security infrastructure is actually impacting network performance and unmanageable complexity.

The Fortinet Security Fabric is designed to deal with all three of these by providing Broad, Powerful and Automated Security. This enables the Fortinet Security Fabric to ensure that the right technology is deployed in the right place throughout the network-technologies that work collaboratively across the whole of the network, from the end point to the cloud.

BROAD

The Fabric covers the entire attack surface — security can be applied to the network, endpoints, access, applications and cloud, and visibility extended to other vendor solutions.

POWERFUL

The Security Fabric utilizes security processors to reduce the burden on infrastructure, allowing comprehensive security without affecting performance.

AUTOMATED

The Security Fabric enables a fast and coordinated response to threats — all elements can rapidly exchange threat intelligence and coordinate actions.

Visit Fortinet stand D80