Q2 /// 2016 /// VOLUME 13 /// ISSUE 2

STRATEGY /// INSIGHT /// TECHNOLOGY

infosecurity

Brexit

How IT Security Will Be Affected

PLUS:

INFOSECURITY EUROPE 2016 /// RETAIL SECURITY /// PRIVACY SHIELD

Locklizard

Protect your Documents against Leakage & Theft

Stop unauthorized sharing, copying, printing.
Enforce expiry and instantly revoke access.

Protect from piracy

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

Share securely

Our document security software prevents unauthorized document sharing and piracy.

It controls access to and use of information inside and outside your organization, so you can securely, and cost effectively, distribute and manage your digital content.

Control BYOD use and lock PDF documents to specific locations.

Dynamic control

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

Apply dynamic watermarks displaying individual user information to viewed and/or printed documents to discourage photocopying.

Revoke documents and users at any stage no matter where they reside.

Total protection

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

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

SIGMA SIX

"We like having the confidence that our materials are not being passed freely around the Internet and via e-mail."

vickie milazzo

"Safeguard PDF Security has helped enforce our copyrights and limited file sharing between customers and non-customers."

AviationExam

"We have eliminated a 1 or 2 week delay for printing & delivery, and saved significant amounts of money on processing / shipping costs."

Contents
April/May/June 2016

INFOSECURITY EUROPE 2016

COVER FEATURE

FEATURES

ISSN 1754-4548

infosecurity EUROPE

07 June - 09 June 2016
Olympia, London, UK

WICK HILL

Come and see Wick Hill on stand D100

Request Your Free Tickets
www.wickhill.com/infosecreg

WE HAVE THE SOLUTIONS TO MATCH ALL YOUR NEEDS:

Authentication
Firewall
Forensics
Optimisation
Data Leakage
Awareness Training
Antivirus
Access Control
Monitoring
Virus
Reporting
Intrusion
DDoS
Encryption
Optimisation
Virus
Awareness Training
Ransomware
Spam
Malware
Intrusion
Awareness Training
Reporting
Malware
Forensics
Antivirus
DDoS
Management
Authentication
Reporting
Ransomware
Authentication
Firewall
Ransomware

Visit Our Stand To Win SONOS Wireless Speakers

WICK HILL

Telephone: 01483 227600
email: info@wickhill.com

WICK HILL

Everything You'll Look for You'll Find

When I wrote my first editorial comment of the year, I did so on the day of David Bowie's death and since then the news has sadly been filled with other famous names leaving us. Of course this is security, and while the sudden passing of Prince, Alan Rickman and Johan Cruyff among others has been bad news, the security industry has not faced much happier tales.

2016 has seen enterprises battle with ransomware as the most malicious of malware hit and shut down hospitals, while wearables, devices and industrial control systems deemed to be "the Internet of Things" has the promise to puncture more holes in an already aerated perimeter.

One story that has dominated the headlines in the first part of this year is that of the FBI's efforts to install a backdoor inside the Apple mobile operating system. In this case, the bureau wanted to access the San Bernandino gunman's iPhone, but despite the back and forth of the case going to court and eventually an iPhone being hacked by a third party, what this story did raise was the issue of device security and how private communications are crucial.

Yes the likes of Piers Morgan may have claimed that he could "take that terrorist's iPhone down to Tottenham Court Road right now & they'd get into it", but this story raised awareness of personal privacy and device security to the most common denominator – the general public.

In this issue, Dow Jones head of cyber content and data Rob Sloan looks at this matter from an enterprise perspective, and how vulnerabilities exist, but how deliberately added backdoors add a completely different side to the debate.

Also in this issue, I take a lengthy look at the state of retail security two years on from the major breaches at a number of retailers. What interested me in particular was how there was a large number of breaches reported in succession, and then they suddenly and dramatically reduced.

While attending this year's RSA Conference, I was able to share some time with the Retail Cyber Intelligence Sharing Center (R-CISC) who have enabled retailers to exchange threat intelligence and knowledge to make a more secure sector. Also while working on this angle I got to sit down with M&S head of information security Lee Barney, who I first spoke to a few years ago and with a strong background in the retail sector, now finds himself at the UK high street giant.

Of course the reason why so many of those retail security breaches were reported by US companies comes down to state-led mandatory data breach reporting, and another area of interest in the past few months has been the proposed General Data Protection Regulation (GDPR) being approved. In this issue I talk to two senior members of the National Association of Data Protection Officers (NADPO) about this, and in particular how data protection officers will play a major part in the rollout of the framework in the next couple of years.

Statistics from the International Association of Privacy Professionals published in April revealed that there will be availability for 28,000 data protection officers when the new data protection standard is rolled out. Should I call that availability or yet another shortage? I first wrote about the need for the data protection officer in 2011 and it does seem to be one thing that businesses have embraced already, but perhaps it is a sign of the times.

Finally, you may be reading this at the annual extravaganza that is Infosecurity Europe and sitting here at my desk in our office in Richmond with the team responsible for putting this show together, the level of organization is really something to admire.

This year will see record numbers attend and floor space sold faster than ever before as the industry sets up camp in Olympia for three days. In particular I'm really interested in seeing the winner of the "UK's Most Innovative Small Cyber Security Company of the Year" named. This is something I have been delighted to have been involved with this year and it is great to see yet more innovation in this industry, particularly from those new companies that will be first time exhibitors this year.

> Following celebrity deaths, the security industry has not faced much happier tales

I concluded my last editorial comment saying that this remains the most dynamic sector of IT, and with headlines driving interest in IT security and people and technology set to meet the challenge, I don't see that changing.

Dan Raywood, Editor

infosecurity®

EUROPE

7-9 JUNE 2016 OLYMPIA. LONDON.

INTELLIGENT SECURITY:
SECURING THE CONNECTED ENTERPRISE

Collect CPE/CPD credits

Everyone and everything you need to know in security

Rather than taking our word for it, look at the facts below:

- **98%** satisfied visitors at Infosecurity Europe 2015
- **93%** satisfied exhibitors with 80% rebooking at the exhibition
- **160 hrs** of free seminars and workshops
- **315+** vendors and service suppliers delivered a diverse range of new products and services
- **ROI £1.39+ bn** of estimated future orders, visitors expect to place with exhibitors as a result of attending Infosecurity Europe
- **4,435** professionals earned CPD / CPE credits

REGISTER YOUR INTEREST

www.infosecurityeurope.com

Part of: infosecurity GROUP

Managed by: Reed Exhibitions

Goodbye EU, Hello Cyber Chaos?

With the big European referendum just weeks away, **Phil Muncaster** assesses the impact a Brexit could have on UK information security

Between Westminster posturing and political expediency, shameless scaremongering and unseemingly jingoism, the debate over whether a 'Brexit' could affect the UK's cybersecurity industry has largely been ignored by those who should know better. A poll by Tech London Advocates of its 3,000 senior members in March found a resounding 80%+ want to stay in the EU, but there are some who remain undecided or actively hostile to the status quo.

The government has been happy in the past to claim that cybercrime costs this country as much as £27 billion each year, but it has been reluctant to articulate the impact an exit from the European Union would have on cybersecurity – across public and private sectors. The truth is there are potentially far-reaching repercussions of leaving the world's largest single market – a region we share vital threat information, employ cybersecurity professionals from, and are about to share data protection laws with.

Securing the Future

Information sharing is one of those areas of cybersecurity which is still undervalued by organizations. There are compelling arguments suggesting better exchange of key threat intelligence and the like – between public and private sectors and between businesses – improves organizations' readiness to respond to threats.

However, the fear of giving away a competitive advantage, or allowing sensitive information to slip into the public domain, potentially impacting the all-important share price, has been difficult to allay. In a post-Snowden world, these concerns have been joined by the feeling that over-sharing with data-hungry intelligence agencies may be counter-productive.

While there aren't Europe-wide mechanisms for sharing threat intelligence as of yet, there is at a law enforcement level, where Europol co-ordinates things. Its director, Rob Wainright, has already argued that the UK is dependent on the EU to help protect its security interest – no doubt including security in cyberspace. If it leaves, the UK might be able to renegotiate some kind of agreement on info sharing but it won't have the benefits it currently has, such as "direct access to our database, the ability to involve itself into our intelligence projects and many other areas," he said back in February.

> Should the UK leave the EU then they would not fall under Europol's mandate and as a result it is likely that different mechanisms would have to be put in place
>
> Brian Honan

Brian Honan is a security consultant and special advisor on internet security to Europol's European Cybercrime Centre (EC3). While stressing he doesn't speak for Europol, he echoes Wainright's views.

"Europol's mandate is to support law enforcement authorities throughout the EU. Should the UK leave the EU then they would not fall under Europol's mandate and as a result it is likely that different mechanisms would have to be put in place for Europol to work with UK law enforcement agencies," he tells *Infosecurity*.

"Europol shares information under its obligations under The EU Data Protection Directive, and other EU regulations, and may have to implement different mechanisms to share certain data with the UK should it leave the EU. Similarly, how the UK shares information with Europol would also have to be reviewed."

However, Adrian Davis, European managing director at certifications organization (ISC)², argues that as most info-sharing goes on at a professional rather than institutional level, Brexit would have little impact in this area.

"When it comes to infosecurity knowledge exchange, the key thing is not just sharing knowledge among intelligence agencies, but encouraging the transfer of knowledge across all sectors, from banks to SMEs, both inside Europe and beyond," he tells *Infosecurity*.

"The best way to achieve this is through transnational social networks that can bring together infosecurity workers and knowledge from every sector of the economy to create a diverse pool of infosecurity insight drawn from an array of professional perspectives." In fact, European-wide information sharing initiatives may be nothing more than a pipe dream, such are the differences between member states, he adds.

Incidentally, European security agency Enisa's only prepared comment for *Infosecurity* is that at this point in time it "promotes best practices for information sharing and this will continue." CERT-UK, meanwhile, would not comment directly but says it is "committed to sharing information where appropriate following the vote and will continue to encourage this."

Plugging the Gaps

Another potentially major impact of leaving the EU on the UK's information security industry is that this would immediately halt the free flow of labor so despised by pro-leave campaigners, who suggest immigration is 'out of hand.' The flip side of this argument, of course, is that where there are industries with clear skills gaps, such as cybersecurity, a Brexit could potentially make it a lot harder for UK businesses to employ talent from the continent to fill such holes.

Currently, sponsored information security professionals are covered under the Tier 2 visa system – which relates to sectors where there is an official skills shortage. A UK business would sponsor the application and candidate, and if successful that person becomes a PAYE employee. Yet Victoria Sharkey, a partner at immigration law firm MediVisas, argues that a Brexit will reduce

the volume of candidates UK firms could hire from.

"As it is unlikely that the limit for Tier 2 visas will be extended, this will obviously restrict choice and some employers will find that they are unable to recruit as they wish," she tells *Infosecurity*.

The problem is even more pronounced for those employing temporary staff. "It will affect contractors the most, as Tier 2 visas are only for employees. There is no visa which allows contracting," explains Sharkey. "This may mean that many people who currently want to come to the UK in order to contract would be reluctant to work in the UK as they would be forced to become PAYE employees."

(ISC)²'s Davis agrees that this could happen, but adds that a skills crisis could be averted if qualifications and experience are prioritized under a new points-based immigration system, as long as those creating the criteria understand the sector.

Out in the Cold?

Perhaps the elephant in the room when it comes to IT security and Brexit is the coming EU General Data Protection Regulation (GDPR). The most fundamental and far-reaching reform to the region's data privacy laws in decades, it will introduce significant new rules around the right-to-be-forgotten, data portability and mandatory breach notifications, and impose tough penalties on serious transgressors of up to 4% of annual turnover. There are also requirements in there for mandatory data protection officers, and an olive branch for large multi-nationals, which will only have to report to one regulator, wherever their HQ is based.

Many organizations already down the long road to compliance before the likely 2018 deadline will be wondering whether they should halt these preparatory efforts until the Brexit vote in June.

Not so, according to Allen & Overy partner, Nigel Parker. "First, preparing for the GDPR is a significant and long-term project for larger businesses operating across multiple jurisdictions, so there isn't time to sit back and wait for the result. Secondly, our expectation is that post-referendum the UK would be more likely than not to amend existing data protection legislation to ensure alignment with the GDPR, to enable free movement of personal data from EU countries to the UK," he tells *Infosecurity*.

"Taking this into consideration, many companies operating across multiple jurisdictions will feel that the best course of action is therefore to continue to prepare for the GDPR in the expectation that even if the UK did leave the EU, a data protection regime which imposes similar requirements to those in the GDPR would be likely to apply."

Others argue that a Brexit could cause massive upheaval from a data protection point of view, severely impacting the UK's digital economy. Chatham House associate fellow, Emily Taylor, is concerned that if the controversial Investigatory Powers Bill passes into law this could require an agreement between the UK and EU in the same manner as the Privacy Shield deal hammered out by the US and European Union, in order to allow data on EU citizens to be stored in the UK.


Is UK dependent on EU to help protect its security interest?

> It will affect contractors the most, as Tier 2 visas are only for employees
>
> Victoria Sharkey

While 'Vote Leave' proponents will argue this can be done, the risk is that while lawmakers are thrashing out a deal – and Privacy Shield took the best part of three years – the market could vote with its feet.

"Given that the Court of Justice of the EU has shown itself pretty allergic to bulk data collection, as envisioned in the Investigatory Powers Bill, there is a risk post-Brexit that the free flow of data between the EU and UK could be impeded," Taylor tells *Infosecurity*.

"Moving data is quicker and easier than moving people, buildings or entire businesses. So, if there's uncertainty over the legal, political or economic conditions, data will often start moving before the laws or policies catch up."

With the most internet-dependent economy of any G20 nation, this would put the UK in a difficult position. Amazon and Microsoft have both announced new data centers in the UK for this year, adding to the hundreds that are already here belonging to major international cloud providers.

"These companies have a choice where they can store and process their data, and they can move the data offshore quickly should the law require it," Taylor concludes.

"In this scenario, our homegrown data industries would suffer. Access to valuable EU markets would be in doubt, and the UK's appeal as an international data center location could diminish."

Taking the Offensive
Disrupting Cybercrime

In this article, **Mark Hughes**, President of BT Security, discusses why the industry is now in an arms race with cyber-criminals and what approaches businesses can adopt to ensure a holistic approach to security is front and center

As the threat of cyber-attacks grows, businesses are struggling to keep pace with the constantly evolving tactics of cyber-criminals, hacktivists, state sponsored attacks and even cyber-terrorists.

Too often, boards have become aware of the importance of robust cyber defenses after a breach or hack. In a joint BT and KPMG report *'Taking The Offensive'*, nearly one-third of CEOs listed cybersecurity as the issue that has the biggest impact on their business. Despite this, only half felt prepared for a cyber-attack. At a time when attackers are moving quickly with an increasing arsenal of tools and techniques, the traditional approach to security isn't fit for purpose. The industry needs to take action, quickly.

Rethinking the Threat

The pace of those that are targeting valuable corporate data information has reached the speed that requires a complete rethink of the security strategy. The threat is so considerable that last year the Chancellor announced a £1.9 billion five-year investment to develop a national cyber plan.

At an organizational level, forward thinking CISOs should approach the role with the mindset of the potential hackers, whereby cybersecurity is a customer experience and revenue opportunity, not just a risk that needs to be managed. This approach puts organizations on the front foot by turning cyber preparedness into a competitive advantage rather than a cost.

Ruthless and Rational Entrepreneurs

The industry is now in an arms race with professional criminal gangs and state entities with sophisticated tradecraft. The 21st century cyber-criminal is a ruthless and efficient entrepreneur, supported by a highly developed and rapidly evolving black market. It's no exaggeration to describe them as 'criminal entrepreneurs'.

Like any entrepreneur, the cyber-attacker's intention is often to make money, fast. They buy malware online, rent botnets by the hour, and compete for the best talent so they can inflict maximum damage. Their motivations have also changed: fame, notoriety, financial gain or political recognition are all common 'trophies', alongside the widespread media attention which often accompanies major hacks.

However, unlike conventional competitors, cybercrime entrepreneurs do not play by the rules. They are also undeterred by laws and regulations, perfectly content to damage the organizations they attack and exploit the customers who are often the ultimate victims.

With such high financial and reputational stakes, CEOs and businesses can no longer afford to sleep walk into a disaster. A report by the Department for Business, Innovation and Skills found that 90% of large companies had suffered a security breach. If a company hasn't yet been attacked, it is either extraordinarily lucky or living in the dark. When BT provided the communications network for the London Olympic Games in 2012, we repelled 11,000 malicious attempts every second and we had to fight off 200 million attacks in four weeks and that was over four years ago. In the last 18 months alone we have seen a 1000% increase in cyber-attacks on BT.

The Need for Speed and Agility

Organizations need to treat cyber-criminals the way they treat challenger brands – by understanding and disrupting their business model. It is clear there is a challenge to develop a digital business model resilient enough for a cyber-attack and requires a strategy looking at the digital risks facing the business as a whole, not simply the information systems, but the customers and supply chains.

Traditional compliance processes seem out of step with the new digital age – and adding more and more controls at the cost of flexibility and agility only increases, not reduces, risk.

Across the UK, organizations, government and academia must collaborate to outrun cyber-criminals' innovation. To do so, our own cybersecurity organizations need to be as creative and agile as their opponents.

Given the pace of research and development in the shadow economy, businesses that don't harness innovative technologies and approaches risk becoming obsolete.

KENSINGTON CLICKSAFE LAPTOP LOCK

- Super strong 5mm thick, 1500mm long steel cable
- Clicksafe lock head pivots 180 degrees & rotates 360 degrees
- 12.7mm low profile lock head
- Attaches to Kensington Security Anchor
- ClickSafe®'s keyless locking mechanism

Sku: 170758

£28.95 Ex VAT
£34.74 Inc VAT

ISTORAGE DATASHUR PRO USB3 256-BIT 32GB

- Tamper evident and resistant
- Autolock on removal
- No software or drivers required - 100% hardware Encryption
- 3 year warranty

Sku: 2566647

£91.95 Ex VAT
£110.34 Inc VAT

KINGSTON 16GB USB3.1 DT2000 DATATRAVELER USB KEY

- USB 3.1 interface
- 16GB storage
- Hardware encryption
- 3 year warranty

Sku: 2578976

£88.95 Ex VAT
£106.74 Inc VAT

HP ELITE X2 1012 G1 2 IN 1 TABLET WITH TRAVEL KEYBOARD

- Intel® Core™ m3-6Y30 processor
- 12" FHD LED-backlit touch screen
- 4GB RAM /128GB SSD
- WLAN AC/ Bluetooth® 4.2 Combo
- Audio by Bang & Olufsen
- Fingerprint Reader/ TPM 2.0
- Windows 10 Pro 64
- 3 year warranty

Sku: 2576140

£689.99 Ex VAT
£827.99 Inc VAT

SYMANTEC PROTECTION SUITE ENTERPRISE EDITION 4.0 PER USER MULTI LICENCE EXPRESS BAND A BASIC 12 MONTHS

- Integrates best-of breed technologies to stop security threats before they penetrate the network
- Leverages existing security technologies and IT investments
- Offers a rules-based firewall engine and Generic Exploit Blocking

Sku: 2514749

£51.95 Ex VAT
£62.34 Inc VAT

LENOVO THINKPAD EDGE SERIES

Built for security and productivity.
BALANCING FUNCTION, DESIGN, & VALUE.

There is no better time to upgrade with the Lenovo Reliability promotion - purchase qualifying hardware and warranty extension receive an additional year of warranty free of charge in the event of in-warranty incident that occurs during the standard warranty period

For more information please visit:
www.misco.co.uk/Lenovo-thinkpad-edge-series

SECURITY IN THE WORKPLACE

MISCO A Systemax Business

Freefone - 0800 038 8880
Email - salesdesk@misco.co.uk
Visit - www.misco.co.uk/security-in-the-workplace

HP LASERJET PRO M402DN PRINTER

- Grab pages and go
- Original HP high yield black toner cartridges with JetIntelligence
- Help save energy with HP Auto-On/Auto-Off Technology
- Easily print from a variety of smartphones and tablets

Sku: 2556893

£141.67 Ex VAT
£170.00 Inc VAT

BROTHER DCP-8250DN MONO LASER ALL-IN-ONE PRINTER

- Print, copy and scan
- Up to 40ppm print and copy speed
- Up to 1,200 x 1,200dpi print solution
- Automatic 2-sided print, copy and scan
- Wired network ready + connect to your mobile device and the cloud
- Up to 50 sheet automatic document feeder

Sku: 2013971

£366.00 Ex VAT
£439.20 Inc VAT

CISCO ASA 5516-X WITH FIREPOWER SERVICES

- Rack-mountable
- 8GB RAM / 8GB Memory
- 100GB Hard drive
- AC 120/230 V (50/60 Hz) Power
- 90 day warranty

Sku: 2491435

£2,555.00 Ex VAT
£3,066.00 Inc VAT

FUJITSU SCANSNAP IX500 SCANNER

- Searchable PDF
- Editable Word and Excel documents
- iOS or Android mobile devices or tablets
- Scan documents from business cards to A4 & even A3
- 2 year warranty

Sku:Q594981

£275.00 Ex VAT
£330.00 Inc VAT

Microsoft Enterprise Mobility Suite

Enterprise grade IT Solutions.
Keep up with businesses on the move.

Microsoft Partner
Gold Volume Licensing
Gold OEM
Silver Software Asset Management
Silver Small and Midmarket Cloud Solutions

Misco recommends Microsoft Software

For information on Microsoft EMS
Contact EMS Specialist on
T: **0800 038 8880**
E: **sbaddock@misco.co.uk**

arcserve

Trust Arcserve for all your critical back up needs

Contact us on **0800 038 8880** or email **salesdesk@misco.co.uk**

How Safe Behind the Privacy Shield?

The announcement of the change from Safe Harbor to Privacy Shield was swift, but its passage has been rocky. **Wendy M Grossman** looks at the story so far

The October 2015 European Court of Justice (CJEU) decision invalidating Safe Harbor, the workaround agreement under which companies were allowed to transfer EU citizens' personal data to the US, which lacks comparable data protection laws, opened the way for months of uncertainty.

The result was a scramble to establish a new framework by the court's deadline: 2 February 2016. The European Commission seemed happy with the new arrangement, the EU-US Privacy Shield, but in mid-April the Article 29 Working Party, the pan-European group of data regulators, disagreed. The group praised Privacy Shield's improvements, but felt the agreement lacked overall clarity, does not protect onward transfers to third countries, and does not protect against wholly automated data-based decisions. It also felt that the proposed US ombudsman was insufficiently independent and the US Judicial Redress Act will not be workable for most EU citizens (see box).

Finally, and most importantly, the group complained that Privacy Shield leaves open the possibility of unacceptably massive and indiscriminate bulk data collection – exactly the reason Safe Harbor was invalidated in the first place. The question for businesses, now facing months of uncertainty, is: what do we do now?

Jörg Hladjk, a specialist in data protection law with Jones Day, gives a simple answer: businesses must find another legal basis for data transfers.

In his experience, "Most companies have opted for implementing EU data transfer agreements." These are of two basic types: 1) intergroup agreements between European subsidiaries and their ultimate US headquarters that are based on model contracts that have been approved by the European Commission; 2) agreements using model text between EU entities and US-

based suppliers such as IBM, Amazon cloud services, or Salesforce.

"The data protection authorities have said that if Safe Harbor is not in force any more, the same is true of the model contracts," he says. This is because there's been no change to the cause of Safe Harbor's failure – access by the NSA and US law enforcement.

However, given that companies have to do something, as long as these contracts haven't been specifically ruled invalid they are being used as an interim solution. Changing business practices to avoid transferring data to the US, he says, is not an option for most companies: "I don't know of any company that can easily say no, we don't need to do it," he says.

"The old Safe Harbor was kind of a free pass for US companies, with very low overhead to avoid all of this complexity," says Willy Leichter, vice-president of marketing for the San Jose-based company Ciphercloud. "It was not well enforced, taken advantage of, out of date...it ended abruptly in October but there were already a lot of people complaining."

He adds, "Many US companies were claiming Safe Harbor, but it was so loose that it was hard to tell whether they really had it or what it meant."

Leichter describes himself as "slightly skeptical" about whether the beefed-up European regulations will hold up against the realities of the internet: "I will say that the internet will eventually win because people will use it anyway, but there are a lot of tugs of war around Facebook, cookies, and the breadth of the new data protection requirements."

Nonetheless, he says there will have to be compromise: both US companies and European regulators will have to find some grounds for agreement because neither the issues nor the usage will stop.

Longer-term, it's not clear what those grounds might be. To go back to the beginning, the prohibition on transferring personal data to countries lacking similar legal protections is a key element of data protection law. The most important such country is, of course, the United States, and in 1998, when data protection laws were first coming into force, Simon Davies, then director of Privacy International, predicted a trade war if the US couldn't understand that data protection was now as fundamental a human right in the EU as freedom of speech is in the US.

Both US companies and European regulators will have to find some grounds for agreement because neither the issues nor the usage will stop

Nonetheless, in 2000, the US and the European Commission appeared to find a solution in Safe Harbor, an arrangement under which US companies could self-certify that their internal practices complied with the seven data protection principles. The following years saw the unimpeded expansion into Europe of companies like Google (founded 1998), Facebook (2004), and Twitter (2006).

Then, in 2013, Edward Snowden's revelations proved that US authorities had ready access to EU citizens' data. Based on that new evidence, the Austrian law student Max Schrems brought a case against Facebook's European subsidiary in Ireland; CJEU's ruling in Schrems' favor invalidated Safe Harbor.

Leading privacy lawyer Lokke Moerel, a member of the Dutch Cyber Security Council, the advisory body of the Dutch cabinet on cybersecurity, and professor of global ICT law at Tilburg University, sums up the key difference in how the EU and US view privacy this way: the US takes a harm-based consumer protection approach; the EU takes a rights-based approach.

Judicial Redress Act

The lack of redress for EU citizens in the US when their privacy rights have been violated was a particular thorn in the CJEU Safe Harbor ruling. In February 2016, to facilitate Privacy Shield, the Obama administration oversaw the passage of the Judicial Redress Act, intended to remedy that situation.

Not everyone is convinced. EU Commissioner for Justice Věra Jourová has called it "a historic achievement [that] will ensure that all EU citizens have the right to enforce data protection rights in US courts". However, as the Article 29 Working Party points out, few EU citizens have the resources or ability to bring a legal case in the US.

The travel data privacy expert Edward Hasbrouck has been particularly scathing, calling the Act "worthless" because the rights granted to non-US citizens are bound by the limitations and exceptions of the 1974 US Privacy Act, which creates exemptions for almost all federal agencies. Hasbrouck also notes that the Judicial Redress Act applies solely to data transferred to federal agencies (or components thereof) for "preventing, investigating, detecting, or prosecuting criminal offenses" and ignores transfers via third countries. Similarly, the privacy scholar Robert Gellman has called the Act "little more than a gesture".

In other words, EU citizens have the right to expect their data to be secured, while the US has no such general obligation except in specific sectors such as health and finance. Under the harm-based approach, companies must notify individuals when their data are compromised. Though the EU requirements seem more comprehensive, Moerel says, the US notification requirements have proven the stronger driver to improve data security.


Lokke Moerel

Moerel sees the arrival in the EU of data breach notification laws as part of the General Data Protection Regulation, passed in mid-April 2016, as a turning point. "For the first time we are seeing data protection regulation implementing this harm-based approach, of breach notification," she says.

Moerel believes that the Privacy Shield requirements are sufficiently onerous that they may not be attractive to businesses. For one thing, she says, Privacy Shield's beefed-up reporting and disclosure obligations place both companies and independent dispute resolution bodies under the continuous scrutiny of third parties, which must report lack of compliance with their rulings to the relevant regulator or courts and the US Department of Commerce.

"Some of the requirements are now even more onerous than the requirements under European law and even the upcoming General Data Protection Regulation, such as the mandatory information requirements," she says. "Now the agreement on the Shield is taking so long to materialize, companies have to implement alternative transfer instruments in the interim, such as Standard Contractual Clauses (SCC) or Binding Corporate Rules. However, once these alternatives are in place, the incentive to yet certify under the Shield is no longer attractive because it's a costly step up."

Moerel notes that since the Safe Harbor decision, she's seen US cloud providers change tack, beginning to offer services they formerly found too difficult, such as European clouds and encryption where the key stays with the customer rather than the supplier. However, she argues, it's essential that the EU and US quickly reach closure on Privacy Shield. "Some European regulators seem to think we can do without US cloud suppliers," she says, "but the big European based multinationals – pharmaceutical companies, banks – this situation also hits them with not being able to transfer data throughout their group of companies, which they do as a matter of course. If they can't comply they are in a total fix."

> Once alternatives are in place, the incentive to certify under the Shield is no longer attractive because it's a costly step up

Microsoft Ireland

The ongoing *Microsoft Corporation v. United States of America* may set an important precedent. In December 2013, a New York district judge ordered Microsoft to turn over to the US Department of Justice emails and data associated with an account hosted by Microsoft and belonging to an individual suspected of drug trafficking. Microsoft demurred; it turned over the account information hosted on its US servers but objected to turning over the email data stored in Ireland on the basis that a US search warrant had no authority there.

In May 2014, a federal magistrate judge upheld the original judge's order, and Microsoft appealed. Organizations such as the Electronic Frontier Foundation, the Center for Democracy and Technology, the Brennan Center for Justice, and the American Civil Liberties Union have filed supporting briefs, as have many technology and telecommunications companies and the country of Ireland.

The case is significant because it is fundamentally about jurisdiction and sovereignty. Which should take precedence: the nationality of the server's ultimate owner or the laws of the country where it is located? Do the requirements of US law enforcement pre-empt the fundamental privacy rights of Irish citizens? Is the US willing to grant similar authority to law enforcement in other nations seeking access to data on US servers? The UK has already claimed extraterritorial jurisdiction: in the 2014 Data Retention and Investigatory Powers Act.

The Department of Justice – and the British Home Office – argues that a loss could create data havens for criminals that will seriously impede its ability to investigate and catch criminals. Opponents generally argue that if the government in question has sufficient cause, they should approach the relevant national government for access; proponents argue that this process is too slow and time-consuming. A loss by Microsoft could pave the way for every country to claim jurisdiction over every server that contains any data relating to its citizens.

Backdoors in Technology - is Privacy and Investigation Possible?

Rob Sloan, head of cyber content and data at Dow Jones, looks at the FBI vs Apple case and whether privacy will be the victor

In the recent legal case between Apple and the Federal Bureau of Investigation (FBI), the FBI wanted to force Apple to provide a security bypass to allow access to a dead gunman's iPhone. Encrypted devices have been a bugbear of law enforcement agencies for some time and FBI Director James Comey has been vocal about the damage being done to investigations stating "I don't know why we would want to put people beyond the law."

The courtroom battle and war of words have not been productive for either side, resulting only in more deeply entrenched positions. In the longer-term, however, there is a fundamental question regarding how best to balance the requirements of law enforcement agencies with the privacy concerns of citizens and software producers.

Avenues of Investigation

Device encryption does not however close off all investigative routes. Far from it.

All telecoms operators in the EU must retain metadata relating to calls and texts for up to two years, while data retention in the US is voluntary. Call audio can be intercepted, as can internet traffic, and mobile phone geolocation data shows a location log. Cloud providers, including Google and Apple, share data where required by law and this can include files and photos, email communications and contact lists. It does not however help investigators trying to understand the data on third-party apps (including other encrypted messaging solutions) or files stored only on the device. Backdoors shortcut investigative legwork and represent the convenience of getting maximum investigative gain with minimum effort.

Keys to the Kingdom

Where access to a device containing crucial evidence cannot be secured, there is the option to charge the suspect under the UK Regulation of Investigatory Powers Act that contains a provision for prosecuting individuals who fail to surrender passwords when required to do so. The penalty is up to five years in prison. The Fifth Amendment in the US protects individuals from self-incrimination and there is currently no key disclosure law, giving law enforcement fewer options.

Speaking in March this year, GCHQ Director Robert Hannigan showed a more practical stance, "I am not in favor of banning encryption just to avoid doubt. Nor am I asking for mandatory backdoors." Such challenges have been navigated many times before by intelligence services, not least when hard drives began to be encrypted. Mandatory backdoors threaten user confidence and software vendors cannot be relied upon to facilitate spying on their customers. A different approach to investigations is required.

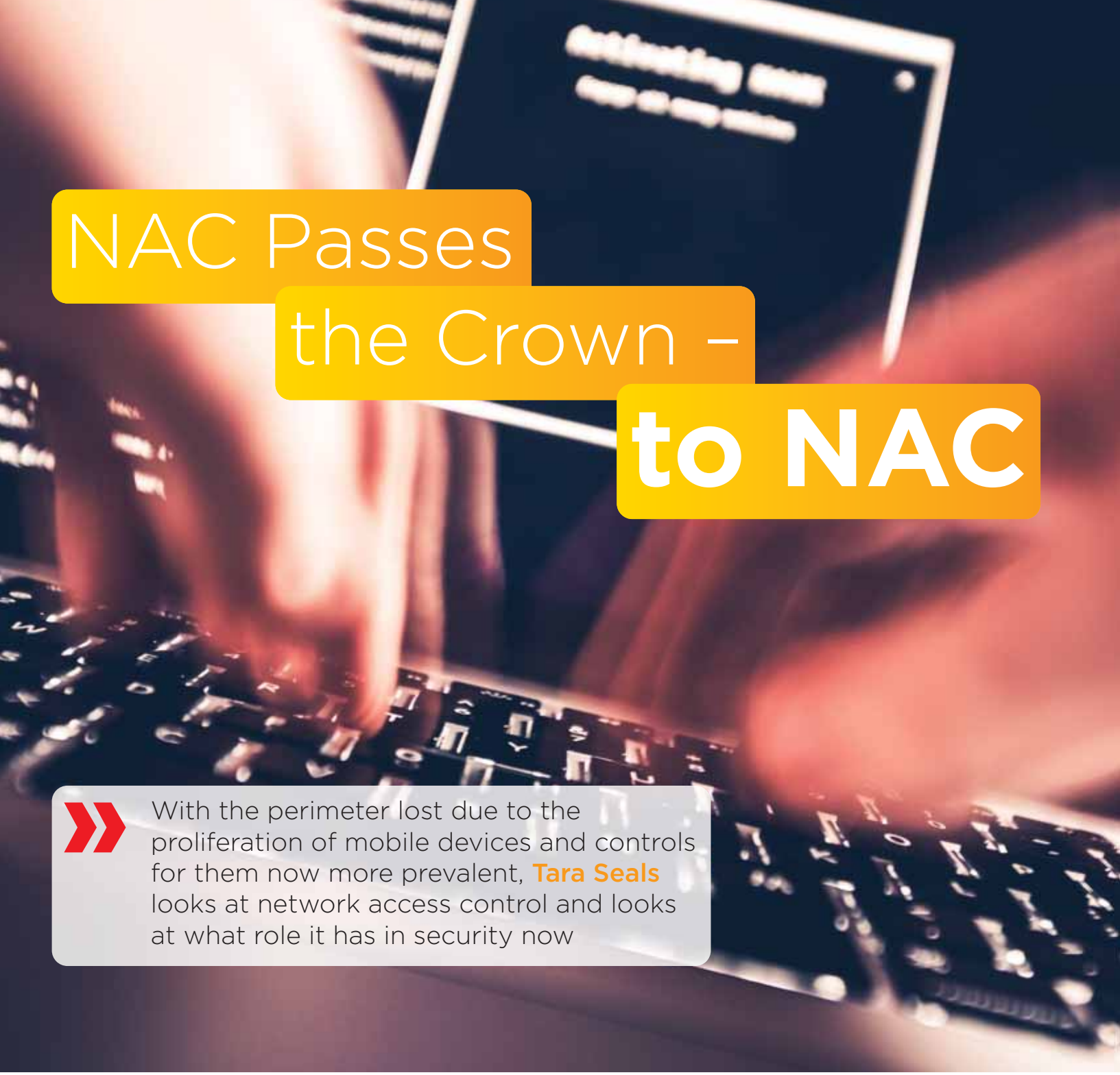
Vulnerabilities in software are still prevalent enough that agencies can develop (or procure) attacks to provide access to data. There is of course a question of leaving a vulnerability unpatched, but with regular version changes the window of exploitation is generally short and the vulnerability can be disclosed to the vendor at any time. Especially when physical access to the device is required, it is unlikely to threaten the security of millions. Finding and fixing bugs is a constant battle between attackers and defenders and provides investigators an opportunity for access. There is also a broader question around terrorist *modus operandi*. By running deception operations, it could be possible to mis-direct terrorists and criminals to use techniques or software that are not as secure as they appear to be, thereby removing the need to implant backdoors in software that is never used by the bad guys.

Unexpected Consequences

Software vendors should expect to see a rise in disclosure and interception requests as investigators seek to collect data earlier in investigations rather than risk losing access to it later. It may also result in more creative ways to get access to phones ahead of arrests, such as the recent case of British police using an undercover operation to secure an unlocked iPhone 5S.

Decisions concerning privacy and government capabilities are too often made as knee-jerk reactions to extreme events. Government spying programs were reined back post-Snowden following widespread anger, while the general public was happy to surrender a degree of privacy for security following the Paris and Brussels terror attacks.

The issue comes down to one of necessity and proportionality. Impacting the privacy of millions of innocent users where the investigative gain is limited is clearly disproportionate and unnecessary, but when lives are potentially at stake that balance can change, perhaps even *must* change, albeit for a limited time. We must be prepared, in certain circumstances, to forego some individual liberties for the sake of protecting our fellow citizens.



NAC Passes the Crown – to NAC

With the perimeter lost due to the proliferation of mobile devices and controls for them now more prevalent, **Tara Seals** looks at network access control and looks at what role it has in security now

Network access control (NAC) seems like such a simple concept on the surface: in its purest form, it's a set of technologies that automates user and device authentication onto networks, blocking risky devices and rogue log-in attempts. It also lets IT departments know what's connecting to the network, from where and for what purpose.

However, as they say, the devil is in the details. Thanks to complexity and implementation challenges, NAC has caused IT teams headaches for years, earning itself a lingering bad reputation.

Ironically, NAC's downfall appears to have become its salvation. More complexity, brought on by shifts in how people work is contributing to a major renaissance for NAC's role in the security landscape. The adoption of cloud IT, mobile working, the Internet of Things (IoT), and requirements for anytime, anywhere access to corporate resources are necessitating the automation of policy enforcement based on authentication, discovery, endpoint configuration or users' role/identity. In this environment, NAC can increase network visibility in order to reduce the risks associated with noncompliant devices and open access to enterprise network facilities.

The NAC market grew 36% in 2014 to earn revenues of $552.8 million; Gartner expects this to more than double to $1.46 billion by 2018.

"There is a key benefit to controlling access to an enterprise's infrastructure

through the network components: such control is endpoint-independent," Gartner said in a brief. "NAC can be used to isolate IoT devices and other nonstandard endpoints at the network switch or the wireless infrastructure."

NAC is Dead

In the past, NAC was first and foremost meant to address otherwise cumbersome ways of managing network connections. IT could use existing network tools for monitoring DHCP and DNS servers to look for new devices that are connecting to the company infrastructure. Typically, this was done on an exception basis, with any out-of-the-ordinary behavior triggering alarms. Alternatively, IT could also closely monitor network traffic for new connections and vet each one manually.

Obviously, neither approach is without headaches and overhead, so traditional NAC came on the scene. Unfortunately, it brought its own set of challenges.

In the early days, NAC capabilities were typically built into network vendor products, like switches and routers – Cisco was a first-mover in the space. As such, these tended to be proprietary solutions and led to a certain amount of vendor lock for businesses. "That's a lingering issue," explained Brian Honan, a security analyst at BH Consulting. "It can prove challenging to adapt to changing needs. If you want to integrate with other systems that have more function-specific approaches, it's a major headache."

A more recent way to implement NAC is to use a software-based solution, where agents are placed on various approved devices, and everything without an agent is blocked from connecting to the network. Honan noted that this is the more flexible and transparent way to do things, but it still can't easily accommodate changes in the way modern business works, and it brings an immense amount of overhead for administrators.

"If you take the fact that most companies are dealing with shadow IT and bring-your-own-device (BYOD), along with more mobile users and teleworkers, you now have devices that aren't physically there anymore, but are rather connecting via cloud or internet," Honan said. "So companies need to look at a combination of NAC for their traditional network, and mobile device management (MDM) for managing mobile platforms. With the growth in new threats you have people in offices with their own laptops and controlling that type of access is becoming much more of a challenge."

> NAC hasn't taken off the way it was expected to a number of years ago; that's down to the vendors and the customers not understanding how to implement it properly
>
> Brian Honan

Not only that, but, as Pulse Secure points out in a recent brief, today's work environment is open and collaborative, and visitors, contractors, and business partners expect on-demand connectivity to the enterprise network and resources, and that makes an agent-oriented approach almost impossible to manage.

"Further to this, the combination of the IoT, cloud applications and BYOD means there are more endpoints accessing the network than ever before," the firm said. "Each employee can have multiple devices accessing the network – a corporate device, mobile phone and their own iPad or Ultrabook, all with different operating systems and regularly updating software."

All of that has earned traditional NAC a bad reputation for disastrous implementations.

"In many large organizations, networks have evolved over years, if not decades," said Honan. "What NAC tries to do is enforce order on that chaos – and that is the biggest challenge. I've seen companies roll out NAC effectively, but I've also seen plenty of NAC projects fail because of the complexities involved. The IT staff tends to underestimate the time and the effort required to get NAC up and running properly. So NAC hasn't taken off the way it was expected to a number of years ago. That's down to the vendors and the customers not understanding how to implement it properly."

Long Live NAC

To address this snowballing complexity in the enterprise environment, NAC has begun to evolve. From a technology standpoint, by all accounts, NAC has gotten easier to use, with a better ability to centralize the administration efforts and to use network behavioral analysis with rules that are dynamic and flexible about what should and should not be allowed on the network. Most notably, NAC support for mobile devices, roaming users and virtual machines is increasingly part of the solution. As the penetration of these devices increases, and the apps they run become more business-critical, NAC is starting to become not just device-aware, but also app-aware.

"Users expect a simple, consistent and app-like experience both on and off the network," said Jodie Sikkel, network infrastructure and security specialist at ANSecurity. "In addition, organizations need technology that allows customers, guests and contractors to have a positive experience of connecting to the guest network when they visit too."

She pointed out that for today's organizations with distributed workforces and BYOD policies, having a user-based policy approach is critical.

"Companies need to decide what a user's access rights are and apply a consistent policy across devices so that they can connect remotely or on-site, no matter what screen they're using," said Sikkel. "This is becoming much more about the user and their role."

To that end, updated NAC solutions can empower IT administrators with the ability to define, implement and enforce granular access polices for connecting endpoints based on contextual information (e.g., user ID, role, device type, security posture, location). This eliminates much of the burdensome overhead that NAC had become known for.

"A solution that takes all these factors into account and prevents unauthorized network, application or data access before the device connects to the enterprise, for both VPN and Wi-Fi access is a must for security," said Pulse Secure in its brief. "This protects the corporate network from infected devices and enforces consistent, cross-network access policies. It also ensures only authorized workers have access to enterprise resources based on their role, location and time of day."

This reduces the need for IT teams to create multiple policies across multiple platforms for access to the same resources.

"I think we're going to see an evolution where you won't have pure, traditional NAC solutions anymore, but rather a collection of technologies that includes endpoint management and MDM," Honan said. "Instead of having different platforms to do all of these things, companies will be looking for one tool to manage them all. So we need to forget the traditional viewpoint of NAC and look at newer technologies."

New Roles – and a Caveat

Modern NAC is also flexing its wings – because of the data that it collects and uses, its role can be exploited to increase overall visibility.

"We barely use the word NAC today, because the value proposition has evolved to do so much more than what it was meant to do originally," said ForeScout chief strategy officer, Pedro Abreu. "The original NAC was a good idea, but the devices were already corporately owned, so this was a second layer of technology. Secondary NAC didn't give you too much more visibility than you already had."

However, in the last four years, companies have seen a 40%-50% on average growth in the number of devices connecting to their networks, he said. "Companies lost visibility to what they really had in their networks. In a number of these breaches, attackers were in those networks for months and months, just hiding. So the value prop today is therefore visibility, while the original value prop was authenticating known users."

> If I'm a giant company with presence everywhere, NAC doesn't work
>
> Nathan Wenzer

It's not just mobile devices that companies have to worry about: it's also all of the IP devices out there now, be it a smart TV in the board room, a connected HVAC system, VoIP phones, printers, digital cameras and so on.

Abreu outlined one customer, a bank that literally had more than a million endpoints on the network, including indoor teller machines, ATMs and building automation sensors. Out of those, only 30% were actually being managed. "The new emerging threat is coming from that IoT space and all of the connected devices," he said. "You have to assume those devices can be compromised."

Abreu pointed out that companies should expect to deploy NAC technology, and then spend six to nine months just understanding what's in the environment and how it behaves. For instance, in one hospital, an Xbox was found – decidedly against IT policy, but after some calls, IT determined that the console was in the kids' oncology department and therefore should be allowed.

"It's a process of understanding why things are out of policy before moving on to the enforcement stage of the technology," Abreu said. "In the past, NAC could only give visibility if there was authentication. Now, it's important to have sequestered connections so you can figure out what's going on, and then take action."

Not everyone is so bullish. Nathan Wenzer, executive director of security at Thycotic, noted that while modern NAC is much more flexible, it's important to resist the urge to see it as a panacea or universally applicable.

"There's a big shift to focusing on users and privilege in the last few years because of the cloud and the hybrid network situation – companies are saying, 'I don't know what network I own, I don't know where users are, I don't control my own access.' The only consistent thing is the user and the credential coming in to access stuff – this has become the control point. You can't control people from the network layer anymore."

NAC therefore is going to be more of a targeted deployment within a controlled environment, Wenzler believes. "If I'm an energy company, where my systems are tightly regulated and airgapped, with a well-known and well-controlled environment, NAC works here," he said. "But if I'm a giant company with presence everywhere—NAC doesn't work. There, it has to be a privileged-based approach."

Ultimately, controlling which devices connect to the trusted corporate network is not a security function that should be left behind any time soon. That's especially true for organizations that have to meet with a compliance standard like PCI or HIPPA. In those cases, a rogue device could put them into a fine-drawing non-compliance state as well as open them up to a costly breach.

"NAC still has a place in our security infrastructure," said Oscar Marquez, CTO at iSheriff. "It remains extremely important that we protect our organization's network from rogue devices and ensure that devices that do connect meet with our security policy for endpoint security. Let's remember that one of the most publicized breaches of the last few years started with a climate control device [the Target breach]."

infosecurity®
EUROPE
07-09 JUNE 2016 OLYMPIA, LONDON.

Everyone & everything you need to know about information security

Guest speakers include:

Levison Wood
Day 1. 7th June 2016
10.00 - 11.00: Keynote Stage

The Right Honourable Lord Hague of Richmond
Day 2. 8th June 2016
10.00 - 11.00: Keynote Stage

Get the most from your visit

Plan your time at Europe's largest and most comprehensive information security event

Download the App
Infosecurity Europe 2016
Available on iOS and Android

Levison Wood
Opening Keynote speaker

Lord Hague
Opening Keynote speaker

Celebrating 21 years

Also featuring Industry Luminaries & Thought-Leaders including:

Mikko Hypponen
Security Researcher, Infosecurity Europe Hall of Fame Alumnus

Bruce Schneier
Security Technologist, Infosecurity Europe Hall of Fame Alumnus

plus many more...

Earn CPD/CPE Credits

If you have not already
REGISTER NOW

Don't miss out! Register online*
www.infosecurityeurope.com

*Online registration is complimentary until Monday 6th June 2016, 12:00 BST. Onsite registration is £35 + VAT.

Securing the Connected Organisation

The standoff between the FBI and Apple in early 2016, and subsequent resolution when a third party unlocked an encrypted iPhone, served to highlight once again the complex challenges facing information security professionals. Not only did the case throw into sharp relief the conflict between notions of privacy and national security, it also demonstrated that a hack can be found to bypass even the most rigorous security controls.

Whilst the high-level encryption debate rages on, at an organisational level information security professionals are charged with protecting increasingly connected organisations. The extended enterprise is connected to multiple partners and suppliers leading to a myriad of governance and assurance challenges. Tech savvy employees and customers are utilising new technologies to connect, collaborate and work smarter, often bypassing security controls and accessing shadow IT to improve efficiency and drive the business forward.

At the same time, a seismic technological shift is taking place towards machine-tomachine communication and the Internet of Things (IoT). Gartner predicts that 6.4 billion IoT devices will be used globally in 2016 and by 2020 they forecast that number will reach 20.8 billion. The potential privacy and security implications of the deluge of data generated by connected things are vast especially as for the manufacturers of IoT enabled products the priority is speed to market rather than security, so products aren't being designed with security in mind. As the cyber-physical threat landscape evolves, information security professionals need to ensure their organisation's security posture is such that they can manage existing risks while being prepared to tackle the emerging challenges on the horizon.

The need to communicate information security risk effectively to the board and wider business has never been more important as the threats become increasingly complex. There is no doubt that information security is seen as a business risk by senior management, and information security professionals really do have the board's attention. Yet, with dramatic headlines about cybercrime causing alarm in the boardroom, information security professionals are still struggling to cut through the hype to turn that attention into genuine understanding of the risk to ensure security is a top-down priority. The Talk Talk breach in 2015 illustrated very clearly that information security is a CEO's concern and that the board needs to be on top of this threat.

As cyber-attacks become increasingly sophisticated and cybercriminals themselves become more connected and collaborative, highly-skilled cyber defenders are needed to protect an organisation's sensitive information security assets. Yet the industry is facing a global skills shortage and as a result, information security leaders are grappling with the challenges of upskilling their security team to ensure it is equipped to deal with the challenges of the future.

Securing the connected organisation is the theme of this year's Infosecurity Europe and the event will provide you with the intelligence, insight and solutions you need to enhance the maturity of your organisation's security posture. Bringing together everyone and everything you need to know in information security, the event represents the highlight of the industry's event calendar.

Whether you want to keep up with the strategic direction of the industry, catchup with colleagues and peers and make new connections, engage with vendors and service providers to find out about the latest solutions, hear about the latest technological developments and research, or develop your career, Infosecurity Europe is the event for the information security community. I hope you will be a part of it this year.

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

Kerry Prince
Senior Director
Information Security Group

Reasons to attend Infosecurity 2016

Innovation, inspiration & learning

Come and help to shape the future of information security at Europe's largest information security event

260+

Renown and thought-leading speakers present

320+

Industry-leading exhibitors showcasing the most diverse range of products and services

160+

Hours of free education

15,000+

Infosecurity professionals, ready to share ideas

Inspirational Keynote Stage speakers at Infosecurity Europe 2016

The Keynote Stage speaker line-up at Infosecurity Europe 2016 reads like a who's who in information security, bringing together industry thought-leaders, expert practitioners, policy-makers and analysts.

Make sure you take advantage of the opportunity to gain insight, knowledge and a fresh perspective on your information security challenges by participating in the wide choice of Keynote Stage sessions.

Here are just a few of the speakers sharing their expertise on the Keynote Stage.

Opening Keynote. Day 1
Tuesday 7th June 10.00 -11.00

Levison Wood, presents **Perceptions of Risk, Resilience and Operational Security**. Drawing on his experiences walking the Nile and the Himalayas and during deployments across Africa and Asia as a Captain in the Parachute Regiment, Levison Wood will share his perspective on risk, resilience and operational security. Gain a fresh outlook on risk and a new way of looking at information security challenges.

Opening Keynote Day 2
Wednesday 8th June 10.00 – 11.00

The Right Honourable Lord Hague of Richmond, presents **Privacy vs Security: Reducing the Tension Between National Security, Privacy & Information Security.** Lord Hague has been a prominent political leader for over 20 years, having served as Foreign Secretary, Leader of the House of Commons and First Secretary of State. As such he is uniquely positioned to share his perspective on the challenge of balancing personal privacy, information security and national security.

Keynote Speaker
Panellist

Visit the website for the latest agenda and the full speaker line-up
www.infosecurityeurope.com/keynote_stage

Mikko Hypponen
Security Researcher, Infosecurity Europe Hall of Fame Alumnus

Keynote Speaker: Profiling the Connected Cybercriminal
Tuesday 7th June, 12.35 - 13.15

Bruce Schneier
Security Technologist, Infosecurity Europe Hall of Fame Alumnus

Keynote Speaker: Privacy, Trust & the Internet of Things
Wednesday 8th June, 14.40 - 15.20

Rik Ferguson
Advisor, Europol and Security Researcher, Infosecurity Europe Hall of Fame Alumnus

Panellist: Fostering Better Engagement Between Business & Law Enforcement to Effectively Respond to Cybercrime
Thursday 9th June, 10.50 - 11.40

James Lyne
Security Researcher

Panellist: Securing the Internet of Things: What is the Real Risk for Enterprise Cyber Security?
Tuesday 7th June, 14.30 - 15.20

Jaya Baloo
CISO, KPN Telecom

Keynote Speaker: Cryptography, Quantum Computing & the Future of Cyber Security Controls
Wednesday 8th June, 12.40-13.20

Cory Scott
Director of Information Security, LinkedIn

Keynote Speaker: How to Build an Effective Security Team
Tuesday 7th June, 13.30-14.10
Panellist: Next-Gen CISO: How to be a Successful Security Leader
Wednesday 8th June, 16.40-17.30

Lee Barney
Head of Information Security, Marks & Spencer

Panellist: Next-Gen CISO: How to be a Successful Security Leader
Wednesday 8th June, 16.40-17.30

Samantha Davison
Security Awareness & Education Program Manager, Uber

Panellist: Securing the Connected Human: Winning Hearts & Minds to Drive Secure Behaviour
Tuesday 7th June, 11.15-12.20

Troels Oerting
Group CISO, Barclays

Panellist: Next-Gen CISO: How to be a Successful Security Leader
Wednesday 8th June, 16.40-17.30

Gaynor Rich
Director, Information Security Risk & Governance, Unilever

Panellist: Headlines, Breaches & the Board: You've Got Their Attention – Now What?
Wednesday 8th June, 15.35-16.25

Brian Honan
CISO, KPN Telecom

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

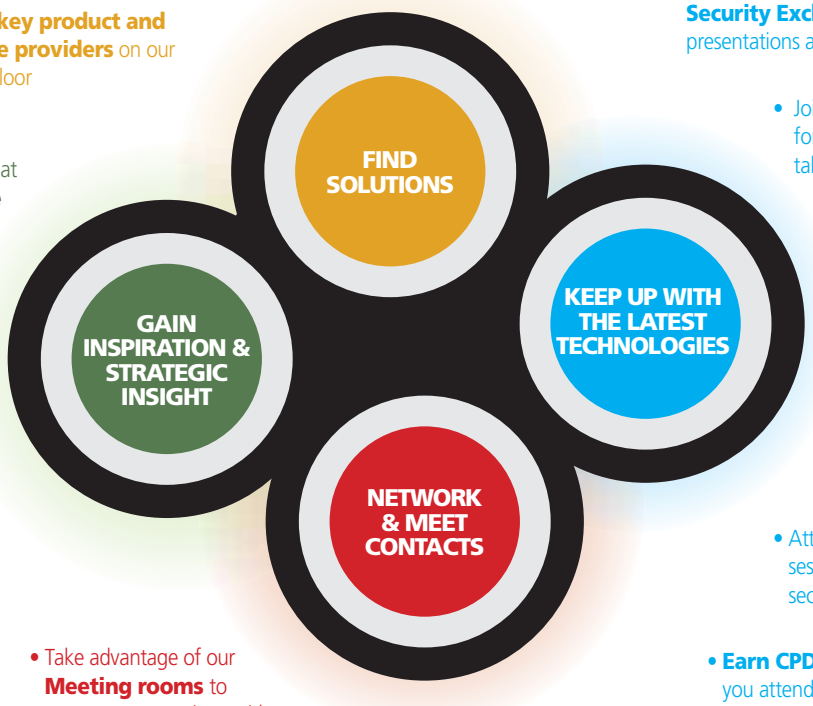
Join Dan Raywood Editor, Infosecurity Magazine in conversation with Brian Honan, 2016 Infosecurity Europe Hall of Fame inductee. During the session Brian will discuss his career in information security and share insight into how connected organisations should tackle cybersecurity incidents.

Thursday 9th June, 10.00-10.35

Be part of the infosecurity community

It's all here. **15,000+ professionals, 320+ exhibitors** and **160+ hours** of complimentary, leading-edge conference sessions. Where will you start?

- Go upstairs to check out the latest innovations at the **New Exhibitor Zone** and **UK Cyber Innovation Zone**
- **Meet key product and service providers** on our Show Floor
- Expand your thinking at our **Keynote Stage** with our best ever speaker line-up
- Take part in **Strategy Talks** to gain insight on how to secure your organisation from the top down
- For our VIPs, expand your network in the **VIP Lounge** and take part in Peer-to-Peer **Roundtable discussions** of strategic business issues
- Take advantage of our **Meeting rooms** to pre-arrange meetings with exhibitors
- Secure **Meet and Seat** with dedicated wifi and facilities for meeting contacts more informally
- Hear our **Tech Talks** to discover new approaches to combating cyber crime
- Take part in our **Information Security Exchange** for in-depth presentations and panel discussions
- Join our **Security Workshops** for practical know-how you can take back to your organisation
- Visit our **Technology Showcase** for a line-up of exhibitor demos and case studies
- Take advantage of onsite **Security Training** and learn how to optimise cloud security
- Attend our **Intelligent Defence** sessions to discover the latest in security research
- **Earn CPD/CPE credits** whenever you attend most conference sessions



cybersecurity innovation

Keeping pace with the sophisticated cyber criminal

Find the new Zones on the Upstairs Gallery at Olympia

NEW EXHIBITOR ZONE

UK CYBER INNOVATION ZONE

CYBER INNOVATION SHOWCASE

New Exhibitor Zone

Growing by 300% year on year, this is where you'll find all the companies you haven't seen before at Infosecurity Europe.

Cyber Innovation Zone

Visit the UK Cyber Innovation Zone at Infosecurity Europe in collaboration with techUK's Cyber Connect programme and The Department for Culture, Media & Sport.

Meet all 11 shortlisted companies in the **UK's Most Innovative Small Cyber Security Company competition** - Assuria, Intruder, Exonar, Device Authority, Sevin, Panaseer , Surevine, Glasswall, Segmantics, 4secure and Torsion Information Security - and join us for the final round of judging on the Keynote Stage on 8th June where the overall winner will be announced.

Cyber Innovation Showcase

Find out what's made the **Cyber Security Competition finalists** stand out, plus discover more innovation from other organisations including BAE Systems, CipherCloud, Citicus, KEYMILE, Netwrix, Pervade Software, Picus Security, Synopsys, ThreatConnect, Varonis, Verint Systems and Utimaco Waratek.

info security
STRATEGY | INSIGHT | TECHNOLOGY

INFOSECURITY AUTUMN VIRTUAL CONFERENCE

27TH - 28TH SEPTEMBER 2016

PLUS VISIT US ON STAND R80, LEVEL 1 AT INFOSECURITY EUROPE 2016, OLYMPIA LONDON

JOIN US AT THE LEADING VIRTUAL CONFERENCE EVENT

THE INFOSECURITY AUTUMN VIRTUAL CONFERENCE WILL PROVIDE THE OPPORTUNITY TO:

- EARN UP TO 10 CPE CREDITS TOWARDS YOUR SSCP®/CISSP® & ISACA CERTIFICATIONS
- ATTEND INFORMATIVE EDUCATION SESSIONS FEATURING HIGH CALIBER INDUSTRY SPEAKERS
- WATCH VIDEO CONTENT EXPLORING THE LATEST IN INFORMATION SECURITY TECHNOLOGY, PRODUCTS & SERVICES
- DOWNLOAD WHITEPAPERS, PRESENTATIONS, PRODUCT INFORMATION SHEETS AND OTHER DATA
- NETWORK WITH COLLEAGUES IN REAL TIME

THE FULL EDUCATION PROGRAM AND SPEAKER LINE-UP WILL BE ANNOUNCED SHORTLY. RESERVE YOUR PLACE FOR FREE TODAY & JOIN THE LEADING INFORMATION SECURITY VIRTUAL EVENT.

WE LOOK FORWARD TO WELCOMING YOU.

WWW.INFOSECURITY-MAGAZINE.COM/VIRTUAL-CONFERENCES

KEYNOTE STAGE

Keynote Stage sponsor:

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

Organisations are more connected than ever before and the resulting myriad of new threats, vulnerabilities and risks are ripe for exploitation by increasingly sophisticated cybercriminals who themselves connect and collaborate. It's against this complex threat landscape that information security professionals are tasked with protecting their organisation.

The Keynote Stage agenda will look at the challenges of securing the connected enterprise and provide strategic and practical advice on how to address them.

Insight, inspiration and fresh perspectives

Attend the Keynote Stage sessions to access information security knowledge and expertise presented by some of the industry's leading end-user practitioners, policy-makers, analysts and thought-leaders. You will gain new ideas, insight and actionable intelligence to enable you to streamline your information security strategy, accelerate the effectiveness of your security tactics and reinforce the critical position of your information security function.

Key themes to be addressed in 2016 include:

- **Securing the connected human:** Effective strategies and tactics to mitigate the human risk
- **Building cyber resilience in a connected enterprise:** Ensuring the essentials of resilient security are in place and new approaches to detect and respond to security incidents
- **Privacy and security in a connected world:** Tools, techniques and strategies to protect data privacy, secure information and balance privacy and security
- **Securing the Internet of Things:** Understanding the new technology paradigm and the implications for information security

Day One: Tuesday 7 June

Official Welcome

Raj Samani, VP, CTO, Intel Security, EMEA

10.00-11.00
Opening Keynote Presentation
Perceptions of Risk, Resilience and Operational Security

Levison Wood, Explorer & Writer

11.15-12.20
Panel Discussion
Securing the Connected Human: Winning Hearts & Minds to Drive Secure Behaviour

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

Thom Langford, CISO, Publicis Groupe

Samantha Davison, Security Awareness & Education Program Manager, Uber

Andrew Rose, CISO and Head of Cyber, UK Transport Sector

Moderator:
David Shearer, Chief Executive Officer, (ISC)²

This session will include the White Hat Charity Cheque Presentation.

12.35-13.15
Keynote Presentation
Profiling the Connected Cybercriminal

Mikko Hypponen, Security Researcher, Infosecurity Europe Hall of Fame Alumnus

---

13.30-14.10
Keynote Presentation
How to Build an Effective Security Team

Cory Scott, Director of Information Security, LinkedIn

14.30-15.20
Panel Discussion
Securing the Internet of Things: What is the Real Risk for Enterprise Cyber Security?

Professor Chris Hankin, Director, Institute for Security Science and Technology, Imperial College London

Ian Smith, IoT Security Lead, GSMA

James Lyne, Security Researcher

Moderator:
Peter Wood, Security Advisory Group, ISACA

15.35-16.15
Infosecurity Insight
How to Hack a Human: Anatomy of a Social Engineering Attack

Dr Jessica Barker, Independent Cyber Security Professional

16.30-17.25
Panel Discussion
Updates, Updates, Updates! Getting the Basics Right for Resilient Security

Paul Watts, CISO, Network Rail

Nick Green, Senior Director of Information Security, Ticketmaster

Jon Townsend, Director of Technology & Information Security, National Trust

Moderator:
Bob Tarzey, Analyst and Director, Quocirca

Day Two: Wednesday 8 June

10.00-11.00
Opening Keynote Presentation
Privacy vs Security: Reducing the Tension Between National Security, Privacy & Information Security

The Right Honourable Lord Hague of Richmond

11.15-12.25
Panel Discussion
Regulation, Risk & Privacy: Data Privacy, EU GDPR & the Global, Connected Enterprise

***Iain Bourne**, Group Manager (Policy Delivery), Information Commissioner's Office*

***Quentyn Taylor**, Director EMEA Information Security, Canon EMEA*

***Nina Barakzai**, Group Head of Data Protection & Privacy, Sky*

***Eduardo Ustaran**, Partner, Privacy and Cyber Security, Hogan Lovells*

Moderator:
***Stewart Room**, Partner PwC Legal, Global Head of Cyber Security and Data Protection, PwC*

12.40-13.20
Keynote Presentation
Cryptography, Quantum Computing & the Future of Cyber Security Controls

***Jaya Baloo**, CISO, KPN Telecom*

13.35-14.25
Competition Final
UK's Most Innovative Small Cyber Security Company of the Year
During this session the finalists from the national competition supported by the Department for Culture, Media & Sport and techUK, 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 Cyber Security Company of the Year'.

Judges:
***David A. Cass**, Vice President & CISO, Cloud and SaaS Operational Services, IBM*

***Warwick Hill**, CEO-in-Residence, Microsoft Ventures*

Additional judges to be confirmed

14.40-15.20
Keynote Presentation
Privacy, Trust and the Internet of Things

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

15.35-16.25
Panel Discussion
Headlines, Breaches & the Board: You've Got Their Attention – Now What?

***Darren Argyle**, CISO, Managing Director, Markit*

***Gaynor Rich**, Director Information Security Risk & Governance, Unilever*

***Matt Palmer**, CISO, Willis Towers Watson*

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

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

16.40-17.30
CISO Keynote Roundtable
Next-Gen CISO: How to be a Successful Security Leader of the Future

***Troels Oerting**, Group CISO, Barclays*

***Cory Scott**, Director of Information Security, LinkedIn*

***Lee Barney**, Head of Information Security, Marks & Spencer*

***Mark Hughes**, CEO BT Security, BT*

Moderator:
***Martin Whitworth**, Senior Analyst, Security and Risk, Forrester*

Day Three: Thursday 9 June

10.00-10.35
Infosecurity Europe Hall of Fame 2016
Brian is recognised for his long term contribution to information security, including as founder and CEO of Ireland's first CERT, special advisor to Europol's Cyber Crime Centre (EC3) and industry expert advising organisations, mentoring new professionals and lecturing on information security at University College Dublin.

2016 Hall of Fame inductee:
***Brian Honan**, Founder & CEO, BH Consulting*

Interviewer:
***Dan Raywood**, Editor, Infosecurity Magazine*

10.50-11.40
Panel Discussion
Fostering Better Engagement Between Business & Law Enforcement to Effectively Respond to Cybercrime

***Andrew Gould**, Detective Chief Inspector, Falcon – SCO7 Organised Crime Command (OCC), Metropolitan Police Service*

***Rik Ferguson**, Advisor, Europol and Security Researcher, Infosecurity Europe Hall of Fame Alumnus*

***Kurt Pipal**, Assistant Legal Attaché, Office of the Legal Attaché, FBI*

***Tom Mullen**, Head of Cyber Response & Security Operations, Telefónica (O2) UK*

Moderator:
***Brian Honan**, Founder & CEO, BH Consulting*

11.55-12.45
Panel Discussion
Enterprise-Wide Cyber Incident Response: Proactive Tactics for Rapid Response

***Calvin Dickinson**, Director of Information Security - Operations, Incident Response and Resilience, Amgen*

***Hem Pant**, CISO, ING Wholesale Bank*

***Vicki Gavin**, Compliance Director, Head of Business Continuity and Information Security, The Economist Group*

***Andy Talbot**, Global Head of Cyber Defence, Vodafone*

Moderator:
***Andrew Kellett**, Principal Analyst, Security, Ovum*

13.00-13.50
Panel Discussion
Managing & Mitigating 3rd Party Information Risk in the Connected Enterprise

***Arnaud Wiehe**, CISO, TNT Express*

***Mark Jones**, CISO, Allen & Overy*

***Steve P. Williamson**, Director, Governance, Risk and Compliance, GlaxoSmithKline*

***Will Harvey**, Head of Assurance and Head of Security Profession, HMRC*

***Daniele Cattedu**, CTO, Cloud Security Alliance*

Moderator:
***Mike StJohn-Green**, Principal Analyst and Technical Advisor, Information Security Forum*

14.05-15.00
Secure Coding & Development: Embedding Application Security into Business Processes
Panel Discussion Featuring:

***Francois Raynaud**, DevSecOps Leader - Threat Management Lead, ASOS.com*

***Anton Karpov**, CISO, Yandex*

***Giacomo Collini**, Director of Information Security, King.com*

Moderator:
***Adrian Sanabria**, Senior Analyst, Enterprise Security Practice, 451 Research*

STRATEGY TALKS

Strategy Talks sponsor

BLUE COAT®

Strategic Insight to Optimise Security Posture

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

Day One: Tuesday 7 June

10.00-10.25
Security Automation in the SDLC – Real World Cases

Ofer Maor, *Director of Security Strategy, Synopsys*

10.40-11.05
Keep Your Eye on the Data Without Breaking Your Budget: Best Practices to Cost Effective GDPR Compliance

Austin O'Malley, *Chief Product Officer, Ipswitch*

11.20-11.45
Securing the Shift to Cloud Application Usage

Scott Reeves, *Senior Cloud Security Specialist, Blue Coat Systems*

12.00-12.25
Formulating a Security Policy for the Modern IT Landscape

Cris Thomas, *Strategist, Tenable Network Security*

12.40-13.05
Can Public Cloud Solutions be Made Safe for Business? What is the Alternative?

Vidhya Ranganathan, *SVP Products and Engineering, Accellion*

13.20-13.45
From Pump Room to Board Room - Tactically Improving the Cyber Security Posture of the Critical National Infrastructure

Dan Turner, *CEO, Deep-Secure*

Keith Chappell, *Technical Business Development Director, Iguana Security*

14.00-14.25
1 Kit, 8 Steps, 30 Days. How We Raised Application Security Awareness

Amit Ashbel, *Cyber Security Evangelist, Checkmarx*

14.40-15.05
How Lloyds Banking Group is Transforming Their Information Protection Strategy

Tim Porter, *Domain IT Security Engineer, Lloyds Banking Group*

Stephane Charbonneau, *Chief Technology Officer (CTO), Titus*

15.20-15.45
Anatomy of an Attack - MEDJACK Spreads Across Healthcare Systems Globally

Carl Wright, *EVP, TrapX Security*

16.00-16.25
How Do You Know if Your DDoS Mitigation Solution Will Stop a DDoS Attack?

Raza Rizvi, *Technical Director, activereach*

16.40-17.05
Exploring Regulatory Standards – Is Your Organisation Protected?

Luke Hull, *Director of Mandiant Consulting – UKI, FireEye*

Day Two: Wednesday 8 June

10.00-10.25
Advanced Incident Investigation: Lessons Learned from APT Victims

Don Smith, Technology Director, Dell SecureWorks

10.40-11.05
Fostering an Enterprise-Wide Security Culture

Professor Mark Skilton, Managing Consultant, PA Consulting

11.20-11.45
Rethinking Defence-In-Depth

Dr Hugh Thompson, Chief Technology Officer, Blue Coat Systems

12.00-12.25
Man v Machine: How Systems and Users can Work Closely to Mitigate Insider Threat and Accidental Breach

Tony Pepper, CEO, Egress Software Technologies

12.40-13.05
Turning the Network Inside Out

Ronen Shpirer, Security Solutions Manager, Fortinet

13.20-13.45
Low Friction Security

Piers Wilson, Head of Product Management, Huntsman Security

14.00-14.25
Why I Quit My Dream Job at Citi: A Data Centric Approach to Information Protection

Mike Bass, Head of Customer Strategy, Ionic Security

14.40-15.05
The CISO Checklist: Do You Know What Your Vendors Are Doing?

Joe Schorr, Director, Advanced Security Solutions, Bomgar

15.20-15.45
How Typical Corporations Use, Move and Store Sensitive Data: The Inaugural Digital Guardian Data Trends Report

Mark Stevens SVP, Global Services, Digital Guardian

16.00-16.25
PCI DSS and Data Protection – Essential Principles for Success

Ian Davis, Head of Consultancy, Red Island

16.40-17.05
The Visible Attack Surface – What it is and Why it Matters

Gidi Cohen, CEO and Founder, Skybox Security

Day Three: Thursday 9 June

10.00-10.25
The New Era in Cybersecurity Legislation: Learning from the German Experience

Rainer Rehm, Chapter President, (ISC)² Chapter Germany

10.40-11:05
Mind and Communication Hacking

Philip Fanthom, Managing Director, Jenrick IT

11.20-11.45
How To Minimise Cybersecurity Exposure Before, During and After an Emergency

Kevin Flynn, Director, Products, Blue Coat Systems

12.00-12.25
Effective and Efficient Management of Vulnerabilities from Security Scanning

Richard Mayall, Partner and Technical Director, Acuity Risk Management LLP

David Williams, Security Manager, Giesecke & Devrient GB

12.40-13.05
Cybercrime-as-a-Service: Driving Next-Gen Antimalware Products

Bogdan Botezatu, Senior E-Threat Analysis, Bitdefender

13.20-13.45
Data Breach Survivor: Real World Tips, Tricks and Advice

Paul Edon, Director of International Services, Tripwire

14.00-14.25
Threat Intelligence – Lessons on Creating a Capability

Mark Tibbs, Intelligence Development Manager, Digital Shadows

14.40-15.05
Elementary! How to Investigate Like Sherlock

Yaroslav Rosomakho, Principal Consulting Engineer, Arbor Networks

15.20-15.45
Insider Threats - Employees are the Weakest Link

Michael Newman, CEO, My1Login

Adrian Romano, Security Co-ordinator, Betsson Group

TECH TALKS

Tech Talks sponsor

CISCO

Technical Approaches to Resilient Security

Gain the latest technical tools, techniques and skills to successfully combat today's sophisticated cyber criminal.
To view the full agenda and latest speaker and session updates please visit **www.infosecurityeurope.com/techtalks**

Day One: Tuesday 7 June

10.00-10.25
Case Study: Modern Malware Investigation Techniques

***Gad Z Naveh**, Thought Leadership Manager, Checkpoint Software Technologies*

10.40-11.05
Allied Irish Bank – The Journey to Secure the Cloud

***Nigel Hawthorn**, Chief European Spokesperson, Skyhigh Networks*

***David Cahill**, Security Strategy & Architecture Manager, Allied Irish Bank*

11.20-11.45
The Continuing Evolution of Ransomware

***Martin Lee**, Technical Lead, Security Research, Cisco*

12.00-12.25
Social Media - Information Security's Achilles Heel

***Simon King**, Head of IT, Infinigate*

12.40-13.05
Ready Player Two - The Role of AI in Security Operations

***Neil Thacker**, Information Security & Strategy Officer, Forcepoint*

13.20-13.45
Defending Against Mimikatz et al Golden Ticket Based Attacks

***Steve Armstrong**, Technical Security Director, Logically Secure*

14.00-14.25
50 Shades of Dark:
From the Surface to the Dark Web

***Staffan Truve**, CTO & Co-Founder, Recorded Future*

14.40-15.05
Automating Incident Response:
Adopting a Continuous Response Model

***Justin Harvey**, CSO, Fidelis Cybersecurity*

15.20-15.45
Full Stack Cloud Attack

***Erik Peterson**, Director of Technology Strategy, Veracode*

16.00-16.25
Leaky Apps and Devices in a New Era of Mobile

***James Plouffe**, Lead Solutions Architect, MobileIron*

16.40-17.05
Who Moved My Network?
Preparing for the Software Defined Era

***Ken Sohal**, SE Director, EMEA, AlgoSec*

Day Two: Wednesday 8 June

10.00-10.25
Privileged Access Management: Controlling the Lock

Kalle Jääskeläinen, VP, Solutions and Services, SSH Communications Security

10.40-11.05
Actionable Analysis: Wielding Threat Intelligence

Brandon Hoffman, Chief Technology Officer, Lumeta Corporation

11.20-11.45
Journey to a Secure Cloud

Jeff Wicks, Chief Security Officer, Cisco Cloud Offerings, Cisco

12.00-12.25
Evasion and Anti-Evasion: An Ongoing Game of Cat & Mouse

Lars Haukli, Senior Security Researcher, Blue Coat Systems

Felix Leder, Director, Advanced Malware Defence, Bluecoat Systems

12.40-13.05
Lessons for the Aspiring Digital Detective

Bernard Parsons, CEO, Becrypt

Chris Cassell, Pre Sales Technical Consultant, Becrypt

13.20-13.45
Defending Against Phishing Attacks: Case Studies and Human Defences

Jim Hansen, Chief Operating Officer, PhishMe

14.00-14.25
Nowhere to Hide: Catching Cross-Platform, Targeted Ransomware

Andrew Young, VP, Product Management, WatchGuard Technologies

14.40-15.05
Fullstack Vulnerability Management at Scale & The Future of Security Assessment

Eoin Keary, CTO/Founder, edgescan

15.20-15.45
Protecting Your Organisation's Crown Jewels: Ignore at Your Peril – Protect at all Costs

Mark Chaplin, Information Risk Management Specialist, Information Security Forum

16.00-16.25
How Cybercriminals Breached the ATM and Why you Should Care…

David Sancho, Senior Anti-Malware Engineer, Trend Micro

16.40-17.05
How the Makers of Candy Crush, King.com Upped Their Game in Breach Prevention

Giacomo Collini, Director of Information Security, King.com

Henry Seddon, VP EMEA, Duo Security

Day Three: Thursday 9 June

10.00-10.25
User Behaviour Analytics: A Sophisticated Tool for Organisations to Detect Malicious Insiders

Balázs Scheidler, Co-founder and CTO, BalaBit IT Security

10.40-11:05
Phishing Attacks - Are You Ready to Respond?

Matthias Maier, Security Evangelist, Splunk

11.20-11.45
Secure Your Digital Transformation

Simon Saunders, Advisor, Security Advisory Services, Cisco

Wil Rockall, Principal, Security Services, Cisco

12.00-12.25
More Trouble at t' Random Number Mill - How to Avoid Common Cryptographic Blunders

Paul Ducklin, Senior Technologist, Sophos

12.40-13.05
DDoS: Barbarians at the Gate(way)

Dave Lewis, Global Security Advocate, Akamai Technologies

13.20-13.45
Ten Years On: Lessons From A Decade Of Website Security Statistics

Ryan O'Leary, Vice President, WhiteHat Security

14.00-14.25
Cyber CSI: Using Security Intelligence to Predict Future Cyber-Attacks

Andrew Hollister, EMEA Director, LogRhythm Labs, LogRhythm

14.40-15.05
Top Ten AWS Cloud Security Best Practices

Justin Lundy, CTO, Evident.io

15.20-15.45
A Year on From a Leaky Kettle. Has Security of the Internet of Things Improved?

Ken Munro, Partner, Pen Test Partners

Infosecurity Europe Hall of Fame 2016

Join Dan Raywood in conversation with Brian Honan, 2016 Infosecurity Europe Hall of Fame inductee at 10.00-10.35 on Thursday 9th June on the Keynote Stage.

During the session Brian will discuss his career in information security and share insight into how connected organisations should tackle best practice in incident response.

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 **Jack Daniel, Dr Eric Cole, Mikko Hypponen, Shlomo Kramer, David Lacey, Professor Fred Piper, Professor Howard Schmidt, Bruce Schneier, Whitfield Diffie, Paul Dorey, Stephen Bonner, Dan Kaminsky, Eugene Kaspersky and Phil Zimmerman.**

TECHNOLOGY SHOWCASE

Discover the Latest Information Security Technologies and Solutions

During these sessions, exhibitors will take to the stage to demonstrate the capabilities of their information security technologies. Keep up-to-date with the latest developments to gain the insight you need to maximise ROI on your solution purchases.

Don't miss this chance to hear about the latest technical developments and breakthroughs and pose your questions directly to the vendors.

Presenting companies include: **BackBox, Black Duck Software, CyberArk Software, Cyberbit, Extrahop Networks, HEAT Software, Juniper Networks, OneLogin, Pulse Secure, Splunk, SSH Communications Security, SySS, Wallix, Wandera, Watchful Software, whiteCryption, Wombat Security Technologies** and **Zscaler.**

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

CYBER INNOVATION SHOWCASE

Access the Latest Innovations in Cybersecurity

Take this chance to hear about the newest innovations in cybersecurity. The agenda includes presentation by the 11 shortlisted companies from the competition funded by Department for Culture, Media & Sport in partnership with techUK's Cyber Connect to find the UK's Most Innovative Small Cyber Security Company.

The sessions will give you in-depth insight into the products and services these, and other organisations have designed, developed and brought to market.

The 11 shortlisted companies showcasing their technologies are **Assuria, Intruder, Exonar, Device Authority, Sevin Cyber Security, Panaseer, Surevine, Glasswall Solutions, Segmantics, 4Secure** and **Torsion Information Security.**

They will be joined by **BAE Systems, CipherCloud, Citicus, KEYMILE, Netwrix, Pervade Software, Picus Security, Synopsys, ThreatConnect, Varonis, Verint Systems, Utimaco Waratek**.

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

SECURITY WORKSHOPS

Practical Techniques and Strategies to Manage Information Risk

Build your skills during in-depth, extended workshop sessions and leave with practical know-how and learning that be applied directly to your business. Take advantage of the opportunity to engage with your peers and learn from leading security experts and leave the workshops with practical know-how and learning that can be applied directly to your business.

Organisations offering workshops include **(ISC)², Appsense, BCS, Centrify, Certes Networks, Cloud Security Alliance, CrowdStrike, Cyberbit, DevOps.com, RHEA Group, Splunk,** the **IISP.**

Topics to be addressed include:

- **Securing Your Cloudy Assets -** Splunk
- **Planning for SOC 3.0: Case Study -** Cyberbit
- **The Case for Privileged ID Management - The New Approach to Identity -** Centrify
- **Evidence-based Trust: Addressing Assurance Challenges and Using Security as a Differentiating Factor -** Cloud Security Alliance
- **Managing Your Career in Cyber and Information Security When so Much is Changing – What Skills do You Really Need? -** Institute of Information Security Professionals (IISP)
- **Professionalising Information Security -** BCS
- **The Case for Privileged ID Management- The New Approach to Identity -** Centrify
- **DevOps Connect: DevSecOps –** DevOps.com
- **Shrink the Attack Surface: Managing Risk in the Modern Enterprise -** Certes Networks
- **Catch, Patch and Match – 3 Simple Steps to Secure Your Windows End Points –** Appsense
- **CISSP Preview: Security & Risk Management -** (ISC)²
- **CISSP Preview: Business Continuity & Awareness Programme Requirements -** (ISC)²

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

SECURITY TRAINING

Certificate of Cloud Security Knowledge (CCSK)

cloud security alliance℠

Discover how to optimise cloud security within your organisation

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

Date: Thursday 9th June 9.00-17.00
Price:£649+VAT
Register and find out more at **www.infosecurityeurope.com/ccsk**

infosecurity INTELLIGENT DEFENCE
European Technical Research Conference

7 & 8 June 2016,
London Olympia

Access the Latest Technical Research and Defensive Tools and Techniques

Take a deep-dive into the latest risks, trends, cyber-attack methodologies and intelligence-based defence strategies to detect, contain and respond.

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

Day One: Tuesday 7 June

10.30-11.30
Keynote Presentation

Details to be announced

11.45-12.45
Sweet Security: Building a Defensive Raspberry Pi

***Travis Smith,** Senior Security Research Engineer, Tripwire*

13.00-14.00
Identifying and Containing Malware Threats with Global Signal and Pattern Analysis

***Dhia Mahjoub,** Technincal Leader, OpenDNS*

***Thomas Mathew,** Security Researcher, OpenDNS*

14.15-15.15
Big Problems with Big Data – Crash Course on Hadoop Interfaces Security

***Jakub Kaluzny,** Senior IT Security Consultant, SecuRing*

15.30-16.30
Fun in Memory with PowerShell and a Debugger

***Pierre-Alexandre Braeken,** Architect, Industrielle Alliance*

Day Two: Wednesday 8 June

10.30-11.30
Keynote Presentation

Details to be announced

11.45-12.45
Barbarians at the Gate(way)

***Dave Lewis,** Global Security Advocate, Akamai Technologies*

13.00-14.00
Demystifying Host Card Emulation Security - Best Practices for Implementing Secure Mobile Payments

***Slawomir Jasek,** IT Security Expert, SecuRing*

***Wojciech Dworakowski,** IT Security Expert, SecuRing*

14.15-15.15
Using Chrome to Attack Users: The Power of JS

***Jokin Guevara,** Infosec Consultant, ClouddyUK*

INFORMATION SECURITY EXCHANGE

Get-to-grips With the Latest Innovations in Information Security

Take advantage of the opportunity to attend in-depth presentations and panel discussions and gain new approaches and techniques to enable you to enhance your organisation's information security strategy and tactics.

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

Day One: Tuesday 7 June

10.30-11.30
Data Governance: How to Protect Your Assets

***Nathan Collins**, EMEA Business Development Director, Druva*

11.45-12.45
Defense Against the Dark Apps

***James Plouffe**, Lead Solutions Architect, MobileIron*

13.00-14.00
Secure Access is About IT Saying "Yes" To The Next Generation Of Workers, Apps, Networks And Things

***Kevin Sapp**, VP of Strategy, Pulse Secure*

14.15-15.15
Cyber Security: Preventing the Known and Unknown

***Amnon Bar-Lev**, President, Checkpoint Software Technologies*

15.30-16.30
Rise of the Machine – Securing the Internet of Things

***Jordi Cuesta**, Evidian I&AM Product Director, ATOS*

***Charles Piron**, IoT & SmartCards CyberSecurity Manager, ATOS*

Day Two: Wednesday 8 June

10.30-11.30
How to Create a Secure Digital Workspace

***Ian Evans**, Vice President - End User Computing, Managing Director - AirWatch, EMEA, VMware AirWatch*

11.45-12.45
State of Vulnerabilities, Exploits and the Best Practices for Prioritising Remediation

***Wolfgang Kandek**, Chief Technical Officer, Qualys*

***Jayson Jean**, Director, Vulnerability Management, Verisign*

***Raimund Genes**, Global CTO, Trend Micro*

13.00-14.00
How One of the World's Biggest Retailers Protect Their Application Infrastructure Against Next-Generation Cyber-Attacks

***Werner Thalmeier**, Director Security Solutions EMEA&CALA, Radware*

14.15-15.15
WiFi - Convenient, Ubiquitous and Fast. All it Lacks is Secure!

***Patrick Grillo**, Director, Security Strategy, Fortinet*

15.30-16.30
The Impact of EU Legislation on Cyber Security in the UK

***Greg Day**, VP and Chief Security Officer, Palo Alto Networks*

Day Three: Thursday 9 June

10.30-11.30
Threat Protection, New Technologies and Data Privacy: Today's View of Security

***Chris Richter**, SVP Global Security Services, Level 3 Communications*

11.45-12.45
Evaluating the Business Case for Cloud Based IAM (Identity Access Management)

***Charles Read**, Director, OneLogin*

***James Smith**, CMO, OneLogin*

13.00-14.00
In a World of 100% Encrypted Traffic, Who Wins?

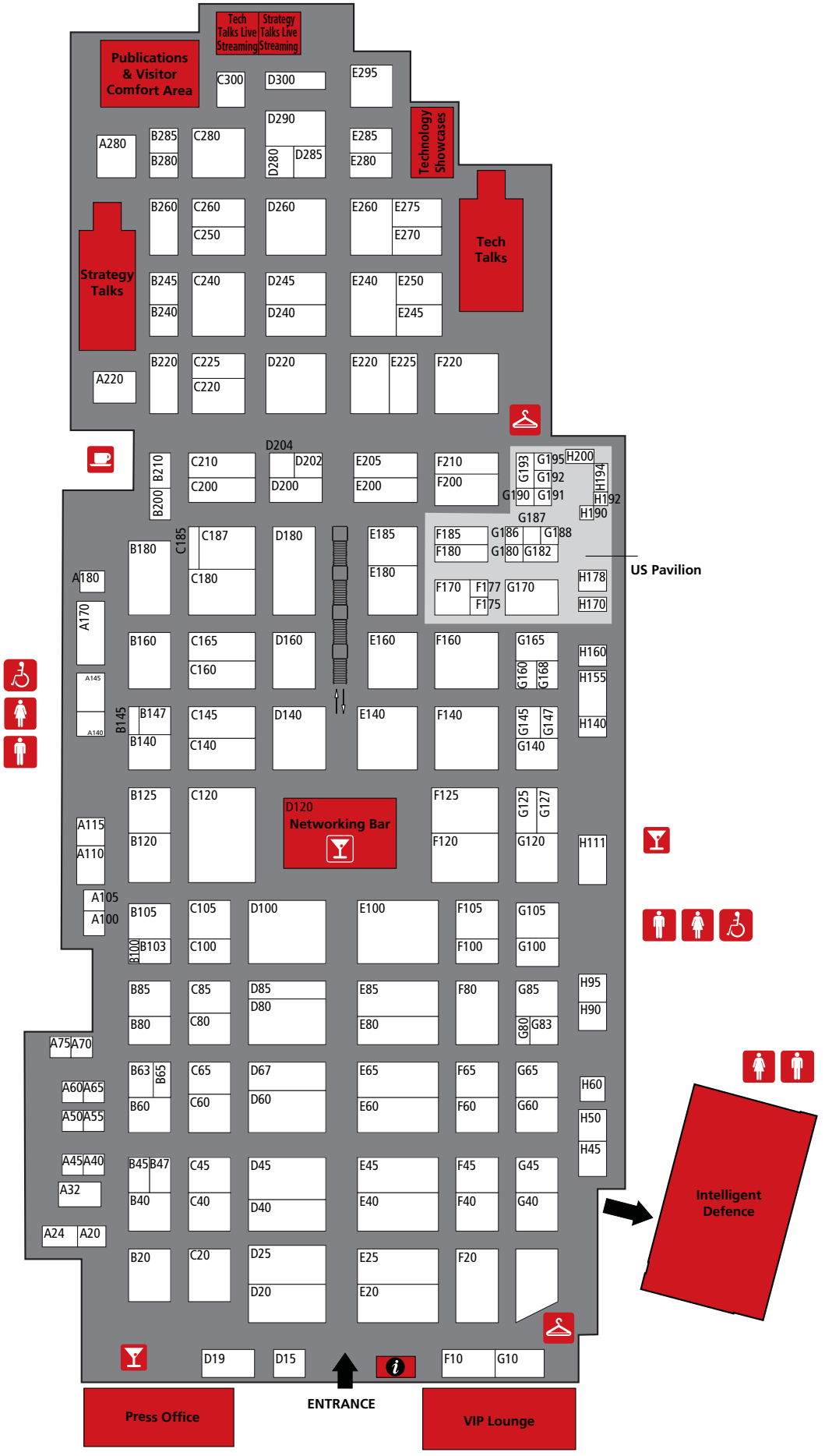
***Günter Ollmann**, Chief Security Officer, Vectra Networks*

14.15-15.15
The True Costs of DDoS Mitigation

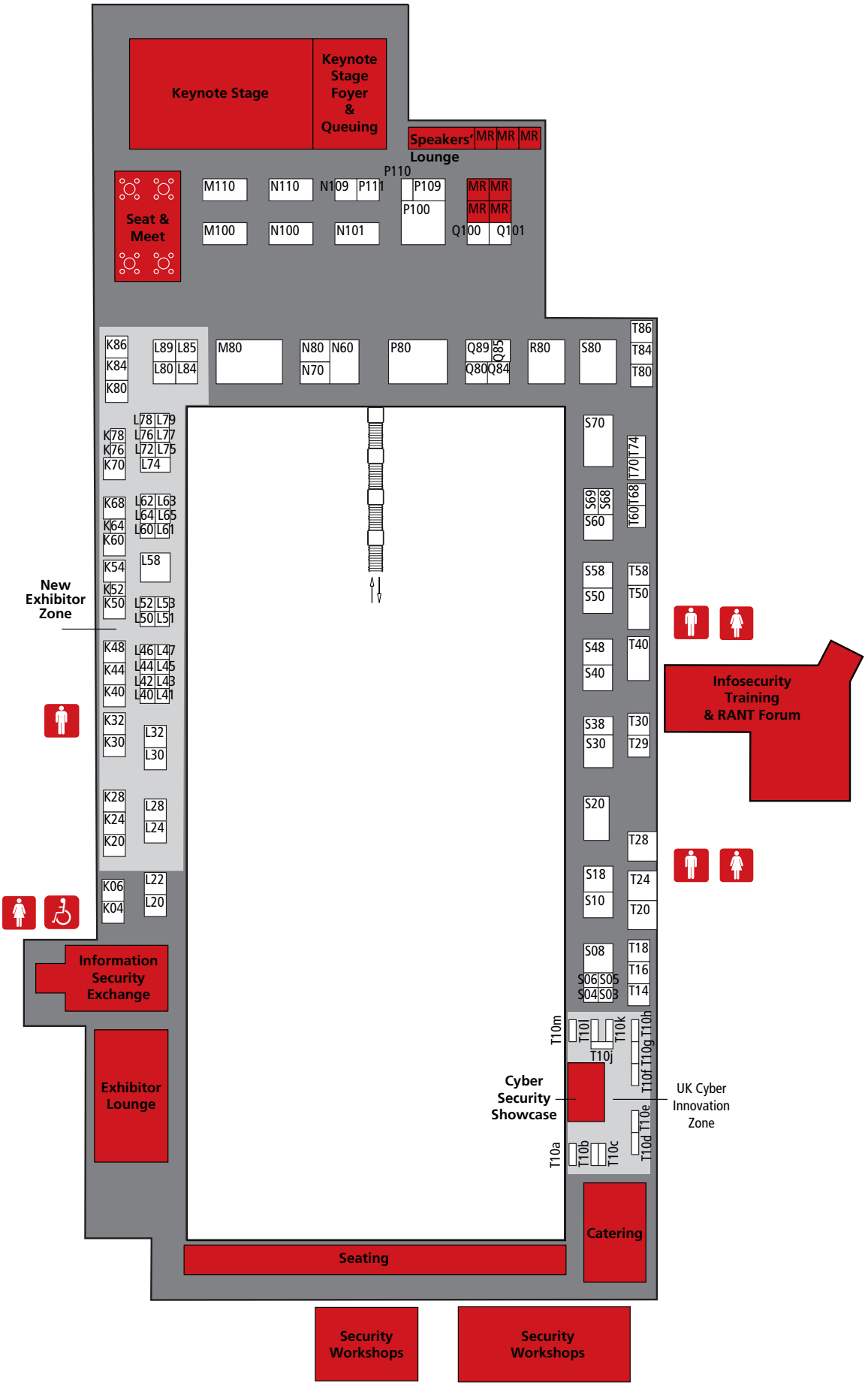
***Alex Cruz Farmer**, VP Cloud Services, NS Focus*

Floorplan

Ground floor



Level 1
Upstairs Gallery



A-Z Exhibitor List

Juniper Networks UK Limited	F200

K

Kaymera Technologies	L77

L

Lancope Inc	F10
Lastline, Inc	H178
Level 3	E250
LibraEsva Srl	H160
Light Cyber	F175
Link11 GmbH	E45
Logically Secure Ltd	C80
LogRhythm Ltd	D67
Louisiana State University	L45
Lumeta Corporation	H190

M

Malwarebytes	D240
ManageEngine	B103
ManageEngine	B103
Memset Ltd	K80
Mimecast Services Ltd	G100
Minded Security UK Limited	L79
Mobile Iron International	H111
MWR InfoSecurity	B260
My1login	B285

N

Natek A.S.	E185
NetSupport Ltd	B45
NETWORK TECHNOLOGY SOLUTIONS (UK) LIMITED	C187
Netwrix Corporation	B80
Neustar Inc	B20
Nexusguard	S10
Norse Group	G195
NSFOCUS Technologies UK Ltd	A280
NUIX TECHNOLOGY UK LTD	C300
Nuro Secure Messaging	L50

O

Observe IT	B65
Okta Inc	A115
Onelogin Inc	G182
OpenDNS	D19
Osirium	T20
Outpost24 UK	D45

P

PA Consulting (7safe)	A170
Palo Alto Networks (UK) Ltd	B180
PCI Security Standards Council	H170
Pen Test Partners	E85
Pentesec Limited	E225
Pentest Limited	G80
Pentura Limited	E275
PeopleNet Security Technologies Co., Ltd	H140
Pervade Software Ltd	S03
PhishMe Inc	F170
Picus Guvenlik A.S.	L42
Plixer	G170
Protected-Networks GmbH (8Man)	P80
Pulse Secure	D85

Q

Qualys	E20

R

R.I.M. Porter Novelli, LLC	S30
Radware	E260
RAPID7	D40
ReaQta Ltd	L46
Recorded Future	G168
Red Island	G165
RedOwl Analytics	K32
RedSeal Inc	E200
Resilient Systems Europe Limited	G140
RiskIQ UK Limited	G188
Royal Holloway, University of London	A180

S

Safe-T Data Ltd.	A24
SailPoint Technologies, Inc.	H155
Satisnet	D245
SC Magazine	E285
SecureWorks Europe Limited	G10
Security Cleared Jobs	T70
Selex ES Ltd	L89
SerNet GmbH	S70
ServerChoice	E220
Singapore Institute of Technology	K52
Sirrix AG	B200
Skybox Security Inc.	B40
Skyhigh Networks	D280
SmoothWall	B140
Solebit Labs Ltd	L40
Soliton Solutions	K54
Sonatype, Inc	G190
Sophos Limited	C120
Spectorsoft Corp	F177
Spikes Security, Inc.	G105
Splunk Services UK Ltd	C20
SSH Communications Security Corporation	F60
SureCloud	C85
Synopsys NE	G83
SySS GmbH	L62

T

Techweek Europe	A50
Tenable Network Security Limited	F160
Threat Quotient	G192
ThreatConnect	S20
ThreatStream	F180
Tier-3 Security Ltd	D160
Titania	G40
TITUS Inc.	S50
TM3 Software GmbH	B100
TrapX Security	G85
Trend Micro UK Ltd	D25
Tripwire International	D20
Tufin Software Technologies Ltd	B60

U

Unipart Security Solutions	K84
Utimaco IS GmbH	D15

V

Varonis UK Ltd	C40
Vasco Data Security SA	E60
Vectra Networks	S80
Veracode ltd	B120
Verint Systems Ltd.	D300
VERISIGN	E205
VÍNTEGRIS SL	N70
Vormetric	C140

W

Wallix	B210
Wandera	G125
Watchful Software Inc	C185
WatchGuard Technologies	E65
Websense UK Ltd	F80
Welsh Government	T24
whiteCryption	G180
WhiteHat Security Europe Limited	B47
WhiteSource	L61
Wick Hill Ltd	D100
Wombat Security Technologies, Inc.	G193

Y

Yoh Solutions Limited	A20
Yubico Ltd	k60

Z

Zenedge, Inc	K30
Zimperium	H194
Zscaler Inc	C220

This information was correct at the time of going to print. For the latest exhibitor list, please visit: **www.infosecurityeurope.com/exhibitor-directory**

CONNECTING THE INFOSECURITY COMMUNITY

SAVE THE DATES

6 - 8 June 2017

Olympia London

Infosecurity Europe 2017

Collect CPD/CPE Credits

Infosecurity Group is here to help the information security community to share, meet, discuss, network and inspire solutions all around the world.

Our global events deliver a physical meeting place for the community with unparalleled opportunities to showcase the latest products and services, network with peers and hear from thought-leaders and innovators.

infosecurity®
NETHERLANDS
Jaarbeurs Utrecht, Netherlands
www.infosecurity.nl

infosecurity®
BELGIUM
Brussels Expo, Brussels. Belgium
www.infosecurity.be

infosecurity®
RUSSIA
Crocus Expo, Moscow. Russia
www.infosecurityrussia.ru

infosecurity®
MIDDLE EAST
ADNEC, Abu Dhabi, UAE
www.isnrabudhabi.com

infosecurity®
MEXICO
Mexico City, Mexico
www.infosecuritymexico.com

infosecurity®
NORTH AMERICA
Omni Barton Creek Resort & Spa Austin, USA
www.one2onesummits.com/SEC

infosecurity®
EUROPE
07-09 JUNE 2016 OLYMPIA. LONDON.

Everyone & everything you need to know about information security

Retail Security – Lessons Learned Two Years On

Two years on from a surge of retail security data breaches, **Dan Raywood** looks at what lessons were learned and what has been done to prevent such headlines from being made again

It was December 2013, a week before Christmas, when the massive breach of US retailer Target hit the headlines. In the following months, 2014 saw the likes of Home Depot, Sally Beauty, Neiman Marcus and other US retailers in the news for all the wrong reasons.

The situation was not new – TJ Maxx reported a breach of over 45 million credit cards in 2007 – but what happened in 2014 was effectively a domino effect of retailers reporting major breaches one after the other. The situation was not restricted purely to retailers either – eBay reported a loss of around 145 million records in May 2014, while restaurant chain PF Chang revealed a data breach involving credit and debit card data stolen from restaurant locations nationwide across the USA.

> There are literally thousands of ma and pa stores that you don't hear about
>
> Steven Bullitt

Now two years on from these headlines, the focus of attackers appears to have switched away from retailers to the healthcare sector, where the lucrative bounty of personally identifiable information is available.

What I wanted to understand was that two years on from the retail security breaches, why did they suddenly stop? Is it the case that us in the media are simply bored of writing about these types of incidents, or have the retail security teams addressed the situation better and made major improvements to their security in the wake of what happened in 2014?

Jodie Sikkel, network infrastructure and security specialist at ANSecurity, said the main

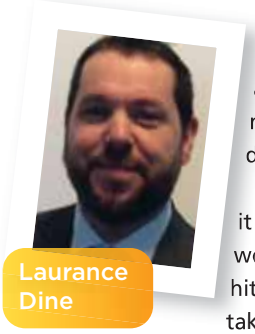
learning point is that compliance does not equal security, and "security is a process that requires planning, education, adaptive technology and regular health checks."

"As a result of these breaches and in order to prevent further breaches, retailers are choosing to work with security specialists and subject experts to design adaptive security solutions to protect against external threats and data loss as well as tick all the obligatory regulatory and compliance boxes," Sikkel said.

One such managed security service provider that I spoke to was Laurance Dine, managing principal for the Verizon Investigative Response Unit – a division of the Verizon RISK Team. In his role he spends time investigating breaches when they happen and doing everything associated with the investigation.

Asked why he thought the stories stopped, he said: "Overall, things have improved in what we are seeing on the investigations side and putting systems in place, and so systems such as Point of Sale (POS) are not online. With the size of the breaches that we saw, it does make you think and based on our research and debugging, I do think it is better."

Dine's team provide a healthcheck to retail security teams to get an idea of weaknesses and he said that while there was not a drop in retailers asking for assistance, things are moving in the right direction.


Laurance Dine

"It is improved, but it doesn't mean you won't be next on the hitlist," he said. "It takes proper defense. It is a continuous thing, and you cannot assume hackers have gone away."

One lesson to be learned in particular from the Target breach, where access was gained and malware uploaded to POS systems between 15 November and 28 November (Thanksgiving and the day before Black Friday) after network credentials were stolen from a third party refrigeration, heating and air conditioning subcontractor, is that better segmentation was now being adopted.

Dine said he is seeing more of this and his team advises clients regularly on creating segmented environments. "If something were to happen, the best thing is to have good protection, so if an attacker gets in they do not get everything you have."

Ben Johnson, co-founder and chief security strategist of Carbon Black, said that the "massive breaches" woke the retail industry up, but a combination of segmented networks and efficient change management has improved the sector.

Investigation

Speaking to CNBC whilst he was still Chairman and CEO of Target, Gregg Steinhafel said that "day one" of the investigation was 15 December 2013, and within hours it had managed to secure its environment. "We eliminated the malware in the access point, we were very confident that coming into Monday guests could come to Target and shop with confidence and no risk," Steinhafel told CNBC.

One of the investigators was the United States Secret Service, and former Special Agent Steven Bullitt, now vice-president of cyber forensics and investigations at security services provider Solutionary (an NTT Group Security Company) told me that as well as setting up the National Computer Forensics Unit in Alabama to train thousands of police officers in computer forensics and network intrusion investigations, he was involved in investigations into big data breaches.


Steven Bullitt

He explained that in cases where the FBI is called, they don't go in concurrently, but often there was better intelligence at the Secret Service so the two departments work together. He said that working as an investigator in retail security breaches, a common finding was with the vulnerabilities that were similar across sectors.

"A lot of the time you may be an opportunity or a target of choice, as there are so many ways to get into a system now, and

> It is difficult to look at this as an industry and say that the standard for the retail security needs to be set
>
> Brian Engle

companies nowadays want connectivity and to be on all of the time. People also want productivity and want customization like BYOD and virtualization, and then on top of that is the Internet of Things, so the standard perimeter for protecting a company has widened now, so with all those things we have convenience but it doesn't align with security as well. So businesses are forced to move with the environment that security is not aligned with," he said.

In regard to breaches, Bullitt was reluctant to go into specific detail as some cases are still ongoing, but he said that as well as the big breaches, there are literally thousands of "small ma and pa stores that you don't hear about."

He said that the common vulnerability between larger retailers and smaller stores is that they all take credit card payments. "You do not hear about those small stores and chains and we have seen that if you have a person who owns five or six small franchise companies, they put in an integrator to put in a phone system and they put in remote access to fix these vulnerabilities."

"So when he puts that in they set a backdoor to the system so the attacker scans the system, they can see the opening and administrator passwords are used to get into the system. I see this all of the time. I say if you have remote access it has to be on demand, meaning that the owner has to initiate it and have strong authentication or a VPN for it. There have to be some security steps involved as it is convenient, but if you can log into your

environment from any place at any time, from any device, so can your adversary."

Aftermath

After the breaches happened, the industry sought a way to make sure it didn't happen again. One way to improve payment security will be with the deployment of EMV/Chip and PIN systems, and Bullitt believed that this will create a more secure and brighter future, as that and the introduction of mobile payments "make it more difficult for those miscreants to monetize the credit card industry, which is a commodity in the black market."

He pointed to the years since 2014, where breaches have been more about personally identifiable information and healthcare data. "I tell people, when you hear about the breaches don't think about those credit monitoring services for six months; if you are breached then you are breached for life."

In a statement to the Consumer Financial Protection Bureau in October 2014, President Barack Obama mentioned the retailers pledging to adopt Chip and PIN technology by the beginning of 2015, and named American Express in its pledge of $10 million to replace outdated card readers at small businesses. I have used the Chip and signature in some US retailers such as CVS and Walgreens, but to date the Chip and PIN system seems absent.

That's not to say that a better payment system would have saved the blushes of the retailers in the headlines though. One thing that did get instituted is the attention of the boards, and Mark Weir, director of major accounts UK and Ireland at Fortinet, confirmed this, saying that he was seeing "an awakening in the sector" at a board level.

He said: "Mapped with customer-level applications and big data, there is an understanding that firms need to work hard to protect their ever-expanding pool of data. In our experience, retail is a really exciting, vibrant and fast-moving sector, transforming itself at lightning speed to react to the steep increase in threats over the past two to three years."

Ben Johnson said that there is a "huge focus on security" within boards, not just in the spending of money, but in the cultural buy-in and getting people on board with new technologies. "There is definitely more spend, more about being smarter with the money and focusing on technology, and general infrastructure and being smart with who you hire. There is a huge focus, and every board meeting that we see has a 45-minute section on cybersecurity and risk as it is such a big issue."

The Cost

It was reported by CSO Online in early 2016 that Home Depot had agreed to pay as much as $19.5 million to remedy its data breach, which included around 56 million payment cards, as well as 53 million email addresses. This included a reported $13 million to reimburse customers for their losses, and $6.5 million to provide them with one and a half years of identity protection services.

The company admitted that it was working to put the litigation behind it, and that while customers "were not responsible for fraudulent charges", they have "been our primary focus throughout", a spokesperson said.

Johnson said that as well as the $10 million paid by Target, this is making boards focus on the risk of security, and many are making progress as the board understands the current risk to the brand. Asked what has changed in the attitudes towards security, he said it is a combination of brand risk, regulatory and national and local government pressure, and the customer's trust.

He said: "If you can create a notion of trust with users, you should have adequate if not solid controls in place to mitigate risks."

Retail is an exciting, vibrant and fast-moving sector, transforming itself at lightning speed to react to the steep increase in threats

Sharing Intelligence

The fear that was struck into retail security led to movements to make sure it did not happen again by the retailers and I guess that by the lack of more breaches in the headlines, that has been a success. One reason for this was the establishment of a cyber information sharing center (CISC), which it describes as "another tool in retailers' arsenal against cyber-criminals by sharing leading practices and threat intelligence in a safe and secure way."

The R-CISC was launched in 2014 as a combination of 30 retailers with retail trade associations and by June, retailers were sharing threat intelligence among themselves with analyst support and with feeds from the NCCIC, FBI and other government sources. Later that year, Brian Engle was appointed as executive director, coming from a CISO background in his native Texas.

The R-CISC counted a membership of over 400 organizations at our time of meeting in March, and I wanted to know what Engle thought had improved the sector and what improvements have been made?

He said that as a very spread out and diverse sector containing thousands of retailers including everything from the local dry cleaners to the largest names, R-CISC is working by creating small groups of organizations into collectives, and he said that this has created "leaps and bounds in improvements in those organizations", as they work together to improve capabilities.

Engle said that the beauty of working in a shared environment is that you can see the infiltration and once that happens, you can see how advanced and complex that is. "The threat may have been there and it was not what they used to get in as that is being shared and re-used and built upon across the hacker community," he said.


Brian Engle

So what are the levels of security within retailers? Engle said that in some of the more capable and advanced organizations, they are building up their capabilities at an advanced rate, and have personnel dedicated full time to assessing what is happening but also pursuing detection – both internally and externally to their environments.

"That ranges down to organizations who are reliant on high degrees of outsourcing and have a small IT show and are a pure e-commerce platform and have developers and a router guy, and that is why it is difficult to look at this as an industry and say that the standard for the retail security needs to be set, and it does, but the bar cannot be one bar as that is stifling nature," he said.

"The effect that has on organizations operating on a 3% margin in a grocery store – telling them to build a financial services capable security model – the costs would outdo any level of capability."

Engle admitted that it is a complex problem and when it sees incidents occur it is easy to think of straightforward ways to solve it, but he said that there is always a deeper story and for the most part, most are not ignoring it.

"One thing I would say is no one gets to build the security program from ground zero, and no one plays the Chess game with all of the pieces on the board, and often you are playing 12 games at once and one of them is the king and the pawn and you're just trying to avoid them!"

Of course as in any vertical, there are variants of companies in terms of size and capability, and I wanted to know if R-CISC was engaging with as many online retailers as traditional high street retailers? He said that actually, it is seeing retailers reinventing themselves but overall, security controls take time to implement.

So with fewer headlines in 2015 and 2016, are companies more prepared after the event? Engle said he thought it was largely yet to be seen, but the response is now there to react at a much better rate.

"Take the warning indicator, plus the types of things to detect, the sharing of information beyond cybersecurity indicators into the fraud space; this all helps to create cross-effecting factors. Think of the breach of the card data and the use of the cards, the impact upon another retailer and we are really reaching into a place where a degree of information sharing is the flag, and detecting that type of theft of a card at a faster rate," he said.

"We can get to that place where all of those converging factors make POS malware only able to affect the smallest retailers with the lowest transaction rates. I think we will see the types of attack vectors shared effectively and quickly so that the types of things in the damage realm can be affected and removed."

"There are so many tools available in the e-commerce realm to help step up authentication and help prevent the fraud; you don't have to have the perfect wall to the credit card safe, you can have all of these other things for detection. Also, having the R-CISC as the clearing house for information that can be shared across the whole sector of retail, and broadly any consumer goods across the eco-system, really positions the retailer to be more proactive and not just chase the liability at the end of the event."

Engle followed the model of other ISACs in saying that cyber-criminals are sharing information and specializing in areas across aspects of breaking into systems or exfiltrating data and moving it around quickly, and of course monetizing it. So if R-CISC can replicate this, then maybe the future for retail security does not look particularly bleak.

Two years on from writing a string of headlines about retail security breaches, it is reassuring to see that major advancements were made so quickly to try and resolve what was turning into a major problem. The case of customer trust is now a board matter, and they have realized that having a brand associated with poor security has a major impact upon the entire business.

It may be that retailers just improved their efforts and the problems stopped. With the European General Data Protection Regulation proposing mandatory data breach notification, maybe we will see a resurgence of bad news in the future. For the moment, retail security had its *annus horribilis* and while the cases are being settled and the instances not forgotten, maybe retail security really did take a great leap forward.

Mister Retail Security

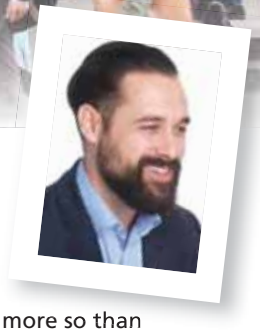
Having held down a number of senior security positions at major retailers, **Lee Barney** is well placed to talk about the challenges faced in his sector. Dan Raywood talked to him about how M&S deals with the modern threat landscape

Since the retail security breaches of 2014, the retail security sector has received much more interest in how it is handling its security, and its people, process and technologies. Sitting in the central London office of UK high street powerhouse M&S, head of information security Lee Barney talked to me about the changes he has overseen since he took the job in 2015.

With a background in retail and senior level security management, Barney now manages a team of 40 people based across two locations. Following a recent recruitment drive, he acknowledged that almost every retailer he had worked at "compares itself to retailers internationally".

He said: "I've spent a lot of time in retail and I like it, which is strange, as it is the hardest place to do security properly! You really need to sell your changes before you can make them, as there is no automatic buy-in to security."

"It doesn't matter where you are, as retail businesses have been around for a long time – M&S has been around since 1884 – and in that time we have seen two World Wars, seen the Cuban Missile Crisis, seen terrorism begin and expand to its current form, we've seen so much and been part of a choppy global dynamic and we've seen the business expand into global territories. We've seen risks and although people say they are potential problems, the business has seen them off and it is still here."



Barney admitted that security is "taken incredibly seriously here", and more so than he had seen anywhere else he had worked, mainly as the brand is of upmost importance and if anything impacts the brand, it will get everyone's attention.

As the Target breach impacted the company's technology, I wanted to get an understanding of how Barney saw the state of security technology in retail. He said he was less concerned about the security technology that we have and more about the people, specifically in the way that M&S works.

The problem, according to him, is that credit card processing technology is 40 years old, and it is attacked frequently, and attacks are seen on infrastructure to get access to credit card data.

"Target was a real game changer for cybersecurity. It was the 'eureka moment' when senior executives realized the business case for investing in cybersecurity. The return on investment became more obvious to retailers – avoiding litigation fees and fines."

Looking at the 2013 Target attack, I wanted to know how much this shook up the typical retail CISO. Barney said that it did impact everyone and not just UK, US or European retailers, as the attacks are not that sophisticated, but a good CISO will see anomalies as there was historic equipment in place and they were not up-to-date in regards to thinking about security and investments.

So is there a problem across retail security that old technology is still there and being used? "Old technology is in every business, and if anybody tells you otherwise they may want to take another look," he said.

"We use mainframe systems as every business does, but the main thing that M&S are good at is taking big and bold decisions to use new technology, and that is why we accept Apple Pay, and were one of the first to do it. That can cause you problems as if you are on the vanguard of change, you don't know what is there to trip you up and it is very easy for those businesses behind you to step over you."

"The thing is that security is not that hard, there is a baseline of things but it is not hard to get the basics right and more often than not, attackers are looking for the basics to be wrong." Barney said he had made steps to improve the security resiliency within the company and in particular hiring ambitious experts who find new solutions to problems. He said he has introduced a gamification concept into the daily work, especially regarding his ethos of detection and response.

"We have a blue team, or cyber operations team, and they look for changes against the baseline and look at all the systems and all of the network and web platforms. If the number of attacks goes up then it tells us that we are detecting it, but it if goes down when we don't expect it, it may be that an attack has been successful and is no longer being picked up."

I'd rather have good people across the country, than have the greatest technology that we spend a fortune on that will eventually go out of date

"To make them do that, we have a red team and we pit them against the blue team and 50% of their day job is to sit outside the perimeter and attack their way back in. Every time they achieve a hack, they get points. Based on competence and capability, they get a number and at the end of every week those numbers are added up and the highest scorer gets a day off. The blue team can try and capture their points and if they win, they earn the day off."

Barney said his team enjoys working in this type of environment. "It is a career progression from the blue to the red team as they shift focus to detection from prevention, and we do 'promote' people."

The team of 40 in Barney's department combine a range of ages, and he said that the opportunity with the younger staff is to make use of people who know about technology, which often comes naturally to them. However, while they may know Windows or iOS, the new generation has been built up with so many expectations on what work life actually is, and Barney said that it doesn't manifest itself in reality. "You bring them down to reality gently and the reason we do all these things is for this purpose, you have to come to work," he said.

"One of my great passions is getting security to be more recognized and diverse, as it is considered to be a subsection of IT and I do see a problem with not enough women in cybersecurity. Simply put, 50% of the population is female, so why are 50% of the cyber team not female?"

"M&S is very diverse and has a very good gender balance, but 30% of my team is female and I want to make that better. I look for female candidates and compare them to male candidates, and hire them as appropriate for the job, but I need to see more women coming forward and going into the industry."

Barney said that it is about getting someone who is right for the role, particularly as he is doing something with detect and respond that is not commonplace, and you cannot lift those skills off the shelf, so time is spent training analysts to make sure that they do have those skills.

As one of three ex-army men in his department, Barney said he does see CVs from people with a military background, but as there are so few people in the military who do a typical security day job due to outsourcing, he believed that the true cyber offensive capabilities do not exist yet, and those who do get full time jobs end up working in government departments.

Barney added that he wants to track the best candidates, but often it is about realizing that a career in cybersecurity is an option, and until then, we are missing out on those candidates who would make great employees.

"I'd rather have good people across the country, than have the greatest technology that we spend a fortune on that will eventually go out of date," he said. "People don't go out of date if you invest in them. Technology has its place, but the people who filter it are human beings at the end of the day. Until we have artificial intelligence, people are our greatest asset."

Mobile Payments, How Secure?

As you can now pay for your purchases with a mobile device, **Robin Arnfield** looks at the mobile payment space and identifies its opportunities and how secure it really is

Mobile payments have taken off, with Apple Pay and contactless cards now widely accepted, but how can retailers be sure these payments are secure and can't be counterfeited or intercepted?

According to Ovum, proximity m-payment users will rise from 44.55 million worldwide in 2014 to 1.09 billion in 2019, of whom 939.1 million will use near field communication (NFC). The total value of proximity m-payments worldwide (both NFC and non-NFC such as QR codes) will grow from $4.77 billion in 2014 to $141.21 billion in 2019, the analyst firm says.

"Factors driving growth include wider merchant support for NFC across POS acceptance infrastructure, which in the US is being helped by upgrades to EMV," Eden Zoller, Ovum's principal analyst, consumer services and payments, says. "NFC is being championed more widely across the ecosystem by players such as Apple, Google, PayPal and Samsung."

Apple Pay, Android Pay and Samsung Pay support NFC. During 2016, PayPal will offer NFC payments for its new in-store Android m-payments app, which currently supports QR code payments.

Ovum says proximity m-payments traction has been low across the vast majority of mature markets. One reason is consumer concerns about m-payments security. GfK's FutureBuy 2015 consumer survey found that 52% of US respondents worry about their personal information when using m-payment apps. Only 16% believe that m-payments are more secure than other payment methods, and 20% are confident that m-payments are 100% secure.

Many consumers have yet to see m-payments' advantage over other payment methods. "M-payments' real value has yet to become reality: the ability to combine payments, loyalty rewards and targeted offers on smartphones using a frictionless m-wallet interface," Alan Goode, managing director of Goode Intelligence, says.

Attitudes Toward M-Payments

"Worried about personal information … "
Total 52%, Gen Z 55%, Gen Y60%, Gen X 54%, Boomers 51%
"Confident that... payments are 100% secure "
Total 20%, Gen Z 33%, Gen 36%, Gen X 24%, Boomers 10%
"More secure than other methods... "
Total 16%, Gen Z 31%, Gen 28%, Gen X 18%, Boomers 6%

Source: GfK's FutureBuy 2015 U.S. consumer survey

An August 2015 survey of 900 cybersecurity experts for ISACA's 2015 Mobile Payment Security Study found that 47% of respondents believe m-payments are insecure due to vulnerabilities such as using public WiFi, lost/stolen devices, phishing/shmishing, and weak passwords.

Survey respondents said the most effective way to protect m-payments involves using two methods to authenticate users' identity (66%), followed by requiring short-term authentication codes (18%). Only 9% recommended requiring consumers to install smartphone-based security apps.

EMV in the USA

To improve card security through merchant adoption of EMV-based card readers, US card networks set October 2015 as the deadline after which liability for in-store fraud involving EMV cards shifted to whichever party isn't EMV-compliant.

"Over 750,000 merchant locations have enabled EMV, representing 17% of total US face-to-face locations," Charles Scharf, Visa Inc.'s CEO, said in January 2016. "We expect 50% of locations to be enabled by the end of 2016."

The majority of EMV card readers installed in the US are contactless card/NFC-enabled, while smartphone manufacturers are increasingly equipping their handsets with NFC and security features such as fingerprint authentication.

Analysts think EMV will spur m-payment adoption. "EMV will drive innovation in the US payments market," says Avivah Litan, a vice-president/distinguished analyst at Gartner. "The way US chip cards work currently, they slow down the checkout process, and consumers and merchants don't like this. EMV will prompt people to use m-payments and contactless cards as they are much faster than contact-based EMV cards."

Card On-Boarding

"Apple Pay and Android Pay have introduced great security features for POS terminals," says Litan. "Merchants just have to pass on the customer identification to their acquirer. The loophole with these third-party services is card on-boarding into m-wallets, especially with the recent data breaches. If criminals load stolen card numbers into secure wallets, this is a major problem."

"Account takeover and stolen cards are the biggest issues," agrees John Dukellis, head of Next Gen Wallet at PayPal. "But PayPal has strong risk controls for fraudulent activities, and has policies such as Buyer Protection in place to protect consumers from fraud."

"Several US banks told me in 2015 that, as they had security gaps for wallet on-boarding, they saw 600 basis points of fraud from Apple Pay on-boarding of stolen card numbers bought online," says Julie Conroy, research director at US-based Aite Group. "While there have been evolutions to the Apple Pay registration process which have helped, it's still a major susceptibility."

Litan says the solution lies in reducing reliance on potentially comprised static data such as personally identifiable information (PII) and increasing reliance on dynamic data including reputation and behavior as well as metadata such as device ID and phone number.

Recommendations

"M-payment security mustn't be harder than existing security measures," says Chester Wisniewski, Sophos' senior security advisor. "If it adds friction, people will be deterred."

Wisniewski recommends proximity m-payment schemes use two-factor authentication and tokenization. "Apple Pay uses Touch ID to authenticate its users as two-factor security," he says. "Also, Apple Pay tokenizes a user's card number so it's never seen by merchants, and generates a one-time security code for each transaction."

> There's no reason to think wearables won't play a crucial part in securing payments
>
> Alan Goode

"PayPal has always used tokenization, so we never share users' credentials with merchants," says Dukellis.

"Multiple security technologies are needed for truly secure proximity and remote m-payments, including behavioral and digital identity analytics," says Conroy. "With remote wallets, you must protect log-in credentials, as there's great opportunity for compromise due to database breaches."

The European Banking Authority's draft m-payment security recommendations, published in December 2013, recommend two-factor authentication involving two or more of the following: something only the user knows (e.g. static passwords or PINs); something only the user possesses (e.g. smart cards or mobile devices); and something the user is (e.g. biometric characteristics).

In October 2015, the European Parliament adopted the Directive on Payment Services (PSD2) which requires payment services providers to use "strong customer authentication" based on the EBA's concept of two-factor authentication, where each factor is independent of the other so they can't be compromised by each other.

"We've all seen the statistics about mobile malware and the innovative ways criminals use to get to their targets," says independent IT security advisor Neira Jones. "Unfortunately, basic security principles are rarely followed in favor of quick time to market (for apps), but times are changing, and regulations such as PSD2 will force the ecosystem to get serious about security, particularly in the area of mobile and APIs."

Kevin Foster, testing services manager at MTI Technology, says cyber-criminals can target smartphones via NFC. "They can transmit small payloads of data between an NFC device and smartphone to exploit zero-day vulnerabilities in the mobile OS and other installed apps," he says. "When successful, this can enable the attacker to gain full rights and access to all data on the device, as well as the ability to install exploit frameworks and send mobile data to a remote listener host."

"From the very start of its lifecycle, a mobile payment app needs to be designed and developed securely and subject to penetration testing," says Foster. "Any web server applications that the app communicates with, via web services, should have penetration tests and code reviews conducted on them throughout the development lifecycle. For example, any data cached or stored on the device should be securely encrypted."

HCE or Secure Element

M-wallet users' card credentials can be stored on a secure element within an NFC-enabled smartphone, or in an issuer-managed database in the cloud using HCE software. However, HCE only works on smartphones running Android 4.4 operating system (KitKat) and above as well as on the mobile version of Windows 10. This means that if a card issuer wants to offer proximity m-payments to its cardholders on Apple devices, it has to partner with Apple Pay.

"HCE gives more flexibility to banks, as, before its introduction, they depended on hardware-based solutions controlled by handset manufacturers and network operators, and had to rely on secure elements," says Jones.

According to Jupiter Research, in 2015 50 banks around the world had commercial HCE deployments. In September 2015, RBC Royal Bank of Canada became the first

North American bank to launch an HCE-based wallet.

"Secure elements win due to the fact that they're geographically distributed rather than centralized," says Wisniewski. "If your card is stored on your bank's internet-accessible server, there's more incentive for criminals to hack the bank than your phone."

RBC has opted for the cloud. "Our m-payments are powered by RBC Secure Cloud, which keeps customer data secure in the cloud, not on the phone, making a safer, faster, more flexible solution," says Linda Mantia, RBC's executive vice-president of digital, payments and cards. "Secure Cloud uses tokenization, and works with multiple mobile devices and platforms and with existing contactless-enabled POS terminals."

Biometrics

Goode says biometrics is the most convenient way to authenticate proximity m-payments users without lengthening transaction times. "Biometrics' potential is being fulfilled with Apple Pay and Samsung Pay's success, in addition to what we'll see in 2016 when issuing banks, payment scheme providers and alternative payment providers bring out biometrics-based user authentication and transaction verification solutions," he says.

"It's a good idea to have two-tier verification in m-payments involving passwords and biometrics," says Joseph Walent, senior analyst, Emerging Technologies Advisory Service at US-based Mercator Advisory Group. "People say we should eliminate passwords to speed up transactions, but retaining passwords that are changed regularly to guard against biometric spoofing provides greater security for higher-value transactions."

M-payment schemes will also be able to authenticate users' phones. "They will check where this data is being sent from; where has the user's phone been recently, and does that fit the pattern the user normally has; is this transaction ordinary or regular for the user?" Walent says. "The technology isn't there yet for this deeper level of authentication, but this is the direction we're going in."

"As smartwatches and wristbands become more ubiquitous, there's no reason to think wearables won't play a crucial part in securing payments," says Goode. "This can either be as stand-alone payment devices, using a smartwatch to make a contactless payment, or in parallel to smartphone-initiated payments, providing a second factor. Biometrics (e.g. heartbeats) will play an important part here."

Mobile Point of Sale (mPOS)

mPOS card readers attaching to merchant-owned smartphones or tablets are popular with smaller businesses. The global number of mPOS units rose by 64% to six million in 2015, US consultancy IHL Group estimates.

"mPOS readers' vulnerability is using the audio jack to connect to the merchant's phone," says Wisniewski. "Card numbers are converted into audio signals, which anyone can record on their phone and stage a replay attack. A more secure way to connect mPOS readers to smartphones is through Bluetooth, provided Bluetooth is implemented correctly."

"While not mandatory from an industry governance standpoint, reputable POS hardware manufacturers require mPOS solution providers to use the manufacturer's proprietary point-to-point encryption (P2PE) system if they lack their own," says Karen Cox, VP, payments and retail solutions at North American processor Moneris. "Solution providers must ensure merchants and consumers are protected in cases where cardholder data passes through insecure smartphones or unencrypted tablets."

mPOS solutions using magnetic-stripe-only card readers are vulnerable to counterfeit card fraud, as they don't offer the additional security of chip-authenticated cards. "This leaves merchants at risk of chargebacks," says Cox. "There are mPOS solutions that connect portable PINpads to smartphones or tablets and enable EMV chip-and-PIN technology to protect against counterfeit card fraud, as the embedded chip is nearly impossible to clone."

"We encrypt transactions at the point-of-swipe and tokenize data once it reaches our servers," mPOS provider Square says. "Also, we use our algorithms to spot and freeze malicious or suspicious activity."

"Square says its transactions are encrypted, but it doesn't meet my standards," says Wisniewski. "It also says it will take liability if something goes wrong, but this is Square's way of saying it isn't secure."

Standards

Currently, there are no standards for payments acceptance by merchants' mPOS devices, although EMV specifications body EMVCo and the PCI Security Standards Council (PCI SSC) have issued mPOS security recommendations.

For example, P2PE technology should be used to encrypt card data at the point of entry into PCI PIN Transaction Security (PCI PTS) certified devices all the way to the processor.

"As m-payments acceptance is still evolving, it's premature for new PCI standards," says a PCI SSC spokesperson. "The Council has a dedicated mobile taskforce that works with other standards bodies, vendors, banks and processors to promote the development of secure devices by providing guidance on what's needed."

Existing PCI compliance standards for merchants accepting traditional POS payments apply to mPOS and to m-wallet payments.

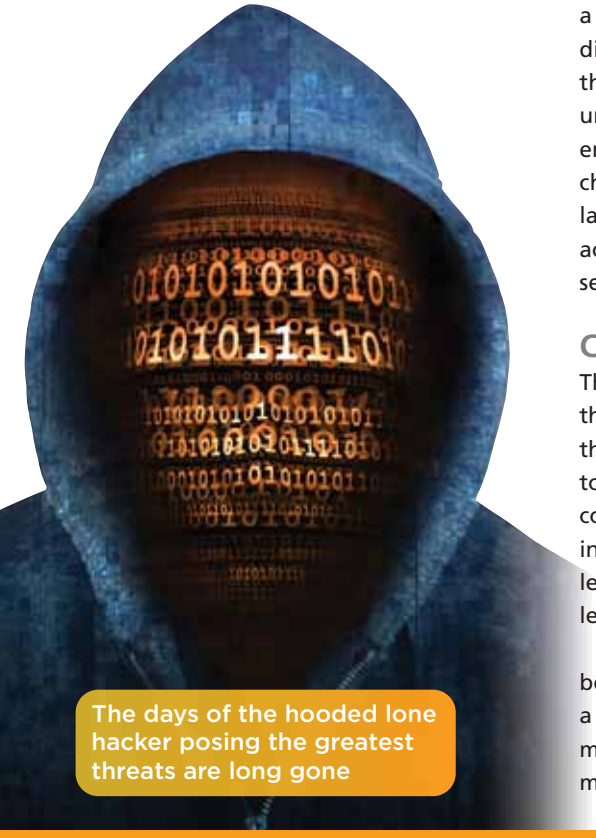
"Any business accepting payments via POS or mPOS solutions must adhere to the PCI Data Security Standard (PCI DSS)," Cox says. "Businesses must also use approved PCI PTS-compliant devices. Any POS solution should meet the requirements for the Payment Application Data Security Standard (PA-DSS), which has been updated to include mobile payments specifications."

EMVCo requires mobile handset vendors supporting m-wallets to meet its EMV Level 1 terminal type approval requirements for contactless payments so that their handsets comply with EMVCo contactless card specifications (e.g. Visa PayWave and MasterCard PayPass). EMV Level 1 is a specification for the hardware interface enabling data transfer between EMV-compliant cards and terminals.

The Cybercrime Corporation

Rick Orloff, CSO at endpoint data recovery specialist Code42 looks at the professional nature of online crime in 2016, and what is being done to battle it

With estimates that hackers who steal just 50 credit card numbers can make up to $1 million, there is little doubt that cybercrime pays. However, cybercrime is not just big business when it comes to revenue lines. Over the last five years we have seen this underground economy reshape itself into a sophisticated enterprise, adopting the same hierarchy, sales models and marketing practices as legal businesses.



The days of the hooded lone hacker posing the greatest threats are long gone

A peek behind the scenes of this black market is like holding up a mirror to the practices of legitimate businesses. The core exception is that, free of the regulation and reporting that encumber legal organizations, cyber-criminals are free to innovate faster. This enables them to remain a step ahead of our defenses, making it difficult to catch the perpetrators or crash the market. However, it is only by understanding how these criminal enterprises operate that we can hope to challenge them through a combination of law enforcement, technical defenses, pro-active intervention (human behavior), and secure operational business models.

Cybercrime Inc.

The days of the hooded lone hacker posing the greatest threats are long gone. While the lone hackers still make a huge impact, today's cyber-criminals operate with corporate structures and are more likely to include C-suite of Armani-clad entrepreneurs leading hierarchies of middle managers, low-level employees and contractors.

In fact, a large organized workforce can be employed to manage the many layers of a cyber-attack, from coding and distributing malware to identifying infection points and managing comprised endpoints or accounts. Further, specialists will be leveraged to mine through data hackers acquire, assessing how it can be monetized.

An in-depth Google report into the underground economy found that the cybercrime industry boasts a thriving freelance model where specialists offer 'crime-as-a-service'. Examples include exploit writers who discover vulnerabilities and create exploit packs, malware testers who validate software, bot herders who lease and infect zombie computers and tool providers who spread spam and malware. At the bottom of the pile are the money mules who—sometimes unwittingly—transfer illegal money into legitimate accounts.

More traditional business roles are also flourishing in this black market. There are specialist recruiters who source the subject matter experts required by cybercrime entrepreneurs. There is also a strong market for content creators who develop spam emails, blogs and phishing sites, ensuring that these look legitimate in any language.

It is also worth noting that, as with any industry, competition is rife and merger and acquisitions are common. In 2010, it was reported that two competing malware giants, Zeus and SpyEye, merged. The well-known banking Trojans continued to operate until summer 2015, when Europol

took down the Ukrainian syndicate suspected of operating them.

Marketing and Sales Channels

Cyber-criminals are making use of the same tools as legitimate businesses when it comes to marketing and selling their wares. According to a RAND report into the cybercrime market, increasingly sophisticated e-commerce stores are launching supported by email marketing campaigns. However, these sites are invite-only and communication is hidden underground on anonymous networks like Tor and Freenet. The laws of supply and demand also rule on the black market according to further insight from Google.

With an increasing supply of goods for sale—be it credit card numbers, personal health information or employee data—sellers have to stand out. Some offer money-back guarantees that their malware will go undetected for months or offer refunds if a stolen credit card gets cancelled, and while "bad sellers" may be able to hide from law enforcement, they cannot hide from their customers: they are often shamed on black market trading forums.

Research and Development

Innovation is at the core of the cybercrime enterprise. Competition and commercial gain drives organizations to invest in research and development at a number of levels. Firstly, as the number of connected devices, cloud services and social platforms increases, the black market is determined to keep pace. Each of these consumer and business solutions offers new entry points for cyber-criminals to access and exploit data.

However, beyond finding new access points, these businesses are also constantly developing and testing new scams, from compromising office devices like printers, to setting up domain names similar to those of known brands to peddle counterfeit goods. Finally, the most sophisticated, headline-grabbing attacks require intense investment in both attack vectors and social engineering techniques to be successful.

> More traditional business roles are also flourishing in this black market
>
> Rick Orloff

Financial Trading Systems

Any commerce relies on a currency system. The introduction of virtual currencies like Bitcoin, for all the advances it has brought to fintech, also made it easy for cyber-criminals to remain hidden from law enforcement. Commerce like Bitcoin make traditional investigative approaches e.g. 'follow-the money', very difficult. Before it was shut down by the U.S. Treasury Department in 2013, the Liberty Reserve digital currency service was used by one million people worldwide to launder about $6 billion over seven years. Digital payment services such as PayPal and Alibaba are also exploited by hackers to transfer funds.

Tackling the Cybercrime Enterprise

Given the sophistication of today's cybercrime enterprise, there is no simple solution to preventing attacks and protecting businesses and consumers. However, we have seen progress on a number of fronts.

Some businesses have started to take a proactive approach to monitoring black market developments. For example, Twitter has been known to track and disable fake accounts, preventing cyber-criminals from selling them to spammers. Google has taken a more economic approach, looking to increase the price of Zombie accounts used for launching attacks to make them less attractive to spammers.

Regulators are also taking action with initiatives designed to improve the way businesses store and protect sensitive data, such as Privacy Shield and the EU General Data Protection Regulation, making it more difficult for cyber-criminals to access and exploit digital information.

It is also safe to say that, in the wake of a number of high-profile attacks, the financial and reputational impact of cybercrime is now understood. In fact, our recent Datastrophe study found that over a third of workers believe the company they work for may be at risk of a data breach in the next year.

With security becoming a board level issue, businesses are starting to invest in multi-layered solutions. With an influx of mobile devices such as smartphones and wearables entering the workplace, businesses can no longer afford to rely on perimeter protection alone. This must be supplemented by an endpoint data solution to protect and backup data wherever it resides.

The best solutions on the market today can track data movement across devices, enabling unusual activity to be detected. The backup and real-time recovery element allows businesses to recover lost data to any point in time, and get a new device up and running in a matter of minutes if required.

Additionally, when it comes to tackling cybercrime, we are held back by the fact that businesses are reluctant to share details of attacks. This is in direct contrast to cybercrime corporations where 'crime-as-a-service' contractors have a market-wide view of the types of attacks that are generating results. By encouraging real time sharing of experiences and intelligence, businesses and governments can work together with a view to collectively staying ahead of the cyber-criminals. Doing so would drastically impact the effectiveness of organized cyber-attacks.

While it is true that none of the measures we have outlined above will bring down the black market alone, taken together they can help us fight back against sophisticated cybercrime enterprises. It is only by bringing together 'protect' and 'prevent' measures across policy making, law enforcement and smart technology solutions that we can start to tackle the cybercrime industry.

Would like to meet

With more and more data being handled by dating websites, **Patchen Barss** looks at the security challenges facing the industry

San Francisco resident Chris Orris uses an electronic dating service called 'Coffee Meets Bagel' (CMB). The site, which draws on users' Facebook information to recommend potential mates, enjoys a positive reputation. In 2014, CMB made Time Magazine's top ten list of apps for people who want to fall in love.

"Last year I was matched with two different women at about the same time," he says. "With one, we never clicked so we didn't meet up. The other, we went on one date, didn't click, and stopped talking."

That should have been the end of the story, but a few months later, Orris got a disquieting surprise.

"I was on LinkedIn, and the "people you may know" section showed *both* of these women, along with their first and last names and everything else you'd find in their LinkedIn profiles," he said. "I never had their last names before."

He acknowledges that he had entered their telephone numbers in his phone, and theorizes that this action might have been the bridge between the two sites, but he doesn't know for sure. Regardless of how the data spread, he wasn't comfortable with the result.

"I had maintained a respectable level of anonymity, and LinkedIn (presumably through my Android phone) blew that away, offering me much more information on those ladies than they had shared," he said. "I assume the same happened in the other direction."

Privacy issues related to online dating exploded into the public consciousness in the summer of 2015 when a group of hackers calling itself "The Impact Team" stole and published user data from Ashley Madison, a website designed to help people arrange illicit affairs. Not only did this data breach reveal a great disparity between the site's promises about privacy and users' actual risk of public exposure, it also brought to light other confidence-shaking issues.

"Ashley Madison's army of fembots appears to have been a sophisticated, deliberate, and lucrative fraud," wrote Annalee Newitz, editor-in-chief of *Gizmodo*. "Whatever the total number of real, active female Ashley Madison users is, the company was clearly on a desperate quest to design legions of fake women to interact with the men on the site."

With personal information leaking so easily out of dating websites, and with tech magazines forced to run articles with headlines like, "How to find out if you are dating a robot," there are good reasons for users to be cautious about their privacy when looking for a mate online.

Dashlane, a company that offers password manager and digital wallet products, conducts industry surveys that rate basic website security features. Their latest data from the second quarter of 2014 puts dating sites at the bottom of the barrel.

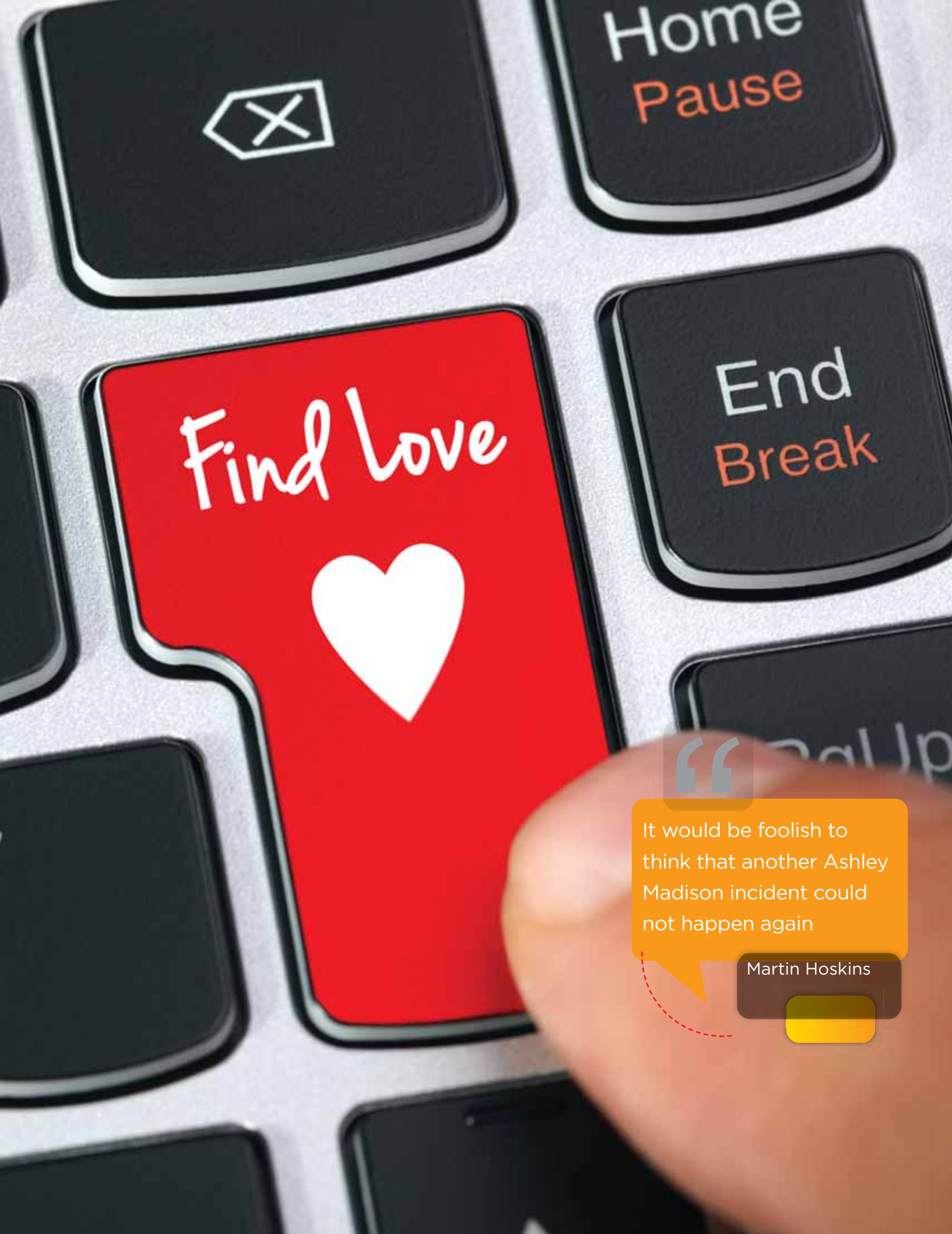
Dashlane assigns numeric values to factors such as whether a site requires alphanumeric passwords, whether it locks accounts after multiple incorrect login attempts, and so on. They consider a score over 50 as the base for an adequate password policy. On average, dating sites had a score of -23.

Despite the sector's dismal showing, analysts recommend users don't simply resign themselves to giving up any hope of privacy and security when they date online.

"Users are much more aware and informed about data protection and privacy these days," says Paul Henry, IT security consultant for Blancco Technology Group. "They're becoming more skeptical and asking more questions to make sure their privacy is protected. I hope this continues to happen."

While the Ashley Madison breach has prompted some sites to seek ways to improve their security, Henry says that users who value their privacy should rely on their own initiative, not that of the sites they're using.

"Security is not the service that is being sold on these websites," he says. "They are often more concerned with collecting, storing and using data to provide real-time matches and to help personalize their marketing efforts."



> It would be foolish to think that another Ashley Madison incident could not happen again
>
> Martin Hoskins

A dating site's iffy privacy protocols place all the more pressure on users to be careful about what they reveal.

Bostonian Jennifer Torode recalls running into what she thought was merely an annoying glitch on what she calls "a respected, paid online dating site." The site's registration system wouldn't accept her personal email address. She used her work email temporarily while tech support worked on solving the problem.

The site's messaging system hides users' actual email addresses, but Torode quickly discovered how inadequately that protected her.

"The next day, I had my work email's out-of-office autoreply on," she says. "Anyone from that dating site who contacted me got a reply with my email signature containing my full name, mobile and landline phone numbers, work address and two of my colleagues' contact info."

Naturally, Torode wouldn't make the same mistake again, but when she tried to alert the site about something she considered a "huge privacy concern," she heard nothing back.

In 2013, 13 British dating sites created the Online Dating Association (ODA), in response to what they call "the need for the industry to step up and take responsibility for setting and maintaining standards." Analysts view this organization, which now has 16 members, with wary optimism.

"While it is very hard for users to put much stock into the bold claims of privacy that some dating sites make, membership of the ODA ought to provide some sense of respectability in the eyes of the (apparently very few) users who appear to be concerned about whether a dating website is sufficiently 'safe'," says data protection consultant Martin Hoskins.

> In a way, just being on a dating website, I expect less privacy
>
> Jennifer Torode

Still, he says, even savvy users should assume no guarantee of privacy – even if a site has good intentions, it still might not have the capacity for follow-through.

"The problem is that these websites are run by people who lack the resources that the global social networking sites can afford," he says. "Naturally there is a higher risk of a personal data breach."

In a recent survey from communications technology company Bandwidth, 97% of respondents rated personal safety in online dating as "very important", but the gap remains between the value people place on security, and their willingness to take steps to assure it.

"It would be foolish to think that another Ashley Madison incident could not happen again," says Hoskins. "People should be on their guard. If they decide to post images or personal details that they would not wish their closest relatives to see, they only have themselves to blame if, unfortunately, an incident occurs that results in over-exposure."

Others tend to talk more in terms of responsibility than blame, but they still look to users rather than business owners or regulators as the most likely agent in maintaining privacy.

"Online dating can be a great way to meet that special someone. However, it doesn't hurt to place a little more caution when using these sites or apps," says Tony Neate, the CEO of Get Safe Online, whose website provides free resources designed to help people protect themselves and their businesses against fraud, identity theft, viruses and other online threats.

"As a rule of thumb, when using any online dating app or site, make sure your internet security software is up-to-date, and that you protect your passwords. Plus, when creating your online profile, keep personal information and contact details private."

Britain's Information Commissioner's Office (ICO), an independent public body sponsored by the Department for Media, Culture and Sport, also encourages users to read the terms and conditions on dating websites before they provide any information.

"Clearly dating websites are going to need to take a lot of personal information from their customers," Simon Entwisle, ICO director of operations, said in a statement. "But it's crucial they let those customers know how their information is going to be used."

Jennifer Torode says she's more careful now, but that she just accepts certain realities about online dating.

"If you've ever read a privacy statement, it's as long as my leg! And I have long legs," she says. "People should know that privacy is not always guaranteed. I still use online dating sites but use them with caution and common sense. In a way, just being on a dating website, I expect less privacy."

Chris Orris agrees – while he was a little surprised at how personal data moved around from site to site, he didn't view it as impetus to do things differently.

"Basically, I've changed nothing," he says. "I work in PR, so I've already made it a point to make most of my information easily searchable on the internet. To me it's a cost of doing business, but by the same token I'm extra careful with potentially harmful information on all networks, regardless of how private they are individually."

In fact, Orris says, he kind of likes it when his online activities collide.

"My networks can leak information between one another and I don't see it hurting me," he says. "In fact it can help. My targeted ads end up being much more relevant and interesting now than they used to be."

FOLLOW US ONLINE

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

TWITTER: **@INFOSECURITYMAG**

LINKEDIN: **INFOSECURITY MAGAZINE**

FACEBOOK: **INFOSECURITY MAGAZINE**

GOOGLE+: **INFOSECURITY MAGAZINE**

WWW.INFOSECURITY-MAGAZINE.COM

GDPR

Good for the DPO

The long awaited reform of the European data protection laws will be implemented in 2018. **Dan Raywood** talked to Tim Turner and Jon Baines from the National Association of Data Protection Officers (NADPO) about how changes are affecting those doing the job

The GDPR will be put upon data protection officers (DPO) from 2018, how ready are they for it?

JB - "Data Protection Officer" is not (currently at least) a defined role. Consequently, the term covers a hugely varied set of people and jobs across a hugely varied range of industries and services. What the GDPR will bring is some level of standardization for the role, at least for those data controllers who will be required as a matter of law to appoint a DPO (broadly, that will mean all public sector bodies, all entities employing more than 250 people and those entities whose core activities involve the monitoring of data subjects).

TT - It depends how good their knowledge of the current legislation is, and how well their organization is complying at the moment. For an organization that is transparent with people, has relatively good security and culture of investigating incidents, and which is conscious of risk, there is still plenty of work to do but it may not be a significant culture change. An organization that takes data protection seriously could see it as more of the same – a lot more, actually, but based on very similar principles to what we have now.

JB - That "standardization" will take the form of requirements that DPOs must, *inter alia*: have expert knowledge and "professional qualities"; be provided with necessary resources to perform their role; be appointed for at least two years and not dismissed unless they fail to fulfil the conditions required for the performance of their duties; report to the organization's management; must undertake specified tasks, in accordance with Article 37. None of this is in the current European Data Protection Directive (nor the domestic Data Protection Act 1998), and as the GDPR takes the form of a binding legislative instrument which must be applied uniformly throughout the EU, these DPO functions and designations *will* come into force.

TT - The problem is, as I've described above, the minority of organizations. Many have interminable privacy policies written to suit the lawyers and hoodwink the individual. Security is complacent or weak. The basics like consent are deeply flawed – many organizations don't obtain meaningful, freely given consent and probably don't want to because that involves people saying no.

One of the challenges that has not had enough attention is the consistency mechanism. The Information Commissioner issues a relatively small amount of fines on a narrow strand of data protection breaches – there are very few on accuracy, none on subject access to data, one on the basic justifications for using data. This is despite breaches all over the place in these areas. I think the ICO, and the rest of us, are going to find it difficult to be consistent with a European culture of enforcement where Facebook gets fined hundreds of thousands of Euros over the use of a cookie.

With ICO fines, Snowden leaks and now the Panama Papers, are data protection officers now under more pressure to comply with regulation that they do not understand?

JB - I certainly think there's a lot of pressure, but when it comes to understanding the legal and regulatory regimes, I come back to my

point above that there's a huge range of people in the UK undertaking the role of DPO. In my opinion some DPOs understand the law better than some people at the ICO! That said, in an era when data processing often involves global transfers and transit of data, it can be extremely difficult to understand simply what is happening with data for which one is responsible, let alone the relevant legal and regulatory regimes applying.

TT - I haven't met many data protection officers who have read the regulation yet. I think if they dig into it, they'll find principles and concepts that they're more than familiar with. The problem is, the IT press and privacy lawyers are hyping the regulation up as being incredibly complicated and difficult, which discourages people from actually picking the text up and reading it. Having said that, I've met quite a few data protection officers over the years who have never read the Data Protection Act.

If you're looking at the underlying principles of data protection, they're exactly the same and the idea that they're difficult to understand is nonsense. The difficulty comes in the practical work – giving more information to individuals in a format they understand (even if they're not interested), carrying out proactive risk assessments, reporting breaches to the Commissioner. It's not hard to understand what the work is; the problem is how much more work there is.

Does the average data protection officer know what "sensitive data" is regarding their business?

JB - To the extent that there is such a thing as an "average" DPO (see above), I would say that they, more than anyone else, should and will know what sensitive (personal) data their business is processing. It's really data protection 101 that a DPO should be up to speed on this, and relevant standards like ISO 27001 and BSI 10012:2009 effectively mandate it.

In practice, in organizations where good data protection practice is not embedded, a DPO will often be left uninformed or unsighted about activities, and this is clearly a big area of professional and corporate risk.

TT - Yes. I think the issue is that the average board and senior managers don't really think about the risks associated with sensitive data. They only want to take action to protect sensitive data after something goes wrong.

I spotted a competition to "explain the difference between unambiguous and explicit consent" offering a £200 prize! Is the wording the problem, or is there a total lack of definition?

TT - That's my competition and I have to admit an element of trolling some of my data protection colleagues. The regulation is drafted to draw a distinction between normal and sensitive data, with sensitive data requiring 'explicit' consent. The current Data Protection Act does the same thing – it says 'consent' and 'explicit consent'. I think there is a shared delusion that somehow if it doesn't say 'explicit', you can get some kind of half-baked, accidental consent and rely on it for years. That isn't true now, even if some well-known privacy lawyers claim that the current arrangements are 'decaffeinated consent', but it's definitely not true of the Regulation.

While some of those who enter the competition may be able to demonstrate a practical difference between unambiguous consent and explicit consent, the point I am trying to make is about unambiguous consent – it's a very high threshold anyway. The Regulation makes clear that opt-outs don't count, inferring consent from silence doesn't count. The person has to have a free choice, they have to understand what they're agreeing to, they have to be able to change their mind and be told that they can change their mind. Many organizations just don't meet this standard now, and they have to face up the challenge that people have a choice, and they have to be allowed to exercise it.

Speaking purely personally, I think the difference between the two is very narrow (the word 'explicit' is part of the dictionary definition of 'unambiguous'). Beyond making mischief, my real message is that organizations handling data need to face up to the fact that they don't get consent at the moment. They have some impenetrable terms and conditions, consent boxes that are mandatory fields, and tricky opt-outs. Unless you have a legal obligation or a contract with the person, in most cases using a person's data is a privilege you have to earn, not an entitlement you can exploit.

Just to emphasize though, it is a real competition and if anyone can draw meaningful distinctions between the two, that would be in everyone's interests, and you can win £200.

JB - Tim asked me to be one of the judges for his competition, and I agreed because, as well as it being a bit of fun, I think it raises a really important point: the notion of consent, and consequently the mechanisms data controllers will use to get consent, is going to be hugely significant under the GDPR. I think too many people think they know what "consent" means (and what "explicit" and "unambiguous" consent mean) but don't appreciate that their interpretation might differ from, say, a data subject's. I don't think this ambiguity is properly addressed in the current text of the Regulation, so anything that can prompt debate on the issue is to be welcomed.

What does Government need to do to improve the life for the data protection officer?

TT - Fund the Information Commissioner properly, and promote a UK quality standard for the role. If the ICO has the resources to take on serious breaches beyond security issues, organizations might take data protection more seriously, and might look to the data protection officer as someone of value. At the moment, I think some organizations will tweak the job description of some low paid data protection or information governance person, and haul them in front of the board every year so that they can say everything's fine. It won't be.

CyberCenturion 2016

Winners Crowned at Bletchley Park Final

Michael Hill attends the CyberCenturion 2016 Final as the last 10 teams battle it out for the title

In April this year, the historic venue of The National Museum of Computing (TNMOC) played host to the national finals of CyberCenturion 2016, a country-wide cybersecurity contest aimed at discovering and developing the cyber skills of youngsters in the UK. It was a school team from Gibraltar who eventually took the spoils after a day of fast-paced cyber competition at Bletchley Park, sponsored by Cyber Security Challenge UK and global security company Northrop Grumman.

Hundreds of players from across the country and overseas territories took part in the competition over three grueling qualifying rounds, leaving 10 remaining teams of the UK's brightest 12-18 year olds tasked with using their cyber skills to protect a fictitious Internet of Things business dubbed 'CyberPatio', whose network was vulnerable to cyber-attack.

"We are extremely happy to host the CyberCenturion Final again this year," said Tim Reynolds, deputy chairman of TNMOC. "Through the Museum's Learning Program, we aim to inspire young people by showcasing our rich heritage of technology, engineering and computing."

"By holding the competition at the Museum, young people can see how skills such as codebreaking, mathematics and computing have developed and now provide fulfilling and rewarding careers in modern day cybersecurity."

In the fitting shadow of Colossus, the world's first electronic computer used to help decipher the Lorenzencrypted messages in WWII and following some rousing opening speeches the final got underway, with competitors battling it out in a cyber-defense scenario much like those businesses face in the real world every day.

"The CyberCenturion competition is becoming one of the most successful coding and cyber events for this age group in the UK," said Stephanie Daman, CEO at Cyber Security Challenge UK, the government's collaboration with UK industry and academia to find hidden cybersecurity talent across the country. "With an expected deficit of 1.5 million unfulfilled jobs in cyber globally by 2020, we need to get children interested in the field at an early age and STEM education programs allow us to do that."

> There's lots of talent out there but it's all about getting it into the industry
>
> Stephanie Daman

"The big issue for the industry is always trying to find properly skilled recruits," Daman told *Infosecurity*. "There's lots of talent out there

Stephanie Daman


Winners, Team G-Sec

but it's all about getting it into the industry, and that's really what the competition helps to do and that's why it's so important."

These were sentiments echoed by Dr Andrew Tyler, chief executive Europe at Northrop Grumman, who told *Infosecurity* that CyberCenturion is focused on nurturing the next generation of cybersecurity professionals and without initiatives like it, the future of the industry would have a far bleaker outlook.

"Quite often a new challenge comes along, like cyber, and we're not very well equipped to produce the people required very quickly to deal with it, and it catches us out" he said.

"Between ourselves, our partner companies and the government, we've pretty much cleared the market in the UK of cyber specialists. We've now got to start growing the next generation of talent and that is 100% what this is all about."

With the contest in full swing and the competitors all hard at work, Cyber Security Challenge took the opportunity to announce the launch of its new Extended Project Qualification (EPQ) in cybersecurity to a brimming room of teachers, security professionals and journalists all gathered at the event.

The EPQ, which is supported by a range of education partners, will be officially rolled-out across schools/colleges, online and via social clubs in September. It is a level three qualification equivalent to an AS-Level (worth up to 70 UCAS points) and is designed to help address the UK's cybersecurity skills shortage by giving students a structured understanding of the whole cyber domain – from risk management to digital forensics.

> The whole experience of attending the event at Bletchley Park and competing against other fantastic teams was an amazing feat in itself
>
> Stewart Harrison

Brian Higgins, business development manager at one of the key supporters of the EPQ (ISC)², explained that the new qualification will link educational content and structure with National Occupational Standards and also the learning outcomes of undergraduate degree programs, "providing a real first step up the ladder for young people looking to move into the cybersecurity industry."

Higgins said that securing a job in cybersecurity requires more than just an interest in computers, you've got to be able to demonstrate "aptitude, knowledge, ability and enthusiasm for the subject" and doing something like an EPQ goes a long way to achieving that.

As the day drew to a close, so did the CyberCenturion Final and it was team G-Sec, made up of A-Level students from Bayside school and led by teacher Stewart Harrison, who were announced as the winners receiving a selection of prizes including resources, books and technology for their school.

"I am delighted that they have won," Mr Harrison told *Infosecurity*. "My boys have worked very hard during the qualifying rounds and in the lead up to the Grand Finals. The whole experience of attending the event at Bletchley Park and competing against other fantastic teams was an amazing feat in itself. I am immensely proud."

"It's very rewarding to see the boys engage and enjoy the competitive element of the event. We don't provide enough opportunities in the education system for students to really stretch themselves and independently develop life skills. The discipline, transferable skills and team work efforts are of invaluable use to them now. All in all they have formed fantastic friendships that I am sure will last a lifetime."

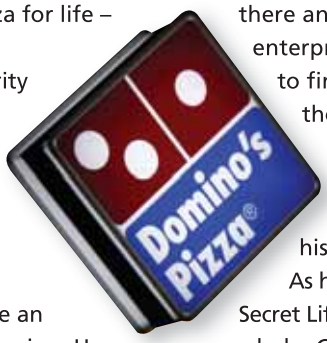
It really was great to see so many young, enthusiastic competitors taking part in the contest with such a clear passion for cybersecurity, something I believe to be a vital factor in the industry's fight to close the current skills gap and with initiatives like CyberCenturion, the introduction of the new EPQ and the ongoing support of companies like Cyber Security Challenge UK, Northrop Grumman and (ISC)², things are certainly heading in the right direction.

Slack Space

Hacking Free Pizza for Life

Sometimes hackers do their thing for sheer financial gain as part of an organized crime ring or otherwise – but sometimes, they're just looking for a slice of the good life.

As in, free delivery pizza for life – yeah, dawg.



Paul Price, a cybersecurity expert based in the UK, was able to exploit a bug in the Domino's Pizza mobile app (featuring everyone's favorite non-Siri voice assistant, "Dom") to place an order for pizza without paying. He said that he noticed that once customers had finished ordering they would sometimes be sent a £10-off voucher code, indicating that the app was processing payments client side via a payment gateway – a far from best practice that leaves apps vulnerable.

After some probing around, he had an exploit and was soon awaiting his cheese-tastic, totally free prize. "I called the store and they confirmed they have received my order and it will be delivered within the next 20 minutes," he told the *Telegraph*. "My first thought: awesome. My second thought: s—t."

To his credit, he ended up paying the delivery driver and alerting the pizza chain, which fixed the app, but it points out an all-too-common developer error. "In this case the hack comes down to the developer not remembering that the application exists in a hostile environment," Paul Farrington, senior solution architect at Veracode, told Slack. "Developing applications that exist on a user's device takes the problem to the next level. The threat model is completely different. These apps can be reverse engineered, or communication intercepted and changed with relative ease."

As easy as, well, pie.

Math Guy: Perfect for 30K+ Women on OK Cupid

When you're an applied math grad student logging a lot of thesis time, sleeping on a pallet in your cubicle, it's hard to get out there and find your soulmate. However, one enterprising young man figured out how to find not just one, but tens of thousands of potential forever-people. He did it the not-so-old-fashioned way: he used a computer algorithm to optimize his OK Cupid profile.

As he laid out on an episode of The Secret Life of Scientists & Engineers, Math scholar Chris McKinlay parlayed his experience working with supercomputers to analyze OK Cupid's question data, which the dating service uses to determine compatibility.

True to his left-brain characteristics, he went about the whole thing in a logistic manner. "The first thing he noticed was that women in Southern California tended to select questions that clumped up into seven categories," Sophos Security explained.

"Looking at those subsets, McKinlay chose a category that corresponded with the type of woman he'd like to date. Next, he wrote some code to determine which questions were most important to the type of women he felt drawn to. Then, McKinlay determined which of those questions he'd feel comfortable answering truthfully."

The next thing he knew, he had become the top match for 30,000+ women – receiving up to 10 unsolicited messages per day. Then he set about becoming a dating robot, meeting one woman per day in a series of what he called "efficient and depersonalized dates."

"I was trending globally," he said. Not bad for a math dude.

The funny thing is, the whole thing worked out well for him: he actually went on to get engaged to date No. 88, who presumably didn't mind his ruthlessly efficient approach to romance. So, the moral of this thoroughly modern and IT-tastic story is this: you can kiss a lot of frogs, but why not just get a computer algorithm to do the frog-kissing for you?

Man Arrested After Tagging Himself as Rioting

Hey kids, here's a tip: if you're engaging in a riot, it's probably not a good idea to "check in" for the proceedings on Facebook. It never fails to amaze this Slacker how some people don't grasp the concept that a social network is, well, social.

Robert Darragh, 21, was arrested for rioting and sentenced to two years (one of them to be spent in jail, the other on probation) after participating in the parade violence in the Woodvale/Twaddell area of Belfast last July. It was a serious event: The BBC reported that a total of 29 police officers were injured during the rioting "after police lines were pelted with masonry, bricks, bottles and other items, with one officer almost losing an ear."

Darragh, who later admitted to throwing items at police lines, had covered his face and had his hood up to avoid being identified on CCTV while the outbreak was going on. However, that prudence evaporated when it came to letting his friends know what was up, tagging himself not once but twice as being at the riot.

The article doesn't say what, exactly, Darragh said. We're hoping it was something like, "TOTALLY hangin' at the riot!!!! #SundayFunday"

A defense lawyer said that when questioned by police about his involvement, Darragh somewhat lamely said that he could not remember quite what he had been up to virtually or otherwise, "as he had been on a three-day binge."

Anyone who wants to share their grumbles, groans, tip-offs and gossip with the author of Slack Space should contact infosecurity.press@reedexpo.co.uk

Data Protection Issues in Turkey

Begüm Yavuzdogan Okumus, managing associate of Gun+Partners, looks at the impact and improvements the GDPR will have on Turkish data protection

In April 2016, Turkey faced one of the biggest data breaches ever recorded, where it was claimed that the personal data of almost 50 million Turkish citizens was leaked online. That breach is currently being investigated by the prosecuting officer, and although officials claim that the data leak only contains data from 2009 and reveals no new records beyond that time – it is still accepted as a colossal data breach.

In the meantime, the long awaited Data Protection Law (the "Law") entered into force on 7 April 2016, just days after the news of Turkey's biggest data breach. For many years, Turkey had lacked a separate legislative measure regarding the issue of data protection. Previous draft laws that had been sent to the Turkish Parliament were either returned to the proposing committee or not even discussed. Adoption of data protection law was a real need both for the Turkish society and for Turkey's harmonization with EU regulations.

The Law contains detailed provisions relating to the protection of personal data, an area that was previously only covered by an insufficient and piecemeal application of different legislative measures and the Turkish Constitution.

The Law introduces an official definition for the term *"personal data"*, defining it as "any type of information that relates to an identified or identifiable natural person". This means that the Law covers data of real people and its scope is very wide indeed. The main principle is that personal data can only be processed once the data subject has provided explicit consent. However, personal data can be processed without obtaining explicit consent in cases of certain exceptions stated under the Law.

The Law also separately distinguished a category of *"personal data of a special nature"* which is subject to a more extensive level of protection. The types of personal data that fall under this category are related to race, ethnicity, political views, philosophical belief, religious denomination or other beliefs, clothing and attire, membership in associations, charities or trade unions, health, sex life, convictions, security measures and biometric data. The law-maker has set the standard of prohibition of processing personal data of special nature, unless explicit consent of the data subject is present.

It must be noted that health and sex life data cannot be processed in any case without an explicit consent and even in the presence of explicit consent, such data can only be processed by persons or authorized institutes bound by the duty of confidentiality for the purpose of the protection of public health, the provision of medical, diagnostic and treatment services and the planning, managements and financing of healthcare services.

The Law further provides for data security obligations for data controllers and stipulates that data controllers are under the obligation to implement all kinds of technical and administrative measures to maintain a security level that would avoid unlawful processing of and access to personal data, whilst also safeguarding personal data. The data controller and data processor are *jointly liable* for maintaining the security measures under the Law.

It should also be noted that the data controller has a duty to inform the Data Protection Board and the relevant party if and when personal data has been unlawfully accessed. Thereafter, the board has the discretion to announce the breach on its website or another via another communications channel.

In addition to criminal sanctions stipulated under the Turkish Criminal Code and repeated under the Law, the Law introduces monetary sanctions. Data controllers will face administrative monetary sanctions between the range of TRY 5,000 (approx. EUR 1,500) and TRY 1,000,000 (approx. EUR 300,000) if they are in breach of their obligations to inform the data subject, to ensure data security, enforce the decisions of the board and to the register.

Under the Law, there is a transition period of two years for data controllers to make personal data that has been processed prior to the enactment of the Law in compliance with the Law. In case such compliance is not ensured, incompliant personal data will be deleted, destroyed or anonymized.

Parting Shots

The term 'privacy' can be defined as "a state in which one is not observed or disturbed by other people."

I think it's safe to say that in today's internet-dependent, ever-connected world it's simply not realistic to guarantee that *anybody's* personal details or that of an organization are ever free from observation or disturbance to at least some degree. Whether it's an authority or a malicious hacker, if somebody wants to find out something about you badly enough, they will.

However, this does not mean that personal privacy is something that should be ignored or sacrificed just because we now live in such a digital-dependent age, and although the average internet user may be a long way away from grasping what actually makes good privacy on the web – you just have to look at the amount of personal information still shared on social media as a prime example – there's definitely been a notable change in attitudes towards privacy in recent times.

"Using the internet and sharing more data online has opened up more questions about privacy," independent consultant Dr Jessica Barker told *Infosecurity*. "A lot of people care very deeply about privacy issues and it has been in the news a lot more in the last few years."

Whilst privacy awareness is something that has slowly, although steadily, gained pace in the last decade, it was undoubtedly the Snowden leaks in 2013 that fast-tracked the issue to the publically discussed topic it is today.

"The Snowden revelations helped to propel the privacy debate into the public sphere," said Jim Killock, Executive Director of Open Rights Group (ORG). "Many privacy activists had suspected that surveillance on this scale had been happening – Snowden confirmed their fears. Much of the public – and even our MPs – had no idea, largely because GCHQ built these programs without prior parliamentary debate.

"ORG has seen a significant growth in our members over the last three years, which we believe is in part because of this growing awareness of privacy as a result of the Snowden revelations," he added. So where has this left public attitudes towards privacy in 2016?

For me, this was made clear earlier this year when, on a train one morning, I overheard a conversation about the San Bernardino gunmen standoff between Apple and the FBI. It struck me that instead of talking about the miserable weather outside or the soccer match the night before, commuters were engaged in a discussion about data privacy and what the ramifications of the case would mean for the general public, which is, in all honesty, not something you see very often.

Similarly, with the Internet of Things (IoT) continuing to snowball in both the workplace and the home, it's becoming ever-clearer that people are growing more concerned with the privacy threat IoT devices pose. This was evident in a recent study by Mobile Ecosystem Forum which found that 62% of consumers are worried that a world of connected devices will see their privacy impeded.

Looking forward then, with concerns over privacy now so widespread, it's obvious that it is going to play an unprecedented role in the handling of business across Europe in the years to come. With the General Data Protection Regulation (GDPR) coming into effect in 2018, companies of all sizes are going to be forced to ensure the data of their customers is kept secure, or run the risk of facing hefty fines of 4% of global turnover or €20m for serious breaches of the new regulations.

"Privacy is a critical topic for most individuals including customers and employees. As a result privacy and security are business critical already and the higher level of fines in GDPR already mean it has the attention of most boards," Jonathan Armstrong, compliance and technology lawyer at Cordery, told *Infosecurity*.

Armstrong believes these new laws will help ease some of the public fear surrounding privacy and give civilians more power than they have had in the past.

"Individuals have important new rights including a right to data portability – this means that if they have concerns about an organization they deal with they can switch much more easily. They also have new rights to know about security breaches and to find out more quickly (and now for free) about how their data is handled," he added. Of course, with the EU referendum just around the corner, it currently remains to be seen what impact the GDPR will have in the UK.

To conclude, it looks as though personal privacy is finally getting the attention it deserves in both business and across the public sphere. I believe it is a fundamental right and not something that should be discounted just because perfection isn't possible, so the fact that it is now such a widely discussed topic can only be a good thing that will lead to better security in the future. People from all walks of life should be able to feel confident that their personal data is protected as well as it can be, with no corners cut and no stone left unturned to ensure it is.

> Personal privacy is not something that should be ignored or sacrificed just because we now live in such a digital-dependent age

After all, as Jim Killock sums up, "We are entitled to a private life and a digital life and we should challenge those who seek to undermine our rights."

Michael Hill, Deputy Editor

“It’s not just security. It’s defence.”

Cyber threats have changed, and the solutions need to change too. The sophisticated techniques BAE Systems uses to protect government and military assets are now helping to defend businesses around the world.

Learn more at BAEsystems.com/businessdefence

BAE SYSTEMS

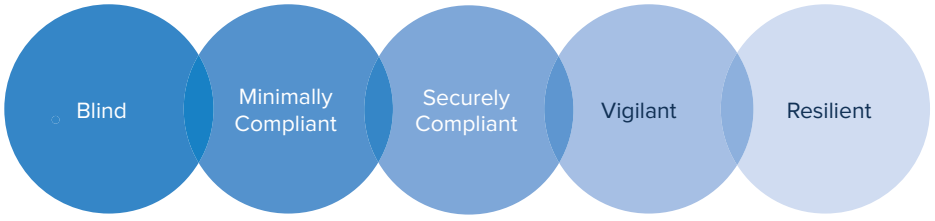
LogRhythm®

The Security Intelligence Company

They will get in

90% of large UK businesses experienced a security breach in the past year[1]

Discover how prepared your business is for today's threat landscape.



Where does your business sit on the scale?

Visit us on stand F20 to find out.

Total **visibility**, smart **detection**, accelerated **response.**

www.logrhythm.com

[1]Bloor Research report, 2016 'How to raise your organisation's security maturity level', page 3