Q1 /// 2016 /// VOLUME 13 /// ISSUE 1

STRATEGY /// INSIGHT /// TECHNOLOGY

infosecurity

The Race for the White House

Why Security is among the Key Battlegrounds

PLUS:

DMARC /// TALKTALK AFTERMATH /// CYBER PSYCHOLOGY

CONNECTED SECURITY EXPO @ ISC WEST

Bridging the gap between physical and cyber security.

CONFERENCE:
APRIL 6-7, 2016

EXHIBIT HALL:
APRIL 6-8, 2016

SANDS EXPO
LAS VEGAS, NV

SPONSORED BY:

SIA SECURITY INDUSTRY ASSOCIATION

ENDORSED BY:

PSA SECURITY NETWORK

info security

IT SECURITY ONE2ONE SUMMIT
ENHANCING BUSINESS OUTCOMES

Presented by: info security

CONNECTED SECURITY EXPO

The only event where you can build a holistic security strategy for the connected enterprise. At Connected Security Expo you will look at how physical and information security can be used together to mitigate new and emerging cyber threats in a hyper-connected world.

BREAKING DOWN THE SILOS
ACROSS PHYSICAL & CYBER SECURITY

- Immersive Exhibit Floor featuring leaders in IT Security Products and Solutions
- Full 2-Day Conference Program brought to you by *Infosecurity Magazine*
- Speakers include: CISOs, CSOs and Industry Thought-leaders
- Innovation Stage where you can see the newest technology advancements straight from the solution providers

TO RECEIVE MORE INFORMATION VISIT
WWW.CONNECTEDSECURITYEXPO.COM

Contents

January/February/March 2016

COVER FEATURE

FEATURES

OPINIONS

REGULARS

ISSN 1754-4548

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

The Stars Look Very Different Today

I write my first editor's comment in rather a sombre mood, as today is Monday 11th January and I have woken up to the news of the death of David Bowie.

Rather than try and draw an analogy about the visionary musician reinventing music over a 50 year career, I'll write this to a soundtrack of Ziggy Stardust. So apologies for any puns in advance.

I've been delighted to join Infosecurity Magazine for the majority of this year covering for the remainder of Eleanor's time away, and with seven years of experience behind me in covering information security as both a journalist and analyst, I've long admired this brand's approach and coverage of the topic. Of course 2016 brings with it a new set of ambitions and predictions, and over the time I get to spend in the editor's chair I'll do my best to address those directly.

Arriving just before Christmas, my inbox was crammed with predictions for the new year and one of the more common was that of healthcare. In 2015 we saw data breach incidents at Premera, Anthem and Blue Cross, and with a memory of numerous Information Commissioner regulatory enforcement notices against the NHS and primary care trusts, it would seem that healthcare has climbed a long and slow path to the level of the most critical data.

Listening to a recent edition of Rafal Los' podcast "Down the security rabbithole" (episode 174 if you are interested), he talked with a progressive CISO from a Fortune 250 healthcare organization, and this was especially enlightening as the major challenges were detailed as being Big Data, third party access, mobile access and HIPAA.

In this issue we look further at the issue of mobility in healthcare, as Arxan CTO Sam Rehman evaluates the threat. This is not an area to be taken lightly, as not only is healthcare and medical data among the most sensitive in regard to personal security, but it is also the hardest to change if you are a victim.

If your credit card is cloned, you call your provider (or in my experience they call you, thanks to some excellent fraud monitoring) and they issue you a new card. If your medical data is breached, you cannot change your DNA on their record or your blood type, so you are stuck for a solution apart from the local data protection regulator giving the company a fine and a public telling off.

It is for this reason that I believe that healthcare data needs to be the most heavily protected data and with RSA Conference a matter of weeks away, I expect protecting healthcare to be on the agenda for 2016. The 2013 Target data breach shook up retail security and the US Government has pushed through stronger payment card security with chip-based authentication now being adopted by major retailers.

Will something be adopted by the healthcare organizations? Those working in those companies would argue that they are doing all they can to best secure the data, and another key challenge is the third parties who connect into the companies—the consultants, the owners of the patents and developers of the medicines, and of course the internet-connectivity of the machinery used in hospitals and surgeries. It all adds up to one big melting pot of security headaches and something we are hopefully going to predict on, but not be writing about, in 2016.

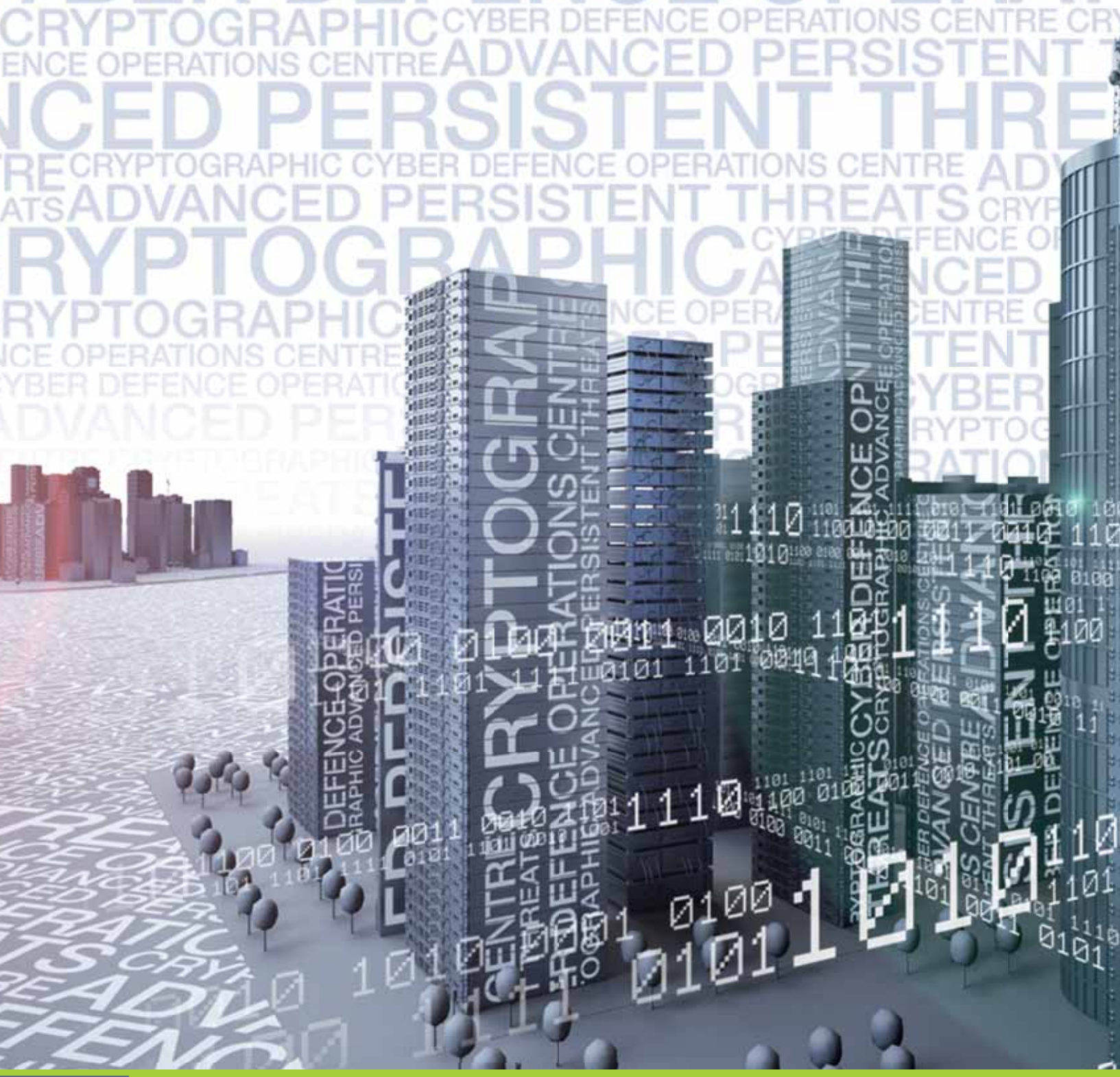
It may be many months away, but in this issue we take a first look at the key players in the 2016 US Presidential election. Much like the UK general election last year, the process begins long before voters go to the polling booth and these days social media plays a large part in the campaign trail.

This will also be the first US election where the largest companies in the world are not in finance or manufacturing, but in technology, and the key state of California is not only one for both parties to take seriously, but to consider the impact both before and after the election of Silicon Valley.

> Healthcare data needs to be the most heavily protected data

I've always remained excited about every new year in information security, as we have no idea of what the year will bring us, but at the end of each year we are able to reflect on a previous year with new knowledge. We may lose some heroes along the way, but this remains the most dynamic sector of IT for a reason.

Dan Raywood, Editor



CyberSecurity

Sophisticated solutions and services for protection against targeted cyber attacks.

www.cybersecurity-airbusds.com

PIONEERING THE FUTURE TOGETHER

AIRBUS
DEFENCE & SPACE

The British Entry for Breach of the Year 2015

TalkTalk:

Phil Muncaster takes a look at what really happened at the ISP last year, and what lessons can be learned from its handling of the incident

TalkTalk

Everything's always 'bigger and better' in the US, or at least that's what they say. Unfortunately for federal employees and American consumers, this also means data breaches that have hit tens of millions over the past year.

In dear old Blighty we don't seem to be able to compete. The breach that has captured most of the headlines over the past few months has been the attack on TalkTalk. But despite the relatively paltry amount of customers affected, this one's worth taking a closer look at.

How can a firm the size of TalkTalk have been successfully attacked via what appears to be a relatively basic security flaw? Why weren't its incident response and crisis comms up to speed? How can we all avoid following in its sullied footsteps?

The story so far

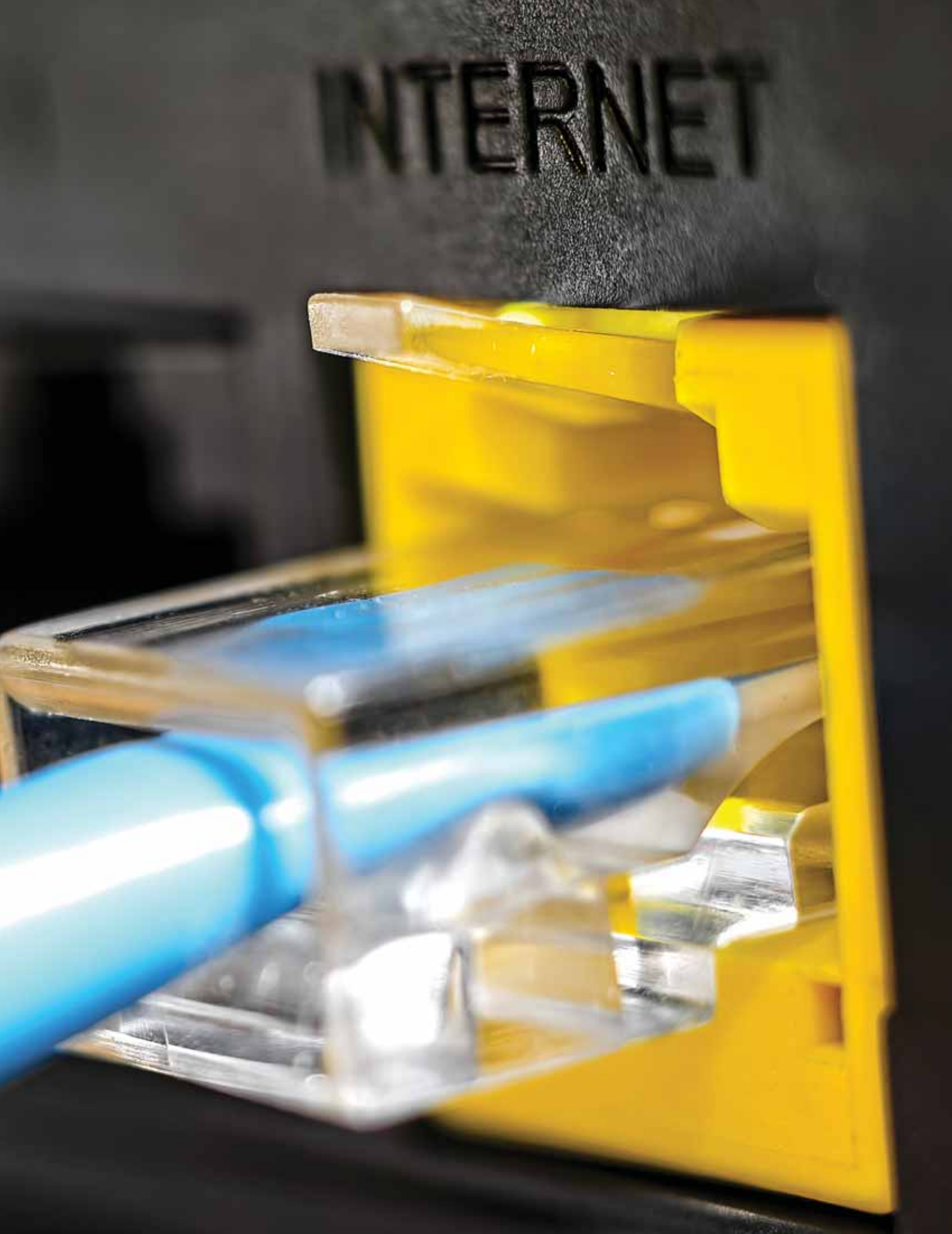
On 21 October 2015 the TalkTalk website mysteriously went down for users, with the firm claiming it was facing 'technical issues' which its engineers were 'working hard to fix'. The following day the firm released a longer statement and began informing all of its approximately four million customers that it had been the victim of a cyber-attack—the third in the space of a year.

Its initial notice had the following: *"Today (Thursday 22nd October), a criminal investigation was launched by the Metropolitan Police Cyber Crime Unit following a significant and sustained cyber-attack on our website yesterday.*

"That investigation is ongoing, but unfortunately there is a chance that some of the following data has been compromised: names, addresses, date of birth, phone numbers, email addresses, TalkTalk account information, credit card details and/or bank details. We are continuing to work with leading cybercrime specialists and the Metropolitan Police to establish exactly what happened and the extent of any information accessed."

The next day, CEO Dido Harding told the BBC that the firm had received a ransom

Dido Harding faced many questions on the incident


INTERNET

email purporting to come from the hacker(s). It subsequently emerged over the weekend that the attack was against its website and related databases rather than "core systems."

As a result, only incomplete card data – if any—had been stolen, although bank account numbers and sort codes were taken. A hacker couldn't use these to access user accounts, but they could certainly be employed to good effect in follow-up phishing attacks. On Monday 26 October, TalkTalk said it would waive account termination fees only on a case-by-case basis if users had money stolen from their bank accounts as a direct result of the attack, causing anger among customers.

It took over a week later for the firm to finally admit the true scale of the attack. Just 156,959 customers (4%) have had sensitive data exposed. Of these, 15,656 bank account numbers and sort codes were accessed and 28,000 'obscured' card details were taken. Other exposed details include name, address, date of birth, telephone number and email address, but the firm said TalkTalk account passwords were not taken.

The police arrested one 15-year-old from Northern Ireland, two 16-year-olds (from London and Norwich) and a 20-year-old Staffordshire man in connection with the attacks and bailed them until March 2016 on suspicion of Computer Misuse Act offenses. An 18-year-old from Llanelli had also been cuffed on suspicion of blackmail.

How did the attackers get in? Initial statements from the firm suggested a DDoS attack was to blame, but of course this couldn't have been responsible for the theft of personal information. CEO Harding then told the FT that a "sequential attack" was responsible—presumably referring to an SQL injection, an extremely common web vulnerability.

Tom Williams, lead investigative consultant at UK consultancy Context Information Security, believes "some kids loosely linked to a hacktivist collective" went looking speculatively for vulnerabilities in TalkTalk's website. Then they shared their findings with others. It was at this point that the information found its way to someone who tried to monetize the flaw via the SQLi attack and DDoS—the latter probably used as a "smokescreen" to distract TalkTalk's IT security staff. Talk of the attack being carried out by Islamic State hackers is likely to be a red herring spread by the real perpetrators, he tells Infosecurity.

> TalkTalk has said data wasn't encrypted because there was no legal requirement. But this is an example of when compliance sometimes gets in the way of security
>
> Tom Williams
> Context Information Security

Unhappy customers

TalkTalk admitted in its financials for the first half of the year that it would have to pay a one-off £35m bill in the aftermath of the attack, to be allocated to things like incident response, external consulting and increasing call volumes. A harder-to-quantify hit will be how many customers leave after their current contracts expire, and how many more potential customers the firm has lost because of the incident.

Although TalkTalk has also claimed on more than one occasion "we want to make customers aware that we will not call or otherwise contact them regarding this incident and ask for bank details or other financial or personal information," customers appear to have been taken in with follow-up scams. Reports emerged that customers are being vished, spammed and phished. For Williams, this could all have been prevented by encrypting customers' personally identifiable information.

"TalkTalk has said data wasn't encrypted because there was no legal requirement," he argues. "But this is an example of when compliance sometimes gets in the way of security—we might do what we need to tick the box but it's not necessarily the best for security."

The firm has tried to limit the PR damage by claiming to offer a "free reporting and blocking service for nuisance and malicious calls" and said it constantly reviews incoming calls "to identify and block malicious callers in a similar way to blocking spam emails." But for Williams both the SQL injection and the smokescreen DDoS—if they were indeed used in the attack—should in the first place "have been preventable for an organization of TalkTalk's stature."

Interestingly, some of the key security steps which should have spotted and prevented a SQLi attack had apparently already been put in place by the end of FY 2015, according to an end-of-year report by the telco. It claimed: "In FY15, key initiatives including the encryption of hardware and removable media, a data loss prevention solution, vulnerability scanning and penetration testing have been completed.

"A new Head of Security has also been appointed to establish and oversee the new Security Operations Centre, the activities of which have been outsourced to cybersecurity experts BAE systems."

Lesson learned?

TalkTalk hasn't just come under fire for its questionable security practises, its incident response has also been criticized for being too reactive, muddled and not taking enough time to educate the customer. New Quocirca research of 100 UK IT leaders found just half (49%) had a breach response plan in place, despite the fact that 38% claimed a breach was "inevitable." This kind of attitude may explain the firm's poor handling of the incident.

"It's something that's easier said than done in an extremely competitive industry because security is an additional cost," says Williams. "But they needed more robust incident response procedures—not just in dealing with it from a technical perspective but also from a comms aspect."

Rolf von Roessing, former international vice president of ISACA, argues that caution is often the best policy with regards to issuing public statements. "Communicating too quickly can cause some confusion with regard to the actual root cause and the consequences of the attack," he says. "To help ensure an effective response to an attack, ISACA's Cybersecurity Nexus (CSX) recommends that organizations have a strong mix of technical controls, cybersecurity education and awareness programs, well-tested incident response plans, and a skilled cyber workforce in place."

Quocirca analyst Bob Tarzey is more forgiving of the firm. "Credit where it's due they did put Harding in front of the media pretty sharpish—the problem is she wasn't well enough briefed," he tells Infosecurity.

TalkTalk has offered upgrade to all customers which could include unlimited calls, TV content and a mobile SIM. It has also offered 12 months free credit monitoring with Noddle. But many have argued this is simply too little to save its reputation. That has already been tarnished by its enforcing those strict rules preventing customers exiting contracts early.

In fact, Hogan Lovells partner Peter Watts believes there could still be some tricky legal waters for the ISP to cross. "For a customer of TalkTalk, the first thing to think about is whether the business has done everything it should have done to keep data safe. If not, the consumer will probably have a claim for any money they lose and may well also have a right to terminate their contract if they want to—limitations of liability in the contract are unlikely to protect the business," he tells *Infosecurity*.

"The problem for the consumer of course is that it is very difficult to be sure that the business hasn't had the proper security measures in place."

Despite customer anger, the firm's shareholders have reacted pretty favorably to its handling of the incident. In fact, shares rose 12% after its 1H financials were released.

So what can we learn? TalkTalk's shareholders might be happy, but its reputation following the incident will certainly suffer. Prevention is always cheaper and less painful than the cure when it comes to cybersecurity. Firms need to concentrate on getting the basics right: pen testing, finding and remediating any vulnerabilities, encrypting data and so on. They might not all be legally required but they could reduce the chances of a successful breach.

> Communicating too quickly can cause some confusion with regard to the actual root cause and the consequences of the attack
>
> Rolf von Roessing
> ISACA

The new European General Data Protection Regulation will require mandatory breach notification and large fines of potentially 2% of annual turnover or €1 million, which should concentrate minds.

For Williams, more info sharing could help firms. "A lot of companies are buying tactical threat feeds but sometimes the best threat intelligence is learning from your own internal incidents and harnessing that," he says. "And when you do go external, look for forums to join where you can learn from organzations in similar sectors. Every firm will at some point be a victim so the sharing experience is good."

For Quocirca's Tarzey, next gen firewalls, context-aware security tools, encryption for sensitive data and DLP could be enough to warn off the cyber-criminals. "Criminals want as easy a life as possible—they're rarely interested in singling out a specific organization, they just want to target the weakest," he says. "So it doesn't take an awful lot to get ahead of a weak pack."

Five of the worst UK data breaches

Major security incidents at UK firms might appear less frequently in the newspapers but that doesn't mean they're not happening. Here's a small selection of some of the most damaging in recent years.

1) In November 2007, HMRC lost two CDs containing details of the families of child benefits claimants in the post—27 million claimants in total. Information included names, addresses and dates of birth of children, as well as the National Insurance numbers and bank details of their parents.
2) A back-up hard disc drive containing highly sensitive personal information on nearly 3,000 prisoners was lost in by HMP Erlestoke in Wiltshire in 2013. The Ministry of Justice apparently didn't realize that encryption had to be switched on with the new drives.
3) Up to 2.4 million customers of one-time TalkTalk parent company, Carphone Warehouse, were affected when the firm was hit in August this year.
4) Personal information on 11 million savers was exposed when unencrypted laptop was stolen from a Nationwide employee in 2006.
5) Hackers accessed the accounts of up to 1.5 million Mumsnet account holders after they took advantage of the Heartbleed flaw.

Cybersecurity and the next POTUS

The 2016 US election will be the first fought in the world where Wikileaks, Edward Snowden and social media have all changed the security and political landscape. **Kathryn Pick** looks at the key battlegrounds and topics to sway the voters

Security is always going to play a big part in any political race in America. But rather than facing a visible threat that can be dealt with through one of the strongest armed forces in the world, the USA is the target of deep, dark attacks through their network infrastructure.

The Obama administration has made a number of moves to try and combat the ongoing cyber-war, be it against small groups of activists or allegedly state sponsored infiltrations. For example, the "cyber wargames" testing out its defences through its "special relationship" with the UK, sharing of intelligence between the public and private sector for another, and the extension of RICO laws.

But for the next inhabitant of the Oval Office, the fight is only going to get tougher when it comes to protecting the Government, businesses and citizens from

> Our country will outpace this rapidly changing threat, maintain strong protections against unwarranted Government or corporate surveillance, and ensure American companies are the most competitive in the world
>
> Hillary Clinton

the increasing technological threat, both from its own soil and abroad.

Where do the candidates stand?

Front runner for the Democrats Hilary Clinton has far from the best record in the realms of cybersecurity. She has attracted widespread criticism for using a private email server for her official business as secretary of state, at a White House report released earlier this year showed her tenure between 2009 and 2013 made for one of the worst records of any agency at the time in protecting the Government's computer networks.

Could Hillary Clinton be the First Lady President?

But the bookie's favourite has listed cyber-attacks as a key battle in the country's future. In her campaign pledges, Clinton said they will have "profound consequences for our economy and our national security" and has promised to continue Obama's work, linking the private and public sector to overcome "the mistrust" that exists between the two groups today and build resilience together.

"Our country will outpace this rapidly changing threat, maintain strong protections against unwarranted Government or corporate surveillance, and ensure American companies are the most competitive in the world," she added.

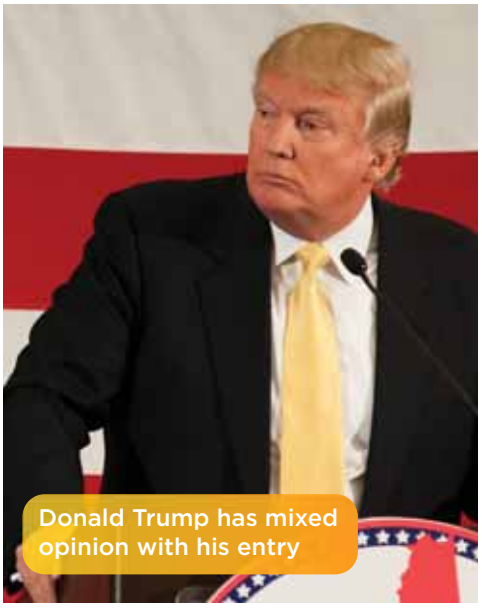
Martin O'Malley, the former governor of Maryland, has also worked as an advisor to the department of homeland security and believes protecting the country is "the foremost responsibility of those in public service."

His policy calls for an "urgently needed new agenda" for the fights on "digital battlefields", again backing the work between Government and businesses, but also calling for more investment into more resources to continue the fight and for every segment of Government to get involved, even "tapping the skillsets of civilians" who may be able to help.

The most left-wing of the candidates, state senator Bernie Sanders, has called for $10bn a year as part of his "Rebuild America Act" to modernise the country's "aging electrical grid," which he believes will "address critical vulnerabilities to cyber-attacks."


John McAfee will represent technology and libertarian interests

The Republicans aren't exactly showered with glory when it comes to knowledge of cybersecurity. Surprise front runner for the nomination, businessman and TV star Donald Trump, seems to think a conversation with Bill Gates will allow him to "switch off the internet" to protect the country from these complex issues.


Donald Trump has mixed opinion with his entry

In his campaign, he has particularly spoken about the threat of China to the US's intellectual property and accused the country of allowing "cyber lawlessness" to threaten prosperity, privacy and national security.

Trump added: "We will enforce stronger protections against Chinese hackers and counterfeit goods and our responses to Chinese theft will be swift, robust, and unequivocal."

US senator Ted Cruz is currently polling in second place—although still with half the points of Trump. Like most of his fellow runners, he hasn't made a huge amount of noise over cybersecurity. But he was the only Republican candidate to vote in favour of the USA Freedom Act, which stops the NSA from collecting most landline telephone records in the country and makes it get a court order to retrieve them from providers.

He said the act "strikes the right balance between protecting our privacy rights and our national security interests." But third place state senator Marco Rubio has made "defending free enterprise and a free internet" a key pledge. His policy says he wants to stop the web being "smothered" by regulation, whilst strengthening cybersecurity in the US.

Like the Democrat candidates, he backs sharing between private and public sector organisations. But he also wants to "use American power to respond harshly to international cyber-attacks on American citizens, businesses, and Governments."

Then, of course, there is the Libertarian Party candidate John McAfee. The man responsible for one of the world's most well-known security companies can surely be trusted when it comes to knowledge of both the industry and the tools needed to protect the public.

But it is unlikely such a figure would inspire people to regard him for his talents, but more likely his controversy, be it his alleged involvement in an unsolved murder in Belize or his thoughts on psychedelic drugs in the work place.

What does Silicon Valley think?

From the depths of California through to the innovations in Massachusetts, it is clear from the stance of most candidates that technology businesses will play a big role in the future of cybersecurity policy, whoever wins the vote in 2016.

But it is the big wigs of Silicon Valley that will not only have an influence but be needed for the White House to tackle the incoming threats.

Duncan Brown, security analyst at IDC, said it was already making a difference. "It is already substantial in this race," he said. "The main players like Symantec and Microsoft already lobby on cybersecurity.

"Importantly, cybersecurity is intrinsically tied up with the privacy debate. This centres on a fundamental balance between an emphasis on cybersecurity which enables privacy, and an emphasis on national security, which favours interception of electronic communications.

"This debate often gets in the way of generally improving cybersecurity practice. Silicon Valley firms need to focus on this practice angle, but often get dragged back into the privacy debate."

There will also be a lot of funding coming from the big firms, whichever side they decide to support. Mike Janke, chairman of

Silent Circle, believes it will be up to the parties to win them over. "I believe it will play a significant role for sure," he said. "Not just the financial side for campaign funds, but most certainly on the voting side.

"Whoever can appeal to the issue that Silicon Valley highlights, will have significant support."

The international stage

But it will not just be home-grown experts that will play their part in the US's future cybersecurity battle. Mikko Hypponen, chief research officer at F-Secure, said it will be as important working with people overseas to tackle the incoming threat as those at home.

"Protecting the internet cannot be done without international cooperation," he said. "The next leader of the White House will have to address some important political and military questions.

"For example, it's typical that online attacks are rerouted through various countries to make it harder to locate the attacker's origin. This means it will be important to work with other countries in combating these attacks.

"Moreover, because laws differ from country to country, cooperative enforcement of laws will be crucial. The question is which of the candidates is best suited for this?"

IDC's Brown added: "Cyber-threats are global and so all countries have to work with each other. Cyber-criminals don't care which country they attack: they'll just go after the rich (or easy) targets."

The future

The fact is, whoever wins in 2016 will be faced with cyber-threats. With Gartner predicting 6.8 billion connected devices to be in the hands of people next year—30 percent more than in 2015—these moving targets will continue to be infiltrated and see attacks spread further and wider than ever before.

In McAfee Labs' threat predictions report for the next 12 months, senior vice president Vincent Weafer said this increased surface, more sophistication from attackers, a lack of integrated security technologies and the shortage of skills to "fight back" will all play out.

"The value of stored and in-transit information is rising rapidly, fuelling new markets, creating a need for securely connecting devices, delivering trusted data to the cloud, and deriving value through analytics," he said.

"But, like anything of value, information is also attracting the attention of adversaries looking for new ways to steal it, leverage it, and benefit from it. Although people often think of organised crime and other criminals, potential adversaries also include hacktivists, nation-states and others not necessarily seeking direct financial gain.

"As we look ahead to the personalisation and consumerisation of cyber-attacks, adversaries may also include a competitor, political opponent, spouse, neighbour, or other personal nemesis, as well as the rising activity of chaotic actors who just want to see things burn."

There are some positives from the report. Claims that passwords will finally become a thing of the past, with more secure authenticating systems coming into play, and people will have a stronger understanding of the need for personal security, as well as getting how valuable their data is.

But this won't stop attempts on the US, be it hacktivism, ransomware, cloud breaches or cyber-espionage to name a few.

> We will enforce stronger protections against Chinese hackers and counterfeit goods and our responses to Chinese theft will be swift, robust, and unequivocal
>
> Donald Trump

Clive Longbottom, founder of analyst firm Quocirca, said the terror threat will be the biggest for the next president. "A new President has to look at changing the old mindsets when it comes to defence," he said. "Although Russia is unstable, it is not a major threat at the moment. Terrorism is by far the biggest threat to the world's peace, and this isn't going to be beaten by nuclear warheads backed by massive aircraft carriers and ground troops.

"The terrorists are way ahead of Governments in their use of cyber-capabilities—and this is where such a new 'war' has to be fought. "Alongside this is the big economic threat of Government-sponsored crime—whether this be through the hacking of organisations for intellectual property or the blocking of sites through DDoS attacks to make life difficult for companies.

"Therefore, there is a massive need for a lot more cyber-specialists in the US (and elsewhere) who can work in the new big data world to better identify what's happening before it becomes a real problem in the real world."

So be it Clinton, Trump, or even McAfee, the new president will need to take the threat seriously and work with all walks of life, nationally and internationally, to protect their country—as well as winning Silicon Valley over. It is no small task.

FOLLOW US ONLINE

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

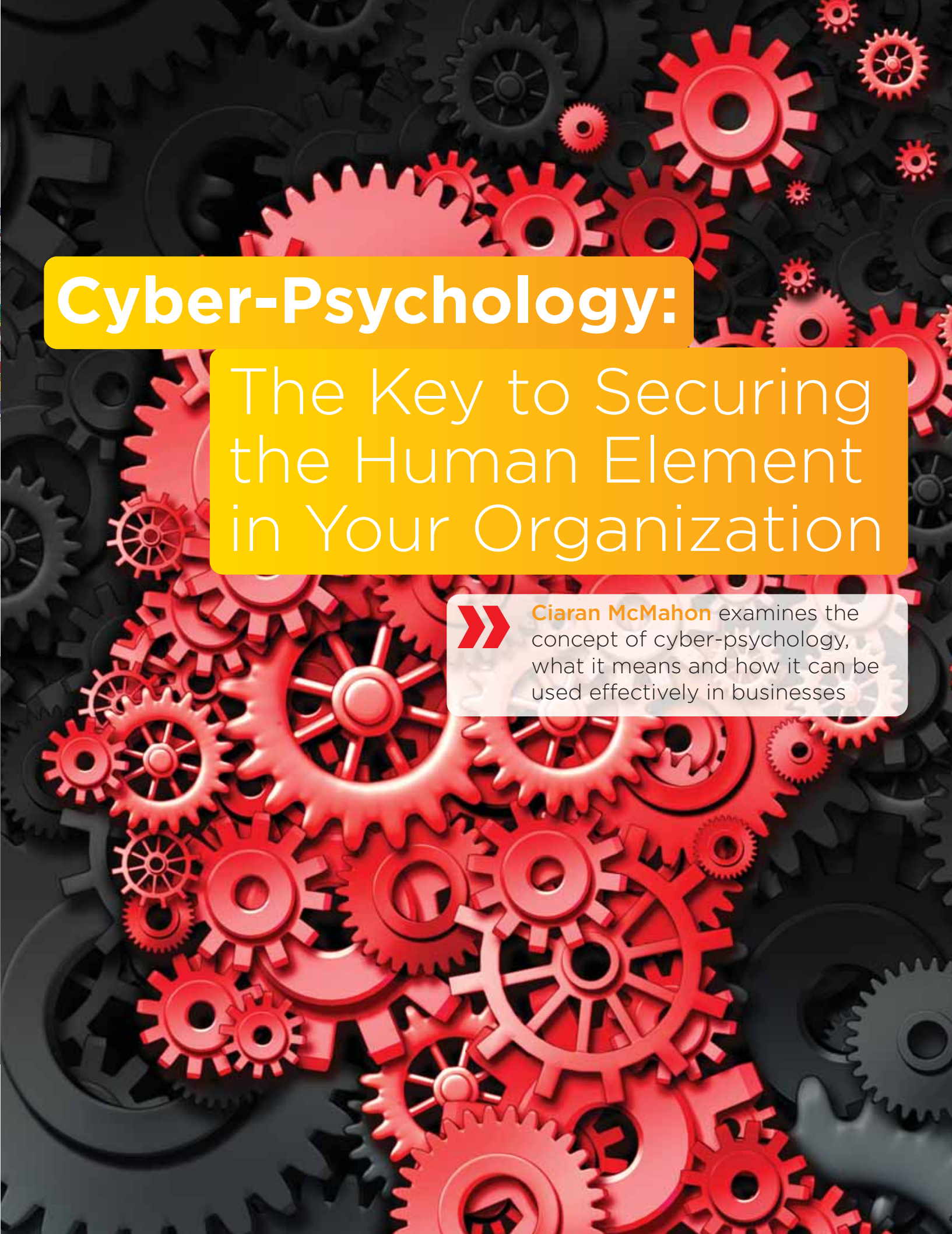
TWITTER: **@INFOSECURITYMAG**

LINKEDIN: **INFOSECURITY MAGAZINE**

FACEBOOK: **INFOSECURITY MAGAZINE**

GOOGLE+: **INFOSECURITY MAGAZINE**

WWW.INFOSECURITY-MAGAZINE.COM



Cyber-Psychology:

The Key to Securing the Human Element in Your Organization

Ciaran McMahon examines the concept of cyber-psychology, what it means and how it can be used effectively in businesses

Since Kevin Mitnick said it in 2002, we have been regularly told that the human element is the weakest link in information security.

The statistics around behavior, policy and awareness are shocking. According to Databarracks' Data Health Check 2015 survey of UK IT professionals, 24% reported human error as a source of data loss in the previous year, while Protiviti's 2015 IT Security and Privacy Survey reports that 33% of companies in North America have no policies for information security.

Overall, this is an insecure environment, to put it mildly. With some lessons in cyber-psychology, the human element can be transformed from information security's weakest link to its keystone.

What exactly is Cyber-Psychology?

Cyber-psychology as a discipline is concerned with the interaction of the mind and behavior with various forms of information communication technology. Not only email, the internet and social media, but also virtual reality, gaming and smart devices.

In practice, what this boils down to is understanding how people experience technology. Here's an example. Your co-worker has a new haircut. It might be nice to compliment them. You could mention it in the office. You could send them a text message. You could write on their Facebook profile. You could even leave a note on the windscreen of their car!

From data perspective, in each case you would have transmitted the same content. But understanding the connotations of different communication media, and choosing the most appropriate one, is the essence of cyber-psychology.

In functional terms for security professionals, consider policy compliance. Let's say there's been a change to your organization's policy. What is the best way to communicate this? More often than not, this will be done by email, but is this really the most effective method? Like, if you really want people to change their behavior, is sending a whole staff mail the best way to effect change? The **medium is the message** is the first lesson in cyber-psychology.

But the second lesson is equally important. To go back to the note on the windscreen on the car idea, you could equally say that your choice of medium depends on who you are communicating with, and you'd be right. Psychology is concerned with the rich variety in human behavior and as such, cyber-psychology is about appreciating that in the context of information technology.

To have resilient security practices, we need to have compliance from the CEO to the temp contractor. As such, cyber-psychology means going beyond the 'end user', to appreciating that real people differ by age, gender, experience, personality, culture, and of course, salary.

Cyber-psychology also involves appreciating that what happens on the internet is somewhat different to what happens 'in real life', but also that what happens on the internet is real life too—a few classic concepts will illustrate the point.

First, the internet is designed to make communication effortless, so we should feel totally immersed in it. This is what is known as **telepresence**. Your average employee is likely unaware of the vast amount of calculations required to allow them log onto work email from their smartphone via public wifi. That's job well done for the engineers, but it represents a significant job of work for the CISO.

Because employees are oblivious to the systems behind the illusion, they are don't know how risky it could be. Cybersecurity awareness necessitates breaking the illusion of telepresence.

Second, anywhere up to 90% of the visitors to any online forum will read but not participate to any noticeable degree. This is **lurking**. Consequently, when an employee is on an enterprise system, unless someone is interacting with them, they assume they are invisible. This is where insider threats slip up—they don't think anyone is watching. But for the CISO the question is how much visibility they have of their internal network. Cybersecurity management requires sight of what is assumed to be invisible.

Third, in the traditional philosophy of the internet, everyone is equal, and there is no central control. This is known as **minimization of status**. It is almost impossible to get people on the internet to do anything through authority: they will simply resist for sheer entertainment value, if nothing else.

Key example: no PR hashtag campaign has succeeded without being hijacked. The upshot of this is that attempting to consolidate discipline within an information technology context is difficult. Cybersecurity compliance requires controlling that which was designed to resist authority.

What are the advantages of it in today's business environment and why is it needed?

There are solutions to these problems. A cyber-psychology-informed information security management process would represent a significant boon in tackling the human element. What would it look like? It would comprise at least the following three essential elements:-

- **Emotional persuasion** – we need more hearts and minds, less fear and conformity. This is about regular, varied and ongoing education. People, unlike machines, do not often change behavior in line with logical information: they need PR and propaganda. The information security team needs to make friends with the human resources and people ops teams.
- **Distributed leadership** – allow teams to develop their own individual policies. Just because you can't have centralized control, doesn't mean you can't have control. Delegate information security decisions downward and outward to create independent modules of resilience.
- **Network citizenship** – CISOs want total visibility of internal networks. But in practice this is impossible, so get your network members to help. Besides being engaged with information security, they will also need straightforward reporting mechanisms.

What are the likely challenges in seeing it rolled out among firms—are there any vertical industries in which it is needed most/be more readily adopted?

The major psychological problem in cybersecurity circles right now is excessive hype, which is heavily fear-focused. Consequently, users resort to neutralization:

A cyber-psychology-informed information security management process would represent a significant boon in tackling the human element

blocking out messaging and pretending it doesn't matter, when they should be engaging with information security and talking about it openly.

Inevitably there will be challenges to rolling out such cyber-psychology-informed policy. The 'sheep dip' model of awareness (half a day once a year for all staff) ticks the box for many line managers. As we know, this model is not going to have much effect on workplace culture. No matter how good the half-day is, it can be easily undone by one senior member of staff soon after being seen to circumvent new policy. Monkey see, monkey do—then everyone else will simply continue on as normal.

Anything more than the sheep-dip would be to admit that there is a bigger problem. However, cyber-psychology teaches us that in such instances, there probably is a bigger organizational problem at play.

Conway's law, a curious software design principle from the 1960s, states that organizations which design systems inevitably end up making systems which look like their own internal communication systems. You will probably end up with a security policy which reflects your organization's communications structure.

Consequently, if your organization's internal communications structure is malfunctioning then your information security policy will show this and similarly malfunction. It is worthwhile stressing this at senior level: if your information security policy is poor, it reflects poorly on your corporate structure.

What are the direct benefits of adopting a cyber-psychology-informed policy and how can these be articulated across your organization?

The 'human element' of information security was also mentioned in last year's Europol IOCTA report, which noted an increasingly more aggressive and confrontational cybercrime environment. The only way forward in such an environment is for greater collaborative efforts, more horizontally across sectors and more bottom-up within corporate structures.

Businesses which are capable of aligning their corporate goals with their information security policies are most likely to succeed through the next decade. Industries in which this is most likely to succeed are naturally the technology, telecoms, financial and media sectors. Although any organization which is committed to original thinking will see the value in developing an information security culture like I've outlined above.

Thanks to several high-profile breaches, 'we take security very seriously' was the top meaningless cliché of 2015. It will not hold water for much longer—the public and their representatives will soon start asking for better data integrity practices.

What does security mean in daily working life? The organizations which manage to instill in their employees the importance of information security: that they have taken serious educational steps to address information security will have a significant edge in time to come, as it is clear that cybercrime continues to be profitable.

Fundamentally, information security culture will become a part of an organization's demonstrated commitment to corporate social responsibility—along with issues like human rights, environmental responsibility and community development.

Trust who you are online with

Big Data identity platforms and social media have gone some way to improving online identity, but is the internet forever catching up with its users? **Wendy M. Grossman** looks at the successes and stories

When Jamie Bartlett, a researcher at the Demos think tank, was writing his 2013 book, *The Dark Net*, one of his biggest surprises was discovering that the best customer service in the world was to be found on the Silk Road site. Despite—or perhaps because of—the questionable legality of many of the site's offerings, the reputation and ratings system kept the site's sellers competing to please and provide meticulous information about the quality of their offerings.

Until the Feds came along and shut the thing down, these sellers were, in Bartlett's account, more trusted by their customers than many big brands are. The site arguably proves what many have contended since the dawn of the internet: reputation can be established without binding it to a real-world identity.

To explain the trust at Silk Road, "Directories automate discovery," Don Thibeau, the founder of the Open Identity Exchange (OIX), said at the early December 2015 Personal Information Economy conference (PIE 2015), run by the specialist consultancy Ctrl-Shift.

"Registries build trust through transparency." His prime example was Lloyd's, which operated an underwriting register anyone could use as long as they agreed to the terms and conditions. But, "There is no global registry for trusted identity systems." It's this that OIX, a cross-sector, technology-agnostic non-profit, is trying to build. "We have to look at every tool to increase trust".

The basic problem is that the internet was built, famously, without an identity layer. That is, its design includes no way for anyone to know with certainty what or with whom they are connecting. For applications such as publishing it doesn't really matter. But the lack of that identity layer is a crucial problem in digitizing government and financial services, and it's the cause of many of today's security problems.

As Kim Cameron, the identity architect for Microsoft, wrote in his widely cited 2005 paper, "Seven Laws of Identity", the systems we all use today are workarounds, a result he called "pernicious". The result: the internet is a vector for criminals because we have no way to evaluate when a site can be trusted or when we're sending personal information to the wrong people.

Cameron's ideas were implemented in Vista and Windows 7 as Cardspace, an effort Cameron now calls "disastrous", though "a technical triumph". Since 2005, large companies like Facebook and Google have geared up to offer the identities consumers have built up on those services as a federated identity for everything. But would you want to use your Facebook account as your login to pay your income tax?

> There is no global registry for trusted identity systems. We have to look at every tool to increase trust
>
> Don Thibeau
> OIX

That approach—a centralized identity provider who ultimately gets to know everything about you—has been the dominant model for the last 20 years. The structure optimises the amount of data organizations can collect about their customers, thereby maximizing both the risk to customers when there are data breaches and the potential for privacy intrusion by the organizations themselves.

As David Evans, the BCS membership director, put it at PIE: "We're creating a world where moral, well-intentioned people can't achieve their business objectives without doing things they're uncomfortable with."

Ideas for alternatives are as old as the commercial internet; even in the early 1990s cryptography experts like Carl Ellison were suggesting using encryption techniques to separate roles and provide only the minimum information necessary to validate a transaction.

A bar owner, for example, doesn't really need to know the identity of the young-looking person who just ordered a beer, just to verify they're over legal drinking age. Today's standard approach, however, has you showing ID that gives your name, address and birth date, with little recourse if the bar insists on scanning the ID and keeping a copy.

Alan Mitchell, co-founder and strategy director of Ctrl-Shift, points out how much extra risk this structure creates for all concerned. "One of the key points we're saying," he says of his company, which aims to assist companies navigate a digital economy in which the audience is in control, "is that the problem with the current way that data collection is structured is that it creates honeypots of data which encourage hackers because the data is in large, centralized databases. On top of that, there's been a culture of not really seeing data security as being important."

The fact that until recently so many companies (Ashley Madison may be an exception—and a turning point) survived data breaches with little apparent damage has fed a certain complacency. Even Target, which in March agreed to pay the victims of its 2013 hack $10 million, and replaced its CEO, still fills its stores with shoppers.

The result, Mitchell suggests, has been to breed a culture of arrogance, in which many companies focus their efforts on grudging, minimal compliance with the law. But, "when a brand or company's entire reputation is on the line they make sure they get it right," he says. "So, for example,

flying a plane from here to NYC is far more difficult than keeping data secure—and yet they manage to get that right virtually all the time. And the reason that they get it right there is because it's a number one priority to make sure it's safe."

Cameron's "laws" were not so much rules as observations of the successes and failures of attempts at digital identity systems. More recent data breaches such as Sony and Target have proven his contention in explaining law number two, "minimal disclosure for a constrained use", that "we should build systems that employ identifying information on the basis that a breach is always possible.

"Storing just a flag that says a user is 'over-18' instead of a birth date, for example, is much less helpful to identity fraudsters. Ten years on, he believes the laws he outlined were all correct but incomplete: they failed to incorporate power dynamics.

"What I learned was wrong with the laws of identity," Cameron says now, "was that they didn't take into account the privileged position of the service provider, the relying party." Going forward with what the industry has begun to call "me2c" will require an identity solution that both relying parties and consumers are willing to embrace.

"You can have as many as you want—it doesn't matter what the movement is coming up with unless service providers adopt it." There are, Cameron says, a number of consequences for how the necessary technologies should be built, but he sums up the most important lesson this way: "We have to build technology for the relying parties in which we simply enable privacy, security, me2b [me to business], and so on."

Newer identity systems being implemented now such as the UK Government's Verify, a product of the Government Digital Service, have three elements: a consumer; an identity provider; and a relying party.

The element that needs to be verified, whether it's an address, an age group, or the existence of a license to drive, is an attribute. So, say an individual is applying for a free pass for public transport that has two requirements: 1) applicants must be over 60; 2) they must live in a specific catchment area. Both of these are "attributes" to be checked; the relying party in this case is the issuer of the free pass.

In that scenario, the identity provider acts as an intermediary: checking the proofs that the individual has the claimed attributes and passing on verification that they exist—but not the proofs themselves. Trust is key all along this chain: both consumers and relying parties must be able to trust that the identity provider has done its job correctly.

But it limits any one party's visibility, since identity providers know only which services it has helped a given consumer access but not what they've done with them or via another identity provider, and consumers' personal data is exposed only to the identity provider.

One of the early implementations of these ideas is the UK government's Verify, now in public beta and created under the aegis of the Government Digital Service, formed in 2011 to transform the provision of public services. Verify aims to create a marketplace of multiple identity providers, offering people the option of using different providers for different uses.

The system should both avoid the creation of huge honeypots of data for criminals to target, or vulnerabilities to expose while giving consumers more genuine control over how and where they give consent for the use of their data.

> What I learned was wrong with the laws of identity, was that they didn't take into account the privileged position of the service provider, the relying part
>
> Kim Cameron

The key to make this structure succeed, says Tom Loosemore, GDS's founder and the leader of Gov.UK for its first five years, is relentless focus on the user. At GDS, Loosemore's goal was to create Government as a platform, an effort to build a new public infrastructure that he compares to the 1850s effort to build a sewage system to improve sanitation and public health.

"In our time," he said at PIE 2015, "that public infrastructure is made of data." The reinvented infrastructure should mean that someone wanting to start a business could do it in three minutes rather than months spent chasing paperwork, while simultaneously protecting citizens from "themselves, others, and Governments".

Sequestered inside a company—or, perhaps even more so, a Government department - it's easy to lose touch with who users actually are. On an in-house corkboard, GDS staff have a photo with a Post-It note saying "our users". It points to a picture of people in an ordinary street scene, meant to serve as a constant reminder of who government services are meant to be designed for and who has to navigate the jargon language and complex, opaque infrastructure that are obvious to insiders.

Says Loosemore, "The most important generator of trust is speaking human."

SITS 16

THE **SERVICE DESK & IT SUPPORT** SHOW

8-9 JUNE 2016
OLYMPIA, LONDON

FREE to attend

The essential event for **Service Desk & IT Support Professionals**

- **Connect** with industry thought leaders & solution providers
- **Learn** from over 50 FREE must attend seminars & keynotes
- **Join** over 4,000 like-minded IT Service professionals

EXHIBITION | SEMINARS | EXPERT ADVICE | KEYNOTES | NETWORKING | CASE STUDIES

REGISTER FOR **FREE** ENTRY

Quote priority code **SDS101** and save £35 on the day!

www.**ServiceDeskShow**.com

Sponsored by SDI Service Desk Institute

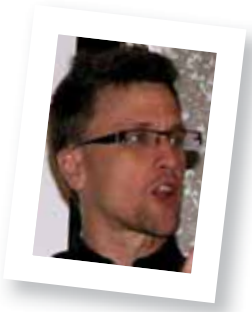
Supported by itSMF UK The IT Service Management Forum

In partnership with SITS COMMUNITY NEWS | COMMENT | DEBATE 360 *The Voice of the Service Desk industry*

SITScommunity360.com

Securing the Human to be Mightier than the Computer

Having written about and presented on the best ways to secure the human, SANS Institute certified instructor **Lance Spitzner** identifies the key ways for your staff to be your best ally in security



People, not technology, are becoming the key to securing organizations today. For years organizations have invested in technology such as anti-virus, firewalls, full disk encryption or data loss prevention.

While powerful, solutions like these fail to secure one key element, people. Until organizations also address the human element, cyber-attackers will continue to easily hack into organizations.

The reason for this is simple, cyber-attackers take the path of least resistance and in today's world that means people. Organizations have become very good at securing technology but very bad at securing their own employees. As a result, cyber-attackers are bypassing technology using methods such as phishing, targeted phone calls, attacks through social media or any other communication means.

Ultimately the result is the same. Cyber-attackers are hacking into organizations by tricking or fooling their employees into doing something they should not do.

The solution is simple, just as organizations have invested in securing their technology, they also need to invest in securing their people. To do that they need to secure peoples' behaviors, and ultimately create a secure culture.

However this cannot be done simply by purchasing a product. To create secure behaviors, and ultimately a secure culture, organizations need to establish a long-term security awareness program. Such a program engages employees, explains to them why cybersecurity is important, and walks them through the behaviors they need to exhibit, to include protecting themselves both at work and at home.

While there are challenges establishing such a program, organizations around the world are taking this step and seeing a huge return on investment. For example, we are seeing organizations reduce the number of employees that fall victim to phishing less than 5%, and those that do fall victim quickly realize and report it.

The first challenge for many organizations is making their security awareness program stick. Engaging people and teaching them about new, secure behaviors is easy, but having those lessons stick long-term and have an impact is more challenging.

The first step to effectively changing behavior is understanding what elements make up a behavior. According to the BJ Fogg Behavior Model developed at the Persuasive Tech Lab at Stanford University, there are three key elements to a behavior: people must be motivated to exhibit the behavior; they must have the ability to exhibit the behavior; and they need a trigger or prompt to know when to exhibit the behavior.

The key this model teaches us is the more motivated people are to change behavior, and the easier we make the new behavior happen, the more likely we will have an impact.

To do that we must effectively communicate to people, first by answering the question why cybersecurity is important to them, why should they care? To do that you must reach people at an emotional level, trying to rationalize security with statistics or numbers will not have a long term impact.

To reach people emotionally, explain to them that what they will learn not only applies to work but to their personal lives. We all use the same technology at both home and at work, and we face the same risks in both locations.

By teaching people how to secure themselves personally, not only are they more likely to listen and change behaviors, but security becomes part of their DNA. As a result, not only are employees personally benefiting but the organization also benefits. In addition, this personal approach is

becoming even more important as peoples' personal lives and work lives are beginning to blend, such as with working at home or BYOD (Bring Your Own Device).

Secondly, we have to communicate this message in a method people want to consume. Different generations, cultures and even individuals learn differently than others. As a result, organizations need to communicate their awareness program using multiple methods.

For example, more conservative individuals or older generations often prefer traditional methods of communications, such as in person training or newsletters. They also prefer to learn during work hours and have the content be more professional or subdued. Outgoing individuals or younger generations usually prefer the latest technologies for learning, such as using tablets, online videos, or social media. They also want the flexibility to learn on their own schedule and like the use of humor, such as memes. By understanding your different target audiences and adjusting how you communicate to those audiences, the greater your impact.

Once you begin communicating your program, you then have to measure its impact. For security awareness there are two types of metrics: compliance metrics and impact metrics. Compliance metrics are measurements that auditors want to see, they measure the distribution of your program, such as how many people took the online training or how many newsletters were published that year.

> Until organizations address the human element, cyber-attackers will continue to easily hack into organizations

While important, what we want to know is if that training is having an impact, are we changing behaviors, are we reducing risk? These are what I call impact metrics. There are a couple of key things to keep in mind when measuring behaviors.

The first mistake most organizations make is they forget people have feelings. A computer does not care if or how it is measured, people do. You need to take that into consideration. For example, you never want to embarrass or humiliate people, such as sending out a Viagra phishing email.

Also, never create a wall of shame where you list the names of everyone that failed an assessment. Everyone has a bad day, we all sooner or later most likely fall victim. The only time it may be necessary to report a name of someone who failed an assessment is if they keep failing, are not changing behaviors and as a result represent a high risk to the organization.

Thirdly, measure your highest human risks. These are easy to measure, and are metrics you can act on. Phishing is a common metric that many organizations use. Phishing is one of the most common human risks most organizations face, it is easy to measure as you simply send out a phishing email every month as part of your assessment, it is actionable as you can identify your most vulnerable people and measure if your training is having an impact.

If a metric measures a low human risk, or a behavior you cannot do anything about, then it does not have much value. Ultimately start with only one or two metrics that are high value.

Finally, when it comes to metrics, make heroes out of the people who start exhibiting the correct behaviors. Recognition is an extremely powerful motivator. Also, by highlighting people who did the right thing you are reinforcing the key behaviors you want people to follow. As people see their behaviors are having a positive impact, not only will they continue to exhibit those secure behaviors, but their attitudes and perceptions to security begin to change. Now you are going beyond just securing behaviors, but creating a secure culture.

People are one of the best defenses your organization can have; unfortunately, they are also one of the most commonly overlooked. It's far too easy to fall into the trap of simply purchasing the latest technology and thinking all of your security problems will go away. By investing in and securing your employees, you will have a long term impact that will benefit not only your organization, but also your people.

The first challenge for many organizations is making their security awareness program stick

Keeping Software Defined Data Centers Secure

Max Cooter looks at the concept of a software defined data center, and if this will put those "how secure is the cloud" debates to bed once and for all

> Institutions are really at the heart, dealing with the complexity of that environment by using automation and templates as the traditional approach to security doesn't scale into the software defined data center
>
> Graham Brown
> Gyrocom

Anyone who has been paying attention to current thought around data center design will be aware of the increasing trend towards a software defined data center (SDDC). It mirrors the growing implementation of software-defined networks (SDN) and follows on from the widespread acceptance of cloud computing and virtualized servers.

What are the risks of deploying such a data center?

In the same way that cloud was, initially at least, seen as insecure, does running an SDDC mean that an organization is more at risk? It is important to state that the point of deploying SDDC is to increase security. Yet according to a recent *Infosecurity* magazine webinar, 55% of respondents had no plans to implement a software-defined data center at any point in the future.

VMware's security and compliance specialist, Peter Bury, says he can understand the reasoning behind this. "There's a tendency to look at SDDC as a zero sum game," he argues. In other words, companies take all the aspects of an SDDC and think that everything has to be implemented at once.

However, Bury explains that the growth of the software-defined data center (and a quarter of the aforementioned webinar viewers had already implemented one) arises from well-established business reasons. He says it's clear why companies are looking to overhaul their data centers. "I'm looking at a world with highly competitive, agile new companies who are able to bring out new products very quickly at a rate that big organizations can't do."

So, many companies are looking at how to broaden the portfolio and react more quickly, and the answer that many come up with is SSDC, but that causes concerns of its own, says Bury. He adds that companies have moved away from a traditional infrastructure to a cloud-based one with little understanding. "A good example is where IT can't move fast enough. In that case, you will find people going to third party providers: just a few seconds with a credit card and a browser, infrastructure and compute can be made available."

Bury proposes that this could cause concerns for CIOs who have no control over that environment, but the people in that organization will point out they need the infrastructure quickly as IT hasn't been able to do that for them.

The reason why they can't bring us to the heart of the problem. "You can try to make that available but you'll have a lot of legacy and processes around security and you won't be sure that you can implement and verify them at the same speed that you can do everything else," he cautions.

"Organizations willingly admit that they have taken security shortcuts just to get a service out to their customers. But can you maintain all the checks, verifications, user interfaces, crawling, patch management that you used to do when you continually stream into a live environment?"

There's a balancing act between speed versus complexity versus security. There are small agile companies who have worked out how to deliver this, but traditionally the view has been that doing things faster and faster is going to lead to operational chaos. This is the underlying fear in the construction of data centers. There is a great deal of complexity, and a fear of that complexity is growing out of control.

"Complexity is the enemy of security," Bury remarks. "The old model was CIA – confidentiality, integrity, availability. It's very easy to get one of those right but hard to get all three correct at the same time."

This brings us to the crux of the matter. The key to designing a software-defined data center therefore is to ensure that security doesn't exist as a separate entity from the compute and storage, but is something built in; part of the same domain. In other words, there's no gap between how the compute is configured and the network and security are configured.

What does this really mean?

A lot of the problems become operational—it's one thing to build a data center and make it secure, it's another thing to continually operate it. If you look at some recent security breaches, Target for example had passed its audit—it was PCI compliant—the problem was the ongoing problem between those audits. This opened up a gap that could be breached.

That brings us on to the second part of the process: automation. "Whether you're taking an open source approach; whether you're taking a vendor-specific or multi-vendor approach: you have to blend together compute, storage, network and security," Bury said.

After that, he says you can start to predefine it. "You can build templates that predefine the compute so why not have objects in that template which predefine the networking and which define the security controls you're going to have?"

In other words, you're not just pre-defining compute but an entire application—not the compute but the network and security around it; and that can give you confidence because you know that anything you create from that when you scale up or down, or create capacity is going to come from that particular blueprint.

Rather than order, build, verify, tune, verify and sign-off each time something needs to be signed off: that process is done beforehand. This can mean that the networking and security is all done beforehand, so you're consuming it with the same operational model as a virtual machine: pre-defined and on-demand.

Bury says that in the world that his VMware customers inhabit, the principle is that as the infrastructure is designed so should networking elements such as switching, routing and load balancing be built in, so companies have consistent, repeatable processes all built around automation. He admits that automation is not an easy concept for his customers to get to grips with, but when you predefine things, you build in security from the outset.

Graham Brown, managing director at Gyrocom, believes that SSDC is a concept that the customers are really getting to grips with, thanks to the flexibility it gives them. "We see [SDDC] going to mission-critical environments. Financial institutions are really at the heart, dealing with the complexity of that environment by using automation and templates as the traditional approach to security doesn't scale into the software defined data center."

He adds that the growing increase on workload volumes was showing the limitations of the traditional tiered approach. "The firewall boundaries between a web and a database tier, for example, are increasingly difficult to manage and maintain, to troubleshoot in case of difficulties and to audit. And, that method is becoming less and less viable."

In such circumstances, automating compute and storage, without automating network and security, defeats the object. "It's only when you put all of these together that the true value of automating a data center becomes a reality," says Brown.

It's not a decision companies should shrink from as workloads increase. "We're already entering a world where data center complexity is already being far beyond human scale" says Brown. "Without throwing huge amounts of resources, then the ability to be able to segment that security problem is absolutely critical for us. The only way to achieve this at scale is through automation."

The rolling out of software-defined data centers will ultimately mean far more security. "We will have the ability to deploy a firewall to secure every conversation, something that hasn't been possible up till now.

It's like the old example of castle versus a hotel. A castle has a big lock but once you break it, you're in. While the hotel has a security lock on every door," says Brown. "And what's more, every hotel room can be different."

Case Study – Financial Institution

Graham Brown describes how one of Gyrocom's customers moved away from the traditional data center set-up.

"As a financial institution, security was paramount. When we first talked to them they were about to upgrade to a traditional architecture. The company wanted a complete infrastructure refresh for the delivery of financial products through bespoke web-based applications.

"We were able to show how a software-defined approach offered advantages over the traditional way of doing things. We implemented VMware's NSX within four weeks. We introduced consolidation, showed there was no need to take on an east/west firewall and ensured every workload was segmented with the correct security policy.

"There were large operational savings but performance also increased as we were able to segment and overlay policies on templates. For example, we could create templates based on Windows "machines", templates based on Linux machines etc. Through the micro-segmentation we could introduce a flatter infrastructure to offer more granular security."

Brown claims that that the company now has a number of key benefits from a software-defined approach: improved security, infrastructure flexibility, simplified processes and reduced cost.

Suffering Security Lag?

Professor **Steve Furnell**, head of the school of School of Computing, Electronics and Mathematics at the University of Plymouth, looks at how security needs to become part an implicit element of our technology culture, and to keep pace with the technology rather than trail behind it

The recent spate of security incidents provides timely evidence that our adoption of technology appears to be outstripping our ability to protect it. If you're wondering which particular incidents this refers to … well, you can probably take your pick.

No matter when you are reading this, there will almost certainly be a completely different set of 'recent incidents' to reflect upon. That, unfortunately, is the problem—the statement has held true for quite some time, and seems likely to continue to do so.

We face a fundamental problem that security practices don't keep pace with the threats. Alas, there is nothing new in this—in fact, many of today's threats can be traced back 20-30 years. However, they didn't pose such a problem back then, and so practices didn't change to address them.

What's changed over time—thanks mainly to the internet—is our exposure, the possible impact, and a more widespread recognition of the need to respond. However, this recognition has been far more gradual than the growth of the problems, and so security is often absent in both the technologies themselves, and in the minds of those developing and using them. While it may follow on eventually, this security lag allows significant windows of exposure.

Unfortunately, we don't have to look far to see evidence of practices not keeping up. For example, in prior research at Plymouth University, we surveyed almost 300 users about security on their personal systems and devices, and discovered that more were actually indicating explicitly bad practice than good practice.

Specifically, while 9% claimed that they chose reasonable passwords, installed updates promptly, and believed they had up-to-date anti-virus protection, 11% fell into the exact opposite group. Meanwhile, the practices amongst the rest were mixed (e.g. behaving well in terms of installing updates, but choosing weak passwords, etc).

Given that none of these were advanced aspects of security, and all could reasonably be expected to be standard elements of IT literate behaviour in this day and age, it is clearly disappointing that less than a tenth of people even claimed to do it properly.

To consider a more specific case, mobile devices offer a classic example of security lag in action. To appreciate this, let's look at a bit of the history in the context of malware risks. A decade or so ago, with basic 2G phones and PDAs, there wasn't a real issue here, aside from some early proof-of-concept cases offering a sign of problems around the corner.

For malware to become a bigger issue, a few conditions needed to be met. First, the devices lacked full networking capabilities—phones had limited internet access, while many of the PDAs lacked connectivity beyond being cabled up to sync with a PC. The second constraint was the inability to install and run code. PDAs could do it, but the earlier phones couldn't. Third, there had to be a sufficient

population of users to make it worthwhile for attackers to divert attention from their traditional Windows-based targets.

So for quite some time, while mobile devices became immensely popular, their limited capabilities and diversity of platforms meant they were largely ignored in terms of malware. As a result, when related concerns were raised, it was easy for them to be dismissed as hype, and few wanted to hear about potential future problems.

Of course, time passed, and all of the preconditions were met, with Android devices in particular now ticking all of the boxes most handsomely. Android's popularity, combined with the openness of its app marketplace (i.e. as opposed to the policing that Apple applies to its App Store) has led to 99% of mobile malware targeting this platform. The scale is still nowhere near that on PCs, but it is real, it exists, and many users now find themselves exposed.

Drawing again upon survey work from Plymouth (this time involving a wider sample of over 1,200 users), we found that while over 90% claimed to have anti-virus protection on desktop devices, only 10% claimed to have it on smartphones (rising to 14% when specifically considering those estimated 700 users that had Android devices).

So, now we have a massive population of users that have become accustomed to using mobile devices without having to worry too much about security, who now need to be re-educated to recognise an issue that they have already accepted in the PC context.

Sticking with mobile devices, some similar comments can be made around authentication. While many users have gradually accepted the need to have some protection here, the method used is still very often the 4-digit PIN. While this may have been perfectly reasonable back in the days of the basic phones that made calls, and only stored text messages and contact details, things are rather different these days.

Is protection via a 4-digit code really commensurate with the apps, services and data on the devices (particularly given that the same content would typically be protected by at least a strong password when being held elsewhere)? Apple's recent update in iOS 9 changed its baseline to 6-digits instead of 4, and while this is clearly progress of a sort, it is certainly not a shift of the same magnitude as the device content.

Despite all the prior experiences, we are still being given technologies that don't offer security until sometime later

So, at the user level, mobile device security still seems optional, and clearly lags behind where it should be. Moreover, it is also falling short in organisations. Indeed, some still kid themselves that they don't have a mobile security issue because they've not given the staff such devices, or they haven't formally sanctioned a BYOD approach. Mobile devices are not even an emerging technology anymore; they are firmly established. As such, any organisation that lacks a policy (or at least a clearly stated position) on their usage has clearly missed something significant!

Looking beyond mobile security, it's easy to cite other examples. For instance, successive security surveys reveal long-term recognition of significant breaches being linked back to (lack of) staff awareness. However, the self-same surveys show little attention towards education and awareness initiatives—the very things that one might consider relevant to addressing the problem. Another good example of lag is around patching latency.

It's well established that exploitation of known vulnerabilities is a significant cause of incidents, and while there are certainly zero-day attacks to worry about, there are many cases in which quicker action would lessen the risk. For example, a recent study from NopSec Labs suggested that it takes an average of 176 days for vulnerabilities to be remediated by organisations in some sectors (compared to an average of 7 days for attackers to build an exploit).

Meanwhile, there are myriad end-user systems that remain open to compromise because updates have not been applied. It is easy to appreciate the viewpoint that such users might be coming from (particularly when dealing with their own personal technologies) because at the system already does what they want, regardless of whether they update it.

So the fact that everything still appears to be working serves to make security look like a choice or an optional extra, rather than a necessity. Of course, the fact that many breaches will not be visible means that this mind-set can persist long after a system has actually been compromised.

Findings from Google from earlier this year revealed that some users actually view updates as a security risk, believing them to be a route by which malicious code might be installed on their system. The fact that there is such a misconception around such a fundamental element of security illustrates just how much distance we need to cover in bringing good practice in line with our desire to use new technology.

Despite all the prior experiences, we are still being given technologies that don't offer security until sometime later. Some of this links back to security being overlooked on the basis of rather casual risk assessment. It is easy to run into the assumption that certain devices won't be attacked because they don't do much, or can't offer much to an attacker, whereas in reality such things have a track record of being exploited simply because they are vulnerable. As with mobile malware, the key point again is that, at this stage, we shouldn't have to be relearning the same lessons.

Unfortunately, but unsurprisingly, there is no magic wand solution. Overcoming the historic lag needs a mixture of action (by developers) and expectation (by the rest of us). We are past the point where systems and devices should be provided proper attention to security, and we ought to be similarly past the point where we would *accept* them.

Managing the Mobile Gap

Stephen Pritchard looks at the problem of mobiles in the enterprise, and will 2016 present any solutions to this consistent problem?

"Mobiles are chaos." This is the unequivocal view of Rob Smith, a research director at Gartner and a longtime observer of the mobile landscape.

"The frequency of updates is unparalleled. There have been 14 versions of iOS in the past year. And if you look at apps, every app update is a new app, every OS update is a new OS. And there are undocumented features with every update."

This contrasts to the more staid and predictable world of personal computers, with its regular rhythm of patches and updates, and OS upgrades that come along just every few years. Phone buyers, by way of contrast, change devices every one to two years, and are motivated mostly by cost.

Mobile devices, though, are essential to business. Gartner, for example, says that 320m PCs were sold in 2015, against 206m smartphones and tablets. The research firm says that over half of households will own a tablet by 2016 across mature markets. In some countries, the figures are already higher: Ofcom, the UK's telecoms regulator, expects three quarters of households to own a tablet at some point during 2016.

The impact on business is clear. Companies need to embrace mobile technology, but many enterprises are only just starting to consider what it means for security.

"We've seen pressure being put on CIOs to ensure a mobile offer. Senior executives have become very used to mobile working themselves, and CIOs see it as a positive direction," says John Skipper, cybersecurity expert at PA consulting, an advisory firm.

"Companies should step back and balance risk and benefits, as with any other technology decision. Because mobile is so ubiquitous, we often don't think of it in that way."

This ubiquity raises risks, including the loss of corporate data and potentially, mobile devices acting as a path for malware into organizations.

Despite this, the real threat posed by mobile devices is less than clear. The vast growth in mobile use has not, for example, led to an equal increase in mobile malware incidents. Although researchers have been uncovering examples of mobile malware since the 1990s, there have not been the large-scale virus outbreaks that have affected PCs. Even so, Verizon, the cellular network, estimates that tens of millions of devices are being compromised every week, most of them on the Android platform.

"Infection rates could be around one percent, up there at the level with PCs," says

PA Consulting's John Skipper. "But the level of danger is may be lower. The top five malware items are targeting the local device, trying to compromise the individual."

This targeting is being driven, experts say, by financial crime and especially by a desire to compromise online banking and other, personal financial transactions.

"There is malware, botnets and other malicious material out there on mobile devices, but so far the volume and scope of the attacks is far less than we have seen targeting traditional desktop platforms," explains George McBride, vice president of the security science practice at Stroz Friedberg.

"But, the infection rates of mobile devices continue to rise with a significant number of attacks targeting users of financial services."

The hidden risks of mobile

One reason is that the mobile world's diversity—both in hardware and operating systems—has, so far, given it some protection against malware writers. Even though the number of mobile operating systems has fallen over the last few years—and could fall further, with brands such as BlackBerry moving to Android - the PC environment remains far more homogenous.

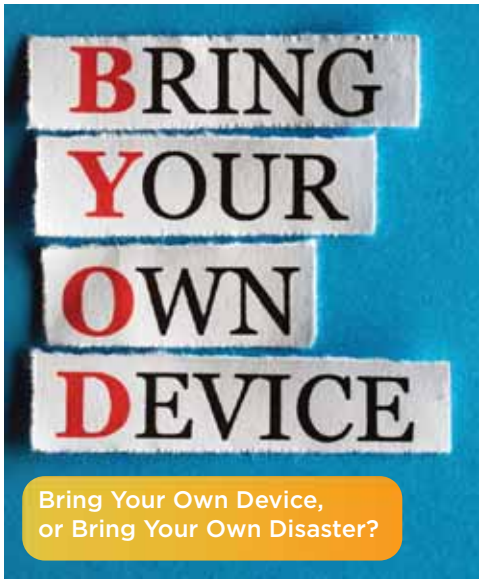
"It is much easier to email malware and run it on the PC, rather than jailbreak or root a phone. [For the hacker] it's an ROI discussion. It is easier to get into an average corporate network, than an individual device," say Gartner's Rob Smith.

"There is a greater barrier to entry for potential hackers of mobile devices," agrees Stroz Friedberg's McBride. "It is significantly easier to create malware on and for a PC, than it is for a smartphone or tablet.

"This barrier will continue to erode as toolkits and materials become available to help hackers develop their own malware; and the number of sources of custom developed malware continues to rise.

"But malware writers and hackers want to attack platforms with the greatest footprint. With more and more users using mobile devices such as phones as tablets as their primary computing device, the threats of malware on mobile devices can only go up."

This, then, is the dilemma facing corporate users of mobile devices. As devices become more powerful, and more widespread, so they become more attractive targets to hackers.



Bring Your Own Device, or Bring Your Own Disaster?

Threats on the move

The fact that attacks against mobile devices have, so far, been limited is no reason for complacency, however. As companies access, transfer and even store more key data on mobile devices, the potential damage from targeted attacks increase, as do the risks of hacking groups developing platform-wide malware.

At the corporate level, threats are more likely to be around data theft and data exfiltration than the use of mobile devices to launch large-scale attacks against networks or systems.

"In the immediate future, I don't think we will see mobile devices used as vectors in big denial of service attacks as we see with desktops," suggests Stroz Friedberg's McBride.

Spyware, or possibly ransomware, are viewed as greater risks, as are targeted attacks that go after individuals with access to high-level data, suggests McBride.

Ultimately, the use of personal mobile devices remains a risk, because they are personal.

"Personal devices are a risk to corporates," cautions Doug Davidson, CTO for cybersecurity at IT firm CapGemini. A move by companies away from "bring your own device" policies, and towards greater use of company-owned devices, especially for sensitive data and applications, can reduce the risk.

> You have to accept risk, it's about degrees of risk. Even with the strongest security measures on iOS and Android, you can't guarantee data is safe
>
> Rob Smith
> Gartner

But it is still vital that organisations, before they look at granting mobile access to core applications and data, understand exactly what they are doing. This should, Davidson says, be part of a wider, strategic approach to mobility.

"You need to go back to the basics," he says. "What type of mobile devices are being demanded by the business? What are current and future mobile requirements? What types of data are being transferred? Which are sensitive, and what data are you sharing with third parties?," he asks. Even email has its risks. "People think it is just messaging. It is not, it is information sharing."

As well as targeted attacks, organizations need to be aware of the value of data that might be carried on mobile devices, including personal devices, and the possible penalties and reputational damage that might follow the loss or theft of a device.

For this reason, businesses need a strategy—as well as tactical and technical measures—for managing mobile devices and the applications that connect to them.

Closing the mobile gap

Fortunately, some of the measures organizations can take to protect their mobile users are simple, effective and cheap.

One of the most cost-effective steps is to move towards six or even eight-digit passcodes; this protects devices against hacking kits that can bypass four-digit codes and the "10 tries and wipe" functionality in handsets. It is also a measure that users of personal devices can implement, as it protects their own information too.

Businesses with any number of mobile devices are also likely to run a central mobile device management (MDM) application. MDM applications offer rich functionality, but do need to be kept up to date. Some mobile operating system updates have, in the past, disrupted MDM controls, so CISOs should check this before allowing users to update their devices. But MDM does, for example, allow enterprises to control PIN strength and OS updates, as well as more basic features such as remote lock or wipe.

"Firms should use encryption—many devices encrypt by default—device management tools, and features like activation lock," says David Rogers, CEO of mobile security analysts Copper Horse. "But the single most effective thing we can do is look at software updates—that can protect people from a lot of malicious activity."

> With more and more users using mobile devices such as phones as tablets as their primary computing device, the threats of malware on mobile devices can only go up
>
> George McBride
> Stroz Friedberg

Businesses with larger fleets of mobile devices, and those with active BYOD policies, should also consider separating mobile devices from the core network. Some companies operate mobile devices in a DMZ; others operate separate wireless LANs for personal devices, outside of the firewall.

Encryption, anti-virus, anti-spam and network access control tools are also all vital for mobile security, as is controlling the interface between the mobile subnetwork and the corporate core. Virtualized environments for running sensitive applications on the mobile device are another option CISOs are investigating, albeit one that puts its own demands on device performance.

However, security measures are only as good as the policies and user education programs that support them; this is especially the case for mobiles.

"Even with MDM or BYOD policies in place, employees will find ways to use their mobile devices to make their jobs easier, even by creating ways around controls," says Stroz Friedberg's George McBride. "Companies have a stake in taking charge of mobile systems; it is after all their data or their customers' data that they are responsible for protecting."

"You can't prise smartphones from people's hands. You have to accept risk, it's about degrees of risk. Even with the strongest security measures on iOS and Android, you can't guarantee data is safe," says Gartner's Smith.

"It is a question of best efforts, and making sure an average hacker can't get past them, unless they are specialists in mobile."

infosecurity
MIDDLE EAST

15-17 MARCH 2016
ADNEC, ABU DHABI, U.A.E
www.infosecurityme.com

SECURE YOUR DIGITAL WORLD.

SECURE YOUR WORLD AGAINST CYBER THREATS AT INFOSECURITY MIDDLE EAST.

In 2016, Infosecurity Europe brings its pioneering cybersecurity event to the Middle East for the first time – and you can be part of it at ISNR Abu Dhabi. From leading-edge innovations and best practice solutions to world-class technologies, Infosecurity Middle East brings it all together, with specialist suppliers, workshops and dedicated technology showcases to help you protect your vital data and infrastructure.

HIGHLIGHTS FOR 2016

- International Conference on Cyber Crime
- Three day workshop in partnership with (ISC)²
- Expert insights on the challenges facing your business

REGISTER NOW

DON'T MISS OUT. MAKE INFOSECURITY MIDDLE EAST YOUR MUST-SEE SHOW.

www.infosecurityme.com

Organised by
UNITED ARAB EMIRATES MINISTRY OF INTERIOR
Reed Exhibitions

Platinum sponsor
TRA هيئة تنظيم الاتصالات
TELECOMMUNICATIONS REGULATORY AUTHORITY

Broadcast partner
sky NEWS عربية

Official media partner
999

#MOIUAE
www.moi.gov.ae

Securing Apps Critical to Advancing mHealth

Sam Rehman, CTO of Arxan Technologies, spent close to ten years with Oracle where he led development groups, bringing multiple innovative and profitable products from concepts to market, including the Sensor/IoT-Based Platform. Here he looks at the challenge of mobility within healthcare and how security can be enabled

Mobile apps and devices are revolutionizing healthcare. What started with a wave of fitness tracking tools has rapidly evolved into an active marketplace of smartphone apps and add-ons, networked personal health devices, Big Data analytics, and transformative healthcare delivery models.

As is often the case, these exciting advancements also create serious concerns. Patient safety and privacy are threatened in new ways by insecure apps, improperly handled personal data, and hackable medical devices. Healthcare and medical device providers face strict data privacy and patient confidentiality requirements.

The handling of mHealth data generated by mobile apps and devices is under intense scrutiny—and for good reason. If mHealth apps and devices are not developed and deployed securely, patient health and physical safety may be at risk.

In some information security scenarios, making trade-offs between functionality and security is acceptable. In healthcare, there is little room for negotiating matters of safety and privacy. Because medical devices and healthcare applications have only recently been deployed in "hacker rich" mobile environments, there is a challenging learning curve. Most healthcare organizations are using some form of Mobile Device Management (MDM) and Mobile Application Management (MAM) technology designed to mitigate risks to mobile apps and devices carrying valuable patient data. But is enough being done?

Security Risks Not Addressed

Many mHealth security risks have been left unaddressed. Mobile technology use in the healthcare industry is so new and advancing so rapidly, vulnerabilities abound, and hackers know this. Because PII-rich data tends to fetch the highest price on the black market, healthcare organizations know they are in the crosshairs of cyber-criminals. The distributed nature of mobile apps increases their vulnerability to both malicious attacks and compromise by human error.

App developers, device manufacturers, and regulatory bodies must move quickly and decisively to assess and contain the very real risks to patient safety introduced by mHealth solutions. The industry is at a critical point; many of the vulnerabilities are shared and catastrophic incidents could very well damage patient and consumer trust across the board.

It is alarming to note that mHealth apps that were "approved" by trusted sources such as the US Food and Drug Administration (FDA) or the UK National Health Service (NHS) are no more secure than unapproved apps.

Indeed, in an assessment by Arxan of 71 mobile health apps, 84% of the FDA-approved apps, and 80% of the (formerly) NHS-approved apps had at least two critical vulnerabilities when tested against the OWASP Mobile Top 10 Risks,. The most prevalent security vulnerabilities identified were insufficient Transport Layer Protection and lack of Binary Code Protection. Such flaws leave apps exposed to code tampering, reverse-engineering, and privacy violations, and data theft.

A Life-or-Death Concern

Not only do these two common weaknesses open the door to malicious use of patient data and credentials, they could very well lead to attacks on the function of the app or device itself. At the extreme, this could literally be a life-or-death matter.

It's important to remember what we're talking about: apps that control the

connected medical devices; apps that turn smartphones into medical devices; apps that display, store, and transmit medical device data; and apps that analyze medical data to produce alerts. Smartphones, mHealth apps, and related add-on devices are used as thermometers, glucometers, heart monitors, and much more.

Protecting the integrity of their operation is just as critical (if not more so) as ensuring the confidentiality of personal data. The intellectual property (IP) contained in the apps is at risk and can be exploited to hack, reverse-engineer, or remotely manipulate devices and app functions.

Device tampering is a common technique for committing data theft in the healthcare industry. Reverse-engineering enables production of low cost imitators. This can lead to the emergence of a class of devices with questionable integrity (akin to cheap knock-off pharmaceuticals). Run-time injection of malicious code into applications can compromise the behavior of the application or device.

For example, an unauthorized user with malicious intent could modify and deliver lethal dosages of medication. Modifying medical device logic can physically impact patient health and safety. Clearly, application logic and libraries need advanced protection against these alarming threats.

What Can Be Done

Given the nature of the threats and risks, there is an urgent need for mHealth apps to bake in self-protection so that security measures follow the apps no matter where they reside. The days of focusing mainly on infrastructure security are long gone; in the era of mobile and IoT there is no longer a perimeter; applications are out "in the wild."

Closely protecting the application layer, with run-time application self-protection (RASP) capabilities, for example, should be a high priority. In fact, security analysts like Gartner are recommending to "Make application self-protection a new investment priority, ahead of perimeter and infrastructure protection."

"Modern security fails to test and protect all apps. Therefore, apps must be capable of security self-testing, self-diagnostics and self-protection. It should be a CISO top priority," Gartner said. Application self-protection is an important component of a defense-in-depth security strategy that can help healthcare organizations sidestep critical security and safety risks while enabling them to more rapidly advance mHealth.

Apps should also be tested and be sure to adequately address the most prominent risks. Testing how mHealth apps fare against the OWASP Mobile Top 10 Risks is a good place to start.

In addition, many healthcare organizations are keeping sensitive data on their backend servers to minimize exposure of data on the mobile device. However, the APIs that communicate to and from the mobile devices and backend servers need to have more robust protection than what is deemed to be standard.

Advanced API protection should become the standard since APIs can act as one the weakest links to the high-value, high-target healthcare data on the backend servers. White box cryptography combined with application code hardening, when used in combination, can deliver substantial protection and help preserve data confidentiality and patient privacy.

Simplifying Security is Essential

As much as possible, we have to find a way to simplify the security of critical apps and devices. Consumers, doctors, nurses and therapists are not security experts, and can't be counted on to properly update, patch, configure, and monitor their devices and software. It's hard enough to get users to practice basic security hygiene consistently.

Because the stakes are so high, it's important to design these devices and apps from the outset to be as secure as possible in and of themselves. This is so that they can plug-and-play into a multi-layered security strategy that accounts for various software, hardware, and cloud platforms, communications channels, networks of all sizes, and third-party vendors like MSPs. A

> Patient safety and privacy are threatened in new ways by insecure apps, improperly handled personal data, and hackable medical devices

protected application reduces many risks: compromise of patient safety; unauthorized access and fraud; confidential IP theft; patient privacy loss and health record exploitation; and damage to brand reputation and consumer trust.

Mobile health is here now, but nothing should be taken for granted. Market growth and technology adoption rates will depend largely on advanced security measures for devices and applications. It's important to keep in mind that healthcare providers are already stretched thin by changes brought about by ACA. Technology has to be an enabler, making practices more efficient and treatments more effective. Physicians and patients won't prescribe or use devices they don't trust.

The potential for mobile medical devices and applications to transform healthcare is enormous, especially as we face the demographic realities of an aging baby boomer generation (chronic conditions, in-home care) and a Millennial generation that vastly prefers virtual communication channels (and controlling everything with their smartphones).

Growth will accelerate once healthcare providers and device manufacturers build more trust and security into their solutions. Healthcare providers, administrators, and patients should have the freedom to run their applications on any device without burdensome security controls, and without fear of privacy loss or personal safety.

infosecurity® MEXICO

APRIL 19-21, 2016
CENTRO BANAMEX, MEXICO CITY
www.infosecuritymexico.com

BE PART OF INFOSECURITY MEXICO SHOW YOUR PRODUCTS AND SOLUTIONS TO POTENTIAL CUSTOMERS IN THE MEXICAN MARKET

AT INFOSECURITY MEXICO YOU'LL BE ABLE TO ENGAGE WITH:

DECISION MAKERS AND SENIOR IT EXECUTIVES

Attend seminars featuring top level information security speakers

SECURITY MANAGERS FROM THE TOP INDUSTRIES IN THE REGION

Exhibit your product and engage with customers looking for security solutions

ENGAGE MEXICAN THOUGHT - LEADERS TO COMMUNICATE THE VALUE OF YOUR BRANDS AND SOLUTIONS

Exhibit your product and engage with customers looking for security solutions

INFOSECURITY MEXICO OFFERS

- Exhibition floor with 2,000 specialized attendees as potential customers
- World class certifications from ISACA
- Earn CPE credits by attending education sessions
- Technical workshops and solutions talks to potential customers

Register your interest to attend
Visit www.infosecuritymexico.com

Contact +52 (55) 8852 6000 / ventas@infosecuritymexico.com / www.infosecuritymexico.com

Infosecurity Mexico
facebook.com/infosecmexico
@Infosecuritymx

Part of infosecurity GROUP

Organized by Reed Exhibitions®

Eyes on the Target

Do businesses have the right target or asset in sight, and do they even know what to protect? Infosecurity talked to Tripwire President **Gus Malezis** for some answers

What are the biggest, most dangerous threat vectors?

Gus: The threat vector that we're seeing are the same ones that you're seeing frankly all over the newsprint, and I think we'll continue to see that escalation. We continue to see the escalation of both volume and intensity; volume—we're seeing more and more of these things.

We would have thought they would have abated by now, or the world would have done a better job securing their infrastructure, and I think there is a better job being done, but it does not seem to be dissuading the bad guys very much. The bad guys are more successful at what they're doing, versus the good guys, frankly, so that's one thing that is probably not a big surprise to anybody.

Should we focus on the target, or the asset?

Gus: We've got to turn and focus back on the asset, or the assets that are most valuable to us, and watch the targets that people are going after. So that to me is a massive shift in focus by the customer, not so much by the industry and not so much by the vendors, but more about enterprise customers, and particularly those that have the skills and the wherewithal to say that they have got to start watching the patient, and has to start watching the target in our house.

That is the biggest threat, or the biggest change that I see over the past say 12 to 24 months.

Are there some cultural things people can do to protect themselves better?

Gus: Maybe the consumer has to come into this conversation at some point, because they need to demand something better from their providers. I think it is about assessing the value of those assets, and whether they can afford to be without them. What's the cost to their business, if something is (a) not available and (b) disrupted? What is the impact to their brand? What's the impact to TalkTalk or Carphone Warehouse, or Target. I mean, in the US, everybody has a project that's called, Don't Be Target!

Pardon the pun, but you talk to the large retailers, like Home Depot, like Costco, and they'll say, we have a project. You know the name now, and they realise the impact, the negative impact to their business, and after it's happened to somebody else, then they tend to respond. Up until that that executives believe that it's not an issue that's worth significant focus, or a change in operational attitude or investment. Then they get the lawsuits.

So how do you separate good change from bad change?

Gus: Well, there are things that we are using, there are policies. So they watched the target, they say they're not watching the wire, that's not helping anymore, so we're going to move investment out to watching the asset. It's clear the anti-virus is not going to cut it, they tell me, or even the personal firewall is not cutting it, because all that stuff blasts right through, so now we've got to watch the asset and watch for change, and that change is something that Tripwire happens to be very good at.

So that's really where the market is now going, and that's where I will say the smart money is investing.

What should businesses be doing?

Gus: You watch the wire, keep doing that, now watch the target, know when something is changing, understand what it is, do something about it, and then integrate your data. That way you can have higher-level business messages that you can communicate to your executives.

We still see a lot of executives that are unclear, they're very uncertain of what they should do about their security, information technology security, and IOT security, and there is no clear message in the market. For the most part, it's a thoroughly confusing foggy space as an executive, so that's the challenge that we see.

DMARC Specification Poised to Take Webmail Woes by Storm in 2016

The majority of attacks are now launched from the web, but this has not stopped email from being abused. Yet new measures are being put in place to further secure email and **Tara Seals** identifies the key ways for your staff to be your best ally in security

Email is one of the most popular vectors for attacks by cyber-criminals, and no wonder: the vast majority of those with internet access use it every day, which opens up a ripe landscape of opportunity for nefarious types.

To boot, email was built insecurely and without authentication—which enables cyber-criminals, hacktivists and nation-state actors to impersonate (or "spoof") legitimate organizations' identities.

To help combat this, the Domain-based Message Authentication, Reporting, and Conformance (DMARC) specification has been developed for web-based mail, which makes it virtually impossible for attackers to spoof, or fake, emails from a protected domain. Essentially, a DMARC policy combats this by allowing a sender to indicate that its emails are protected, and tells a receiver what to do if none of the accepted authentication methods passes.

The initial spec was published on 18th March 2015, and it's in the process of being adopted as the official input to the IETF DMARC Working Group. DMARC is now in the final stages of standardization, and 2016 is likely to be a big year for adoption, especially as Gmail Enterprise and cloud-based email providers move forward to integrate DMARC into their email platforms and email gateway solutions. DMARC supporters are also looking to additional use

cases for the technology as part of a second wave of protection.

A Problem That Had to Be Solved

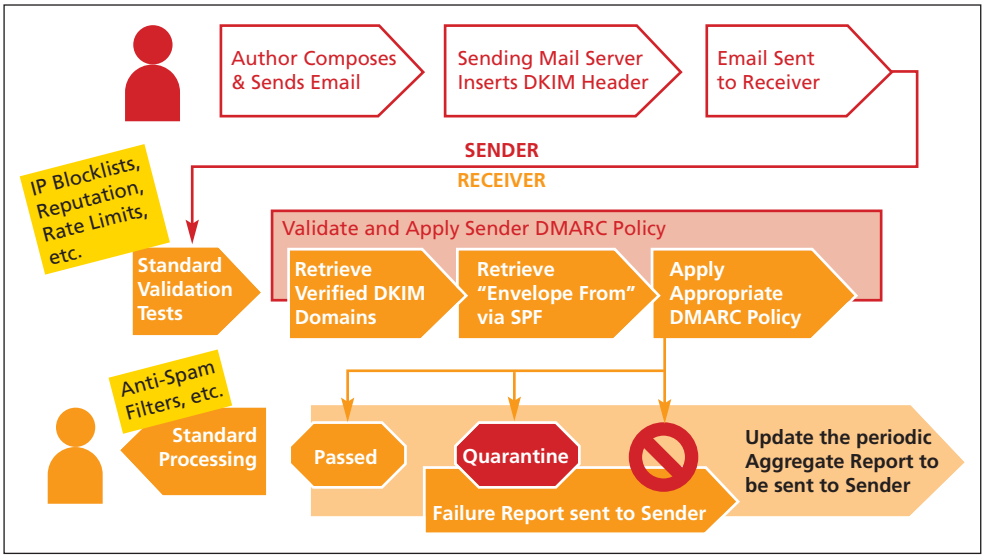
Email attacks are most commonly carried out after cyber-criminals hack into user accounts. Hackers can scrape the victims' address books, and then use a different server to spoof messages from the hacked user to his or her own contacts. They do this for spam and fraud purposes, for phishing and to spread malware.

"Most people don't know that when the fundamental email protocols for the Internet were designed in the early 80s, functionality was favored over security and the protocols were designed to trust input, which made spoofing incredibly easy," said Daniel Ingevaldson, CTO at Easy Solutions. "[However], 'fixing' email spoofing is a complex problem that requires buy-in from many stakeholders, and the time was right for DMARC."

There's little time to waste. In email fraud, the attacks are becoming more virulent. The FBI reported $1.2 billion in financial losses from business email compromise (CEO-CFO spoofing), and found that email is the number one malware delivery method. Similarly, the Verizon Data Breach Report stated that 78% of all data breaches start with email.

It's very easy to convince someone to open a mail and download an attachment or click on a link if that person believes the mail is coming from a trusted source; and no manner of end-user security awareness has seemed to help.

"For 20 years the industry has been fighting a plague of spam, phishing, targeted attacks and malware with email as the primary vector," said Patrick Peterson, CEO at Agari. "Despite the blood and money expended, we have failed. DMARC was invented to solve this problem. The inventors of DMARC (Agari, Bank of America, Facebook, Google, JP Morgan, PayPal and others) believed that if email became secure we could dramatically reduce the harm on the Internet."



Big Mail Providers Lead the Way

DMARC has enjoyed significant uptake in the past year—so much so that 85% of the mailboxes in North America are protected by the technology—and a total 2.5 billion mailboxes are protected globally. This is largely the result of the biggest email providers in the world, including Google, Yahoo, AOL and Microsoft, have thrown their considerable their weight behind the standard and are leading the way.

Google, which alone provides 900 million Gmail boxes, has announced that it will be moving Gmail to a strict DMARC policy starting in June 2016. Also, Yahoo recently expanded its use of DMARC to protect users of the ymail.com and rocketmail.com services, with more coverage to be added to additional domains in the coming months.

Yahoo's use of DMARC goes back to the nascent stages of the standard in 2014, when it used it to prevent a large-scale campaign of abuse of its Yahoo Mail. At the time a Yahoo executive wrote in a company blog post, "And overnight, the bad guys … were nearly stopped in their tracks." This was so successful that AOL followed suit later in the same month in response to a similar large-scale campaign targeting its marquee domain.

In all, 10 of the 10 biggest mailbox providers in the world support DMARC validation for inbound messages. Similarly, most major social media companies and banks use the same technology to protect their customers from email fraud and abuse.

Looking Ahead: Expanding Adoption in 2016

Even though the DMARC picture is looking good, it's important to understand that adoption lags in important areas.

This is especially true in other parts of the world outside of North America. Globally, some DMARC uptake is being held up because of privacy and data stewardship concerns. For instance, the data privacy laws in Japan and Germany offer no clear indication that they're allowed to share information in the form of the DMARC notifications. While DMARC uses aggregate reporting, rather than making specific IP addresses available, there is still confusion and concern when it comes to privacy.

"The question is what to do about messages that don't pass authentication," Steven Jones, executive director of DMARC.org. "If you're a big mailbox provider, and you see that some messages are passing, and some are not, should you do something? There's a lot of uncertainty and in some markets it's an issue of liability."

He added that market education for policy-makers is critical and will be an important initiative for DMARC.org in 2016. "The Japanese concerns about data sharing


For 20 years the industry has been fighting a plague of spam, phishing, targeted attacks and malware with email as the primary vector
Patrick Peterson
CEO at Agari

for instance show a lack of understanding that DMARC is really in accord with those privacy laws when you really look at it," Jones explained.

Within the US, there's more work to be done. For instance, some of the largest ISPs in the States, like Comcast, are deploying DMARC; but others, such as Time Warner Cable (RoadRunner), Earthlink, Cablevision and Charter have not deployed the technology yet.

"We continue to evangelize adoption, not just on the sender side but also on receiver end," said Rob Holmes, general manager of the email fraud protection business unit at Return Path. "More regional ISPs need to adopt DMARC on the receiving side so that the protection isn't just afforded to people in North America using the big mailbox providers."

Jones meanwhile believes that the role of email in data breaches will spur the demand for email authentication for B2B communications within the States—forcing some regional ISPs' hands. This will also be an important factor for gateway providers and smaller cloud mail providers to build DMARC support into their services.

"So many breaches start with phishing—and smaller companies don't have security resources to protect themselves," Jones said. "So, inbound message filtering with DMARC for SMBs will be the next wave of adoption—we're up to over a dozen commercial gateway products so far."

Next Steps: Focus on ARC, New Threats

DMARC is also taking steps to address the downsides of using the specification. When Yahoo and AOL began protecting their customers from abuse, there were a small percentage of users who were negatively impacted by the change as legitimate mails failed authentication checks. This can happen for a variety of reasons, including improper configurations, and indirect mail flows like the use of email forwarding and mailing lists.

To address these issues, several workarounds were quickly deployed by service providers and mailing lists, but a long-term solution has been submitted to the IETF for consideration. The Authenticated Received Chain (ARC)

ARC is being refined and tested with deployers such as Google, Microsoft and Yahoo, with an interoperability event being organized for the first quarter of 2016. ARC could be deployed as early as late summer; Google will be a first mover, which will make a large market impact.

"We are pleased to be supporting the ARC protocol to help mailing list operators adapt to the need for strong authentication," said John Rae-Grant, lead product manager for Gmail.

"More and more companies have been adopting DMARC and email authentication over the past few years, with more vendors and service providers adding the necessary support to their offerings in order to make that adoption simpler," said Jones. "With new protocols like ARC emerging to address the traditional email use cases that were problematic under some DMARC policies, and the leadership of forward-thinking companies like Google, Microsoft and Yahoo, I expect to see the rate of adoption accelerate globally."

Going forward, DMARC.org is also looking to other long-term pain points for email security, especially when it comes to display names. In an email "sent from" field there are two component: the address that shows the domain, as in user@mailprovider.com. Then there's the actual name that shows up as being associated with that address, i.e.,

"DMARC will become the standard for Internet-scale email spoofing protection in 2016" - Daniel Ingevaldson

> Most people don't know that when the fundamental email protocols for the Internet were designed in the early 80s
>
> Daniel Ingevaldson
> CTO at Easy Solutions

User One. Senders can set this field to say whatever they would like it to say.

"The limitation of DMARC is that it blocks domain spoofing," said Holmes. "But I don't need to spoof a domain to convince a person that I'm someone else—the most important identifier is the display name. It's an editable field. So while I can authenticate the address I can still put anything, say JP Morgan Chase, as the name."

This is an increasing issue as more and more email is read on mobile devices, where mail clients often just show the display names.

There are also Issues around cousin domains—i.e., lookalike domains where one letter or number may be changed in the URL, but is otherwise identical to a legitimate domain.

"We are hopeful that we can come up with some best practices for organizations to combat these issues, to be able to flag discrepancies for attention," Jones said.

In all, 2016 will be a big year for email security. "DMARC will become the standard for Internet-scale email spoofing protection in 2016," said Easy Solutions' Ingevaldson.

"By the end of 2016 most, if not all, of the major enterprise and cloud-based email providers will support DMARC. DMARC is truly only effective if it is deployed widely. This scale of global deployment will correct a major weakness in a fundamental Internet email security weakness that has existed for decades."

The Investigatory Powers Bill: the end of our online freedom?

The controversy over Government-led surveillance continues in 2016, almost three years since the revelations by Edward Snowden. Liberty's Policy Officer **Silkie Carlo** looks at the proposed Investigatory Powers Bill and what impact it could have upon UK citizens

The draft Investigatory Powers Bill was long-awaited, not least by Liberty. For years, we've campaigned for a fundamental overhaul of the law to ensure surveillance is conducted in a necessary, proportionate and accountable way—online and offline.

Again and again, we've challenged ham-fisted attempts by successive Governments to take us further toward a society where every man, woman and child's communications are intercepted and processed—where none of us is any safer, and we're all a lot less free.

This legislation represents a once-in-a-generation chance for parliamentarians to lay down vital democratic protections in law.

Announcing the Bill in the Commons, Home Secretary Theresa May said it would "provide the strongest safeguards and world-leading oversight" and give our agencies "the powers they need to protect our country." In its current form, it does neither. She also called the legislation "unprecedented". That it certainly is.

Sadly the Draft Bill – currently hurtling through pre-legislative scrutiny at breakneck speed – is more than just a vast disappointment and a wasted opportunity. It is littered with disproportionate powers that would fundamentally alter the relationship between individual and state—mass interception, mass hacking, mass acquisition of communications data and retention and linking of databases containing sensitive information on huge swathes of the population.

In short, it aims to legalise and extend the breath-taking practices revealed by Snowden, which Liberty is currently challenging in court—the mass, suspicion-less surveillance that has let our Government spy on human rights organisations, hack into the largest SIM card manufacturer in the world and capture webcam pictures of 1.8 million Yahoo users, many of which were sexually explicit. Snowden himself has branded it "the most intrusive and least accountable surveillance regime in the West".

It sets us still further apart from other liberal democracies, constitutes an extraordinary attack on the internet security of every person in the UK, fails to provide even the most basic privacy safeguards and—crucially—won't make us any safer.

Internet Connection Records

The Bill would require telecommunications services to retain our communications data—the who, what, when, where and how of calls, texts and emails – for a year. It also contains a new, controversial power to force them to generate and store Internet Connection Records on all of us – every website we visit, every app we open, and the date, time and device we use to do so, map searches, GPS locations, and details about other devices we communicate with.

These records will be accessible not just to the security services and police, but to public bodies ranging from HMRC and the NHS to the Food Standards Agency and OfCom.

The Home Secretary has downplayed this provision as no more intrusive than an itemised phone bill. This is disingenuous. Our online

searches provide a startlingly detailed picture of our most personal lives – together, they can reveal our health issues, race, religion, age, sexuality, job, location, family and friends.

More than that: they can betray as much about our innermost thoughts and desires as any diary. We live our lives online. Many of us share information with our devices, with barely a second thought, that we would be reluctant to disclose to our partners and closest friends. As the Internet of Things expands—and it already incorporates everything from cars and kettles to children's toys—the level of detail revealed by this data will become even more disturbing.

It's an unbelievably intrusive measure that would create a seismic shift in the relationship between citizen and state, which is perhaps why no other European or Commonwealth country demands the compulsory retention of this data – and Australia recently explicitly banned it in law.

If companies are forced to store mountains of data this personal and valuable, hacking isn't just a risk—it's pretty much inevitable. High-profile incidents in recent months—TalkTalk, Vodafone, Ashley Madison—show all too clearly how easily information can end up in the wrong hands, and just how distressing the repercussions can be when it does. Imagining the potential for blackmail and identity theft boggles the mind.

To echo Lord Strasburger's response to similar proposals in Theresa May's abandoned Communications Data Bill, the same Government which is investing £1.9bn to protect our national infrastructure from hacking is now happily building a "honeypot for casual hackers, blackmailers, criminals large and small from around the world, and foreign states."

Mass Hacking

This Bill represents the first time the Government has admitted to indiscriminate mass hacking—or "bulk equipment interference", which it seeks to provide a legal basis for in the Bill. This would legalise automated State hacking en masse, giving intelligence agencies the legal power to access millions of devices, systems or networks to view files, passwords and encryption keys, monitor internet activity and remotely control cameras and microphones.

The Bill will make service providers complicit, forcing them to "provide assistance in giving effect" to hacking warrants. This would compel them to take any measures, unless "not reasonably practicable", to assist authorities in hacking our devices. Also the general public is likely never to know what hacking assistance their CSP has been obliged to give because the Bill introduces a new imprisonable criminal offence for CSP whistle blowers.

Bulk hacking is the most intrusive surveillance technique conceivable—yet we've had absolutely no public debate on its use. It leaves devices and networks open to further attack from foreign spies and criminals, though you may never know if you've been hacked. The Bill doesn't make clear exactly how this legal hacking will be made any safer than illegal hacking, or prevent doing massive and irreparable damage to our security.

Authorisation

Most of these powers will require a warrant, currently authorised by public bodies' senior staff or a relevant Secretary of State, usually the Home or Foreign Secretary. In 2014, the Home Secretary personally authorised more than 2,300 interception warrants.

For many years, Liberty has been calling for that sign-off to fall to an independent judge – a view now held by MPs across the political spectrum and experts including former spy chiefs and the Government's Reviewer of Terrorism Legislation.

The Home Secretary made much of the Bill's "world-leading oversight" during the Government's pre-publication spin onslaught. Unfortunately, the much-trumpeted Judicial Commissioner role it creates is anything but.

Ministers will continue to authorise warrants before passing them to a Commissioner to "review" the decision. The Commissioner will not have a substantive role in the decision, instead relegated to playing second fiddle – only able to disagree with outrageously unreasonable warrants.

As the legislation seeks to endorse the speculative hacking and interception of billions of devices and communications the Commissioner is left with very little wiggle room. Modifications can be made to warrants with no judicial oversight and, if the request is "urgent", judges can be bypassed altogether.

Another way

Industry figures have lined up to tear the Bill to shreds. Adrian Kennard, head of ISP Andrews and Arnold, has pointed out that "the retention of any sort of Internet Connection Record is of very limited use at present. The current proponents of this logging do not understand how the internet works." Mozilla has called it a "harmful step backward for the interests of internet users." Jimmy Wales has dared Apple to refuse to sell the iPhone in the UK if the Government succeeds in weakening encryption, adding "Does Parliament dare be that stupid?"

Apple CEO himself Tim Cook summed it up best when he said the Bill "would almost certainly cause serious physical and financial harm across our society and our economy. Weakening security with the aim of advancing security simply does not make sense." When the figures condemning your flagship surveillance legislation read like a who's who of the global tech industry, you'd think it might ring some alarm bells with the Government. But if its track-record so far is anything to go by, a dogged refusal to listen to logic, evidence and valid civil liberties concerns appears to be the Home Office's calling card.

There is another way. It involves creating a dynamic, targeted system with surveillance conducted only for tightly defined reasons, like investigating serious crime or preventing loss of life.

The Government is banking on misinformation, fear-mongering and post-Snowden public apathy to get this Bill through. We must raise awareness of what these measures really mean for our society, and for the human rights of generations to come—and we need to tell our MPs that we won't stand for a Bill that makes us less safe and far less free.

Because once the Government has succeeded in opening these particular floodgates, they will be all but impossible to close.

Top 5 "Anti-Resolutions" to Fix Cyber-security in 2016

In the new year, rather than predicting the future **Jack Danahy**, co-founder and CTO of Barkly looks at the main things that need to be changed to make security a better place

To move forward in a healthier direction, I've identified five common approaches organizations should avoid for a more productive 2016.

5) Let's Stop Blindly Spending More

As breaches increase, everybody is trying to understand what the right amount of security is. Vendors, writers and analysts insist that there is some baseline amount that should be spent on security, either as a percentage of revenue or fraction of an IT budget. Worse, human nature leads us to believe that more is better, so improving security means buying more. As with most simplistic proxies for complex discussions, this just isn't true.

What I'd like to see instead: Companies figuring out the right protection strategy, then re-evaluating their investments to get the protection they need and can consume.

4) Let's Stop Playing the Weak-Link Card

Everybody knows that user mistakes are usually the first step in the chain of events that result in major breaches. When this happens, organizations remind us that security is only as strong as its weakest link, and the user is always identified as the most fragile element. By stopping there, and bypassing the real weaknesses, users take the hit for the vulnerabilities.

What I'd like to see instead: The "user weak link" excuse loses its get-out-of-jail free card status, and instead becomes a driver of new investment to make that weak link stronger.

3) Let's Stop Giving Ourselves Rave Reviews for Security Success Theater

Security status is reported as more threats are identified, more machines and networks instrumented, and new technologies adopted. What stakeholders actually want to know about is what attacks were identified and stopped, or what systems were made secure. When reports show progress against the wrong goals they provide a sense of false confidence, and reduce the pressure to improve strategy and practices.

What I'd like to see instead: Organizations become brave enough to recognize success only when there is a material reduction in critical weaknesses and decreases in successful attacks. This shift will be hard, but is better than investing in a mirage of better security.

2) Let's Stop Speaking in Incomprehensible Security Gobbledygook

As a security guy who has been a vendor, advisor and buyer, I've watched the industry language become a mush of overused and overloaded terms. Some just don't make any sense (anyone trying to "protect" their "intrusions"?). Others have been construed to make them applicable to almost anywhere (behavioral analysis, endpoint/system protection, application security, oh my).

Part of the problem is that talking about "protection" could mean traffic monitoring, incident response, and threat notification. Don't get me wrong—monitoring and response are vital, but lumping them together under the term "protection" is like saying hospitals are a form of protection against the flu.

What I'd like to see instead: A return to simpler, more courageous language. Security teams can say, "We are investing in A, to protect B, reducing our risk of C because it will D." Vendors can say, "Our product does X, protecting our customers against Y, which is visible by looking at Z."

1) Let's Drop the Unhelpful Security Superiority Complex

Breaches happen. Reasonable security people know breaches will continue happening, evidenced by the dominant cliché for the past 25 years, "No system is 100% secure." Although this is the case, commentary usually starts with assigning blame before details are known about the attack. We all live in glass houses, yet we can't resist throwing stones.

What I'd like to see instead: Security become more empowering than investigative or auditing. Our job should be understanding how to improve the system, without castigating the organization for not knowing as much as we do. Everyone has differing pressures and priorities, and we can only advance our impact by making the interaction more constructive.

The truth is the security industry has been resigned to these attitudes for too long. This year, let's agree to step back and reconsider so we can chart a better, more effective course.

Slack Space

Delivery Drones and Robots—Still a Bad Idea

Despite security concerns, the idea of delivering retail goods using unmanned vehicles seems to persist—and in fact is getting more concerning.

Amazon announced Prime Air, an initiative to drop off books and more via drone, two years ago. That has kicked off a parade of bone-headed initiatives. This autumn, Google's Project Wing head David Vos said the company hopes that its drones will be delivering packages by 2017. Meanwhile Wal-Mart has asked US federal regulators for permission to test its own delivery drones.

Also in perhaps the most concerning of the idea's evolution, one of the original founders of Skype is setting a course for the home delivery market with Starship, which, despite its name, will use ground-based drones.

Starship, targeted for a 2017 rollout, functions like its airborne drone cousins, only it drives autonomously to the shopper's doorway and then texts an alert message to announce its arrival. The bot is described as "low-speed" and the general premise is this: It picks up small packages from a fulfillment hub within its radius ("a few miles," according to its creators). Then, it self-drives using sidewalks and pavements to a customer's suburban location.

All of these schemes, flight or flightless, have a big, gaping problem: A concern about the ability to hack these vessels to disable their sensors and deliver the goods elsewhere—cyber-enabled larceny, basically. Also, Starship has the added charm of being able to A) be run over and B) simply picked up and thrown in a panel van, never to be heard from again.

Oh, but they all have GPS and locks! Well…so do full-sized cars, and somehow thieves still manage to steal those. Not only does this open up a completely new and unnecessary chapter for law enforcement, but it sets the stage for inevitable cost-overruns (and higher consumer prices) stemming from what the retail industry charmingly calls "shrinkage" (theft), and the loss of the presumably not-cheap equipment of the drones themselves.

The Apple Sub-Genius Bar

Who needs back-up for their mobile phone data when the courts are more than willing to compensate you for your loss?

That is the dubious lesson from a nearly 12-month-long court battle between Apple and a 68-year-old London pensioner Deric White, who went to the Apple Genius Bar at the flagship store in London for help with a password reset problem. He ended up with a wiped phone, after a bumbling Apple employee decided to reset the iPhone without warning his customer.

It's more like he visited the Sub-Genius Bar, amirite?

For most of us, this would be a headache and an inconvenience, and would say that the employee would deserve to be censured. But for White, who hadn't backed up his phone data or photos for years, it was an all-out crisis. He had other ideas as to how to handle the situation.

He detailed the reality of the struggle in the hearing, according to the *Daily Mail*: "My life was saved on that phone. I lost my favorite video of a giant tortoise biting my hand on honeymoon in the Seychelles. I was absolutely livid and my wife had been in tears. We had beautiful pictures of the Seychelles and other pictures as well, of African rhinos."

No word on whether the emotional testimony—*tortoise videos!!*—swayed the decision, but a judge in Central London County Court ruled that Apple had been negligent and awarded White almost £2,000 for his loss.

White, striking a David and Goliath chord, called the decision a "monumental victory for the common man." A common man who, apparently, cared enough about his exotic African safari pics to take Apple to court—but not enough to back the photos up for safekeeping in the first place.

Email-Happy Brits Obliviously Open Stuff

Seven in 10 Brits don't see emails as a threat to cybersecurity—and in fact, a significant percentage will cavalierly open, well, just about anything. Mails containing swear words, unsolicited notes about celebrity gossip, promises of pictures beautiful people in nude situations—it's all good!

Mailjet researchers found that even broken English, unsolicited offers from Nigerian princes to share their wealth, porn-y subject lines and dubious "urgent bank messages" aren't really turn-offs for the average UK citizen. Apparently, willy-nilly email opening is a national trait.

Almost two in 10 (19%) admitted to knowingly opening an email that said it contains images of a beautiful woman or man. Another 10% have admitted to opening an email that explicitly mentions containing nudity. Well, that one speaks for itself. Back to work, lads—and ladies.

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

infosecurity
MIDDLE EAST

15-17 MARCH 2016
ADNEC, ABU DHABI, U.A.E
www.infosecurityme.com

SECURE YOUR DIGITAL WORLD.

SECURE YOUR WORLD AGAINST CYBER THREATS AT INFOSECURITY MIDDLE EAST.

In 2016, Infosecurity Europe brings its pioneering cybersecurity event to the Middle East for the first time – and you can be part of it at ISNR Abu Dhabi. From leading-edge innovations and best practice solutions to world-class technologies, Infosecurity Middle East brings it all together, with specialist suppliers, workshops and dedicated technology showcases to help you protect your vital data and infrastructure.

HIGHLIGHTS FOR 2016

- International Conference on Cyber Crime
- Three day workshop in partnership with (ISC)²
- Expert insights on the challenges facing your business

REGISTER NOW

DON'T MISS OUT. MAKE INFOSECURITY MIDDLE EAST YOUR MUST-SEE SHOW.

www.infosecurityme.com

Organised by
UNITED ARAB EMIRATES MINISTRY OF INTERIOR
Reed Exhibitions

Platinum sponsor
TRA هيئة تنظيم الاتصالات
TELECOMMUNICATIONS REGULATORY AUTHORITY

Broadcast partner
sky NEWS عربية

Official media partner
999

#MOIUAE
www.moi.gov.ae

info security
STRATEGY | INSIGHT | TECHNOLOGY

INFOSECURITY SPRING VIRTUAL CONFERENCE

15TH - 16TH MARCH 2016

JOIN US AT THE LEADING VIRTUAL CONFERENCE EVENT FOR THE INFORMATION SECURITY INDUSTRY.

THE INFOSECURITY SPRING 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