Q1 /// 2015 /// VOLUME 12 /// ISSUE 1

STRATEGY /// INSIGHT /// TECHNOLOGY

infosecurity

I WANT YOU TO DECRYPT

Cryptowars Returns: Privacy Advocates Fight for the Right to Secure Comms

PLUS:

INTERNATIONAL INFOSEC LAW /// THE RISE AND RISE OF DDOS /// IOT AND RISK

Gigamon®

LIMITED VISIBILITY IS AS GOOD AS NO VISIBILITY

If you can't see everything that's happening on your network, you can never be completely confident you're not already under attack.

To truly protect your network, the ability to see into even its darkest corners is vital – Gigamon's Unified Visibility Fabric™ delivers 100% visibility and security solutions that scale to handle any threats to your critical data, now and into the future.

Gigamon's network security solutions put the power back in your hands.

TEL: 01344 859 870

LOOK CLOSER. GO FURTHER.

www.gigamon.com/campaign/security

infosecurity EUROPE

02 - 04 June 2015 | Olympia | London | UK

Visit us at stand: D180

Contents

January/ February/ March 2015

COVER FEATURE

FEATURES

POINT-COUNTERPOINT

OPINION

REGULARS

INFOSECURITY

Editor & Publisher
Eleanor Dallaway
eleanor.dallaway@reedexpo.co.uk
+44 (0)208 9107893

Deputy Editor
Mike Hine
michael.hine@reedexpo.co.uk
+44 (0)208 4395643

Online UK News Editor
Phil Muncaster
philmuncaster@gmail.com

Online US News Editor
Tara Seals
sealstara@gmail.com

Proofreader
Clanci Miller
clanci@nexusalliance.biz

Contributing Editor
Stephen Pritchard
infosecurity@stephenpritchard.com

ONLINE ADVERTISING:
Ben Race
ben.race@reedexpo.co.uk
+44 (0)208 9107991

PRINT ADVERTISING:
Melissa Winters
melissa@showtimemedia.com
+44 (0)1462 420009

Sophie Bottazzi
sophie@showtimemedia.com
+44 (0)1462 420009

MARKETING MANAGER
Rebecca Harper
Rebecca.harper@reedexpo.co.uk
Tel: +44 (0)208 9107861

ONLINE MARKETING COORDINATOR
Rianna Ramkissoon
Rianna.Ramkissoon@reedexpo.co.uk
Tel: +44 (0)208 4395463

PRODUCTION SUPPORT MANAGER
Andy Milsom

ADVISORY EDITORIAL BOARD
John Colley: Managing director, (ISC)² EMEA
Marco Cremonini: Universita degh Studi di Milano
Roger Halbheer: Chief security advisor, Microsoft
Hugh Penri-Williams: Owner, Glaniad 1865 EURL
Raj Samani: CTO, McAfee EMEA, chief innovation officer, Cloud Security Alliance
Howard Schmidt: Former White House Cybersecurity Coordinator
Sarb Sembhi: Past-president, ISACA London, editor of Virtually Informed
W. Hord Tipton: Executive director, (ISC)²
Patricia Titus

ISSN 1754-4548

Ensure Secure Sharing & Protect your Revenue Streams

Locklizard's document security software prevents unauthorized document sharing and piracy. It controls access to and use of your information both inside and outside your organization, so you can securely, and cost effectively, distribute and manage your digital content.

1 Stop Unauthorized Access

Documents are locked to specific users and their devices and will not work if users distribute them to others. You can also enforce the location from where they can be used (e.g. office only).

2 Control Document Usage

Decide whether authorized users can print your documents and if so how many times. Stop screen grabbing, and change access controls even after distribution.

3 Expire & Revoke Documents

Set documents to automatically expire after a given no. of views, prints, days, or on a fixed date. Instantly revoke access to documents at any stage no matter where they reside.

4 Log Document Activity

See when users open and print your documents. Apply dynamic watermarks displaying user information to viewed and/or printed information to discourage sharing of printed copies.

Locklizard document security software is used worldwide by information publishers either selling content or ensuring compliance, corporates protecting trade secrets, or providing a controlled method to share their information, and government agencies concerned over potential misuse of their information.

So what do companies use Locklizard for?

Protection from piracy & revenue loss

The drivers that made us go to DRM for our electronic courses

NetMasterClass develops on-line training courses which cost thousands to produce. Two days after one course was released they found it offered for sale on e-bay. That blew away the costs of development and sales going forwards in one single hit. They had to take positive steps to protect their IPR in order to stay in business.

"The return on investment to our company has been immediately evident. We are now creating new products for our electronic portfolio without fear of seeing them being distributed through unauthorized channels."

Cost and time savings

A greener and more cost effective means of document distribution

For 25 years TSD policy was to send out paper based manuals for its product lines to new customers. Manuals could take 7-10 business days from ordering to reach the customer, and could be copied and distributed outside of their control. They needed a solution so customers received instant gratification upon purchase and achieve a 'greener' result.

"Using Safeguard Enterprise PDF security has meant the elimination of many man hours, printing resources and postage. We currently estimate that costs have been cut by over 50%."

Secure sharing & Trade secret protection

Preventing information leakage

CCS Companies needed to protect commercial proprietary documents which they have to share with clients but also keep secret. They often have to provide specific individuals with temporary copies of confidential documents for their review. It is essential that they are able to do this without them being copied or forwarded to unauthorized users.

"Proprietary documents are not misplaced, and cannot be forwarded to the wrong individuals. You cannot place a value on that."

Start protecting your IPR now. **Call us on 800 707 4492** (US) **or +44 (0) 1292 430290** (UK & Europe) or visit **www.locklizard.com** to arrange a free 15 day evaluation and/or an online demo.

Locklizard

I Want to be Free

This issue's cover story tracks the so-called 'cryptowar' between governments and technology companies, who are, once again, squaring up over encryption.

Whilst a world with no privacy will no doubt appeal to intelligence agencies and governments, the general public is much endeared with the widespread encryption it has come to expect from the web and internet-enabled communications.

The issue has hit headlines once again over the past few weeks, as Prime Minister David Cameron – in the wake of the terrorist attack on the French satirical magazine *Charlie Hebdo* – decried the use of encrypted communications, noting that messages that "can't be read" by government should not be allowed.

Predictably, these comments have caused a backlash, and not just from within the infosec industry. Various experts have even gone as far as saying that the proposal is on par with authoritarian regimes such as those in Russia and China, with the potential to economically devastate the British information technology industry.

Addressing the House of Commons, Home Secretary Theresa May declared: "We have always been clear that the police and security agencies must have the capabilities and powers they need to do their job." The consequence of such powers being withheld, according to May, would be unpunished crimes, and innocent lives put at risk.

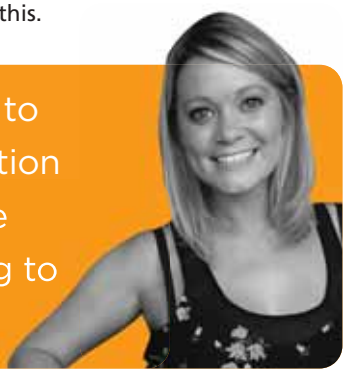
But just how direct is the correlation between enabling eavesdropping via a government-deployed and sanctioned backdoor in all online communications, and saving lives?

Assuming that banning encrypted communications will remove the risk of terrorism is naïve at best, and absurd in reality. But if the passing of the so-called 'Snooper's Charter' would minimize the risk, is it worth the sacrifice of privacy?

Personally, I think the question is a redundant one, and not only because privacy is a fundamental human right. Firstly, assuming that the very people that the Communications Data Bill is trying to obstruct will be deterred by the Bill is wishful thinking. In the age of Tor and Blackphone, they will always find another stealthy and untraceable mode of communication.

Secondly, assuming that a backdoor into encrypted communications would aid only the intelligence agencies is incredibly remiss. There is no backdoor that allows only the white hats in.

> Encryption is needed to safeguard the population from the exact people that Cameron is trying to 'protect' us from



The UK government must be fully aware that encryption is vital for security, and that their own systems would be left entirely vulnerable without it. Further, their own website – www.gov.uk – recommends that citizens use encryption to protect their data. In light of this contradiction, it's no surprise that Cameron's speech has been ridiculed.

Let's not forget, a great deal of what happens on the internet relies – entirely legally – on encryption, from the online banking industry to communications systems like WhatsApp and iMessage.

It's almost impossible to think of any serious part of the IT industry that doesn't use encryption in a significant way. Encryption is needed to safeguard the population from the exact people that Cameron is trying to 'protect' us from with the proposed 'Snooper's Charter'. The industry trend is very much towards more, rather than less, encryption. There's a good reason why smartphones are moving towards default encryption, and why Apple made a great play of this in the launch of its newest iPhone.

The UK's general election is just a few months away and Cameron knows that being seen to come down tough on terrorism could be a vote winner, which is one of the things that annoys me the most about all of this.

Exploiting tragic incidents of terrorism to cause a moral panic in order to win votes is highly unacceptable. Furthermore, using the terrorist attack on *Charlie Hebdo* to deprive individuals and businesses of their freedom to communicate without interference is, in no uncertain terms, a misuse of power.

This is a highly emotive topic, and one that I'd love to hear your views on. So email me: Eleanor.dallaway@reedexpo.co.uk and we'll compile and publish your own thoughts on the matter.

Take care,

Eleanor Dallaway, Editor

Are Your Files Protected From The Cloud?

GoAnywhere™ is a **managed file transfer** solution that tightens data security, improves workflow efficiency, and increases administrative control across diverse platforms and various databases, with support for all popular protocols (SFTP, FTPS, HTTP/S, AS2, etc.) and encryption standards.

With robust audit logs and error reporting, GoAnywhere manages file transfer projects through a browser-based dashboard. Features include Secure Mail for ad-hoc file transfers and NIST-certified FIPS 140-2 encryption.

Visit GoAnywhere.com for a free trial.

GO ANYWHERE™ → a managed file transfer solution by LINOMA SOFTWARE

GoAnywhere.com 800.949.4696

SAVES US A LOT OF TIME AND HEADACHE

"It's helpful every single day as the lifeline for communications with our customers."

Matt Booher
President
WIS:DOM Information Systems

SBA U.S. Small Business Administration

Funded in part through a Cooperative Agreement with the U.S. Small Business Administration.

Ten Years of White Hat Ball:

The Difference a Decade Makes

As the White Hat Ball prepares to celebrate its tenth anniversary, **Eleanor Dallaway** takes a look back at the highlights and successes from the past ten years, and learns what a difference a decade can make

Picture the scene: It's January 2005, and it's Marcus Alldrick's birthday. For those of you who don't know the wonderful senior manager of information risk and protection at Lloyd's of London, he's the current White Hat chairman. Sitting down to a birthday dinner with KPMG's Malcolm Marshall, and with the gripe that the SC Awards dinner had recently stopped its charity raffle, the pair brainstormed how the information security industry – "one that isn't short on cash" – could do more for charity.

Soon after, and back around a lunch table, this time in Covent Garden, with the added attendance of BT's Ray Stanton and then SC editor Ron Condon, the group put flesh on the bones of their idea. "We organized a gathering of industry players to set up a steering committee and agreed on two objectives: to raise lots of money for charity, and to make fun and enjoyable events," recalled Stanton.

From our vantage point ten years down the line, it's clear to see that both objectives have been achieved, and achieved beyond expectation. With nine highly successful events in the bag, and the tenth poised to be the best yet, the White Hat Ball has earned its place on the industry must-attend calendar and is highly anticipated and enjoyed each year by a loyal and ever-growing information security community.

> The commitment and enthusiasm of the industry has been phenomenal
>
> Marcus Alldrick
> White Hat chairman

ChildLine was selected as the chosen charity because of the work it does to protect children from abuse, which as Gerry O'Neill – White Hat committee member and former chair – adds, "is increasingly relevant to the industry as abuse has moved online, and the ChildLine service has also moved online. When we chose ChildLine as our charity, only half of their calls were able to be answered."

Now, the picture is a much brighter one. In the year 2013/14 ChildLine answered over 1.6m contacts from children. Since 2005, ChildLine has developed its online presence and now more than half of all counseling sessions happen online.

Peter Wanless, CEO of NSPCC, says, "Fundraisers like [White Hat Ball] are essential to the survival and development of the work that we do. With the support of the information security community, we can be there for children who will otherwise have nowhere else to turn."

Time to Reflect

Alldrick recalls the first ever ball in 2006 as his proudest moment as part of the White Hat committee. "Just getting it off the ground, making it happen, setting the scene for years to come… we were innocent and naïve," he laughs," but we did it."

In contrast, Stanton declares the upcoming tenth year his proudest moment, "because we never knew we'd get past year one."

O'Neill declares breaking the £100k mark his personal highlight. "The ball had come of age: We broke six figures, we had professional AV, a professional MC and a brilliant band. The caliber of the event had hugely stepped up."

From the offset, the original founders had principles in mind which would shape the future events. "We wanted it to be affordable and inclusive. We did not want to build an exclusive event," Alldrick remembers. "We wanted the White Hat Ball to be accessible to all levels of security and risk professionals," Stanton concurs, "Whether they are admin support, CEO or CISO."

Over time, that original group of four founders and initial steering committee has evolved, with new committee members replacing retired members. This ever-passionate group of industry professionals all give up their personal time to support the cause. "It's the people that make this, the work from all the individuals, and that includes the NSPCC special events team – they have been wonderful," Alldrick comments.

O'Neill endearingly describes the committee as "a magnet for prima donnas, over-indulged with character." Everyone contributes in their own way, he adds: "There is really strong goodwill amongst the team, a great diverse committee which is fun to be a part of." Having joined the committee myself nine months ago, I agree whole-heartedly with O'Neill.

All committee members interviewed for this article wanted to give kudos to one committee member who has served right from

The White Hat Committee at the 2014 Ball

The White Hat Ball committee would like to thank its 2015 sponsors: KPMG, BT, Qualys, RiskIQ, Barclay Simpson, BP, McAfee, NFU Mutual, Digital Shadows, and the Infosecurity Group, Reed Exhibitions.

From humble beginnings, the White Hat Ball has grown into a highlight on the industry calendar

the start: Joyce Bell-Walker, the committee secretary, whom Alldrick declares a "solid constant who deserves the recognition."

But without the support of the information security industry, all of the committee's work would be in vain. "The commitment and enthusiasm of the industry has been phenomenal," Alldrick remarks, humbled. From the loyal corporate sponsors, like BT and KPMG, to the individuals who buy their tickets out-of-pocket, it's the generosity of the information security industry which has allowed the White Hat Ball to prosper and grow.

"We've had no problem getting people to support us. The White Hat Ball is always a sell-out," says Stanton. "The industry has really embraced it, and in return we stay true to our initial objectives, and protect the intimacy of these events."

O'Neill praises the security industry's desire to "give back." He recalls that, "It took time to build momentum, and the first six years were a fairly hard slog." But now, he says, "companies actually approach us to sponsor. They want the association with the brand, and of course, the other motive is altruistic."

Celebrity Endorsement

The White Hat Ball has also had its share of celebrity endorsers: From Esther Rantzen, who attended the first ball, to Neil and Christine Hamilton who acted as the very enthusiastic and mischievous chairs of the tops and tails game, to Robert Powell, Nicholas Parsons, Ian Royce and Graham Cole, who have all taken a turn hosting.

> The industry has really embraced [the White Hat Ball], and in return we stay true to our initial objectives
>
> Ray Stanton
> White Hat committee

Gerry O'Neill recalls how Ian Royce, in particular, left a huge impression. "At last year's ball, Ian Royce made a very personal speech revealing that he himself had been abused, and he hadn't had the option of a service like ChildLine to help him. It really brought it home to me. You could have heard a pin drop in the room," he recalled.

Celebration Time

Whilst the White Hat committee strives for improvement year on year, the tenth anniversary celebration looks set to be the best yet. "There will be more of a party atmosphere than ever before, and we hope to raise even more money and have even more fun," Alldrick said.

So, here's where you come in, infosec community. Support White Hat, get behind us. "Help us to raise even more money for charity, help us to make an even bigger difference, and have a great time doing it," urges Alldrick.

And it seems the party spirit is going global, as White Hat events spring up across the world. There's now a White Hat Ball USA, and current liaisons regarding a launch in Singapore. This is, of course, in addition to the other annual UK events which sit under the White Hat umbrella, including the White Hat Rally, White Hat Golf Day, and the White Hat Marathon Team.

As Ray Stanton reflects on the "legacy that four drunken fools created, and that has been supported and followed by a whole bigger bunch of drunken fools," it's easy to recognize just how big a difference a decade has made: £1,000,000 to be precise.

"The last ten years have been an absolute joy," says Alldrick. "It's one of – if not the – high point of my career, watching White Hat grow from a conversation over lunch into a phenomenon. It would never have happened without the support, enthusiasm and dedication of a lot of people."

"Long may this continue," echoed O'Neill who also shares his gratitude to all the people who have made White Hat such a success.

The final word, however, goes to Ray Stanton, who many will recognize as being totally synonymous with the White Hat Ball. "In another ten years, I won't just be proud of the millions we raised, but I'll be proud of our industry and how close we are to charity, and knowing how much we give back."

INFOSECURITY SPRING VIRTUAL CONFERENCE

24TH - 25TH MARCH 2015

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

When good go

The mainstream news media is facing transitional, and to some extent troubling, times – with falling print circulation, and the erosion of traditional revenue streams offset against positives like global reach and the vast possibilities of the digital age. Although the internet has changed how we consume news, mainstream press outlets on both sides of the Atlantic still wield a lot of power when it comes to disseminating information and influencing public opinion.

Cybersecurity stories are proliferating in the mainstream press at an unprecedented rate, with recent research from Deloitte reporting that the first ten months of 2014 produced 24,105 data breach news stories, a huge 340% increase from 5474 in the corresponding period a year earlier.

Whether or not this is having a positive effect beyond a vague sense of raising awareness, however, is far from self-evident. Certainly within the security industry, there are mixed feelings about the nature of this widespread reporting, and what its impact might be.

Fear and Loathing on Fleet Street

The problem, says Maire Byrne-Evans, web science researcher at the University of Southampton, is that "even the reputable newspapers have to sell through fear." She adds that, "Although it's easy to be dismissive and roll out clichés about the media being driven by sales and by having to sell ads, this is the economic bottom line

Hacks Bad

The past year brought greater mainstream press interest in cybersecurity matters than ever before. But despite the wider profile of security issues, the important messages still aren't getting across, **Mike Hine** discovers

for them – without sales and clicks they cease to exist."

Alarmist headlines and sensational stories undoubtedly grab attention and garner clicks, sales and eyes on the page. A November 2014 print edition of London's free *Evening Standard* daily newspaper, which has a circulation of around 850,000, bore the front-page headline 'Met War on 200 Cyber Crime Gangs'. Emotive language like 'war' and 'gangs' – with connotations of intimidation and violent street crime – make this headline stand out, and a sanitized version wouldn't read, or sell, nearly as well. This is nothing new – but should we just be satisfied that cybersecurity is able to make the front page at all?

"It's great to see cybersecurity incidents and issues featuring more prominently in the media," offers independent cybersecurity consultant, Dr Jessica Barker. "However, the way threats are reported is not always constructive. Research into the psychology of fear suggests that for 'a fear appeal' (a message arousing fear) to change behavior, it needs to show that a threat is real, that individuals are susceptible to it, and that there are effective mitigations."

Far from having a positive effect, news stories in the mainstream media can do more harm than good if they peddle fear over effectual response. Dr Barker argues that, "If the media just communicates the threats, people will engage in controlling the fear rather than the danger, so they will go into denial or reactance, believing

that they are simply being manipulated by the media."

'Computer Apocalypse'

Sensationalism is engaging, and people don't necessarily look to newspapers for advice on how to lead their lives. Nonetheless, the effect of negativity and sensation on readers is not limited to denial only. "Without the right messaging, there is a danger that people will not be motivated to find out how to be safer online or that they will be put off using the internet out of fear," says Dr Barker.

With Forrester research predicting that online retail sales are set to rise to $370bn by 2017, the risk that hysteria around cybercrime could impact the economy by driving people away from the internet is not to be taken lightly.

The reality of cybercrime's economic threat is illustrated by the significant effect Sony's decision to initially withdraw *The Interview* from cinemas had on box office earnings. As this story unfolded, media outlets pushed the 'cyberterrorism' angle as hackers threatened more and more repercussions for Sony throughout the holiday season. Once again, the language of warfare permeated such coverage. There is little doubt that this is bad for public perception of cybersecurity matters. If hackers become synonymous with terrorists in readers' imaginations, hysteria begins to overshadow the reality of the threat and the messages about how to take simple measures to be more secure online.

Writing on Norse Corporation's Darkmatters blog, Edwin Covert says that "By using terms such as cyber-attack, terrorist, 9/11, computers, tragedy, and the like, unwary readers get the sense that a computer apocalypse is nigh."

Some commentators, however, take a less critical view of such doom-mongering. Barry Scott, chief technology officer EMEA for Centrify argues that "sensationalizing these events, and using overly emotive language can be beneficial, particularly in situations where consumers may not recognize the company that has been breached, and cannot relate as well as they might to a familiar name such as eBay."

Getting the Message Across

Whatever the drawbacks of sensationalism and fear-peddling in the media, the increased profile of cybersecurity no doubt represents an opportunity for industry advocates to spread the gospel and actually influence positive behavioral change. The key is making sure that impartial, educational commentators are given their fair share of column inches. However, for a variety of reasons, this is not yet happening.

Is Cybercrime Under-Reported?

Despite the escalating presence of cybersecurity in the media – with the risk of 'breach fatigue' that this brings – some experts raise the point that the true scale of the cybercrime problem is undoubtedly much vaster than we know.

"If anything, cybercrime is under-reported because of undetected breaches and reputational damage-particularly in the finance sector," says Tony Marques, cybersecurity architect at Encode Group.

With the potential negative market effects, many companies – those that aren't obliged to, at least – can cover up incidents they feel it would be detrimental to expose. Until we have greater transparency, assessing just how large a problem this is will be impossible, many security experts argue.

"Effective password creation and management, cyber liability insurance for the small business, and two-factor authentication (2FA) – these are all achievable actions. But such messages get thrown by the wayside in the scrum for a good story," argues Pen Test Partners' senior partner Ken Munro. "Take, for instance, Celebgate. That was a great opportunity to educate the public on 2FA and how to implement it, but the media was far more interested in promoting the salacious story of a naked Jennifer Lawrence."

Dr Barker concurs that promoting solutions is essential if increased cybersecurity coverage is going to have any positive outcomes. "Explaining what mitigations there are and why they protect against threats is really important," she told *Infosecurity*. "If you're asking people to change their behavior, they will usually only be motivated to do so if they understand why they should do so and if the steps are broken down and made accessible."

But while more and more security experts are quoted giving advice in news articles, there is still a suspicion among some commentators

that others are not open enough when it comes to dispensing free advice.

"Obviously security companies sell through raising fear of crime, too," says Byrne-Evans. "It's in their interest to overstate the case."

Munro concurs, suggesting that "much of the content in the media on security is based on PR put about by product vendors trying to sell their kit. That's why it's very light on practical advice."

Specialist media outlets, like the plethora of security blogs and online magazines, are, of course, replete with the kind of constructive advice that would help consumers, SMEs and otherwise cyber-unaware parties improve their security with a few simple steps. But as these outlets generally cater to a tech-savvy audience of security professionals, their potential impact and ability to instigate positive behavioral changes is limited to this niche. It's about time that messages such as these get more prominence in the mainstream media.

Power of the Press

Assessing the impact of negative news on the public psyche is difficult. Munro perceives "a state of apathy bordering on the catatonic," adding that, "Joe Public has become so turned off by these stories that many now ignore them."

> Without the right messaging, people will not be motivated to be safer online
>
> Dr Jessica Barker

Some recent surveys indicate that attitudes to cybersecurity do, indeed, tend to range from pessimistic to apathetic. Research from Deloitte suggested that 63% of 2000 people surveyed did not have 'much or any' confidence that firms could keep their personal data safe from harm. A LogRhythm paper, meanwhile, revealed that while 59% of 1000 UK citizens surveyed believed harsher penalties should be levied against organizations that suffer a data breach, 61% claimed they did not actually know of any businesses that had fallen victim. A third of those surveyed by LogRhythm had never heard of Heartbleed or Shellshock, while 42% believed that the threat of cyberwar or cyber-terrorism is real.

This kind of data paints a picture of a general public that is low in confidence when it comes to the security of their personal information, and has serious concerns about the potential impact of 'cyberwar'. But it is also a general public that is not necessarily *au fait* with the details of the major incidents that security practitioners, by contrast, would rank as the most significant news stories within a calendar year. News coverage is leaving a general impression – but not a good one.

"I think the security industry has a huge role to play in this, in communicating with the media, explaining threats, and what can be done to mitigate them, in simple, accessible and understandable ways," says Dr Barker.

Advice from retailers post-breach also needs to focus on the core issues rather than mere stop-gaps, argues Munro: "Retailers need to stop this knee-jerk reaction of issuing dictums that merely see one weak password replaced by another and begin offering concrete advice that improves password creation and management. It should then seldom be necessary to change passwords at all."

Whether or not the mainstream media is currently interested in promoting cybersecurity best practice, injecting some constructive tips for mitigation into news stories is clearly a sensible tactic. As an angle, it might not be as eye-catching as the doom and gloom, but consumers will quickly tire of endless stories about breaches that are essentially very similar in nature.

And there is, as always, still a place for journalists to ask very trying questions of those companies who do fall short on their security, and help educate consumers about the demands that they should make of firms that hold their data.

"That's where the power of the press comes into its own," concludes Munro: "Demanding answers and bringing pressure to bear that improves disclosure and security advice."

With 24/7 rolling news coverage around the world, there is an ongoing effort to raise the profile of cybersecurity

Interview: Kevin Hickey

Kevin Hickey is the president and CEO of BeyondTrust. He's also one of the nicest guys you could ever hope to meet. Sat against a backdrop of the beautiful mountainous desert, in his office in Phoenix, Arizona, Hickey told **Eleanor Dallaway** what the key to retaining good infosec people is, and why, despite his reputation for M&A, BeyondTrust is different...

I first met Kevin Hickey at a pool party, hosted by BeyondTrust, in Vegas. In shorts and T-shirt, he mingled with his guests, giving time to – and showing genuine interest in – each and every one. How many CEOs can you say that about?

So, as I turned up at the BeyondTrust office in Arizona, I had high expectations for my interview with Hickey, and I wasn't disappointed. Afterwards, I went for dinner and drinks with him and some of his senior exec team, and realized that a lovely CEO must attract lovely staff. I had a lot of fun that night.

Kevin Hickey's reputation for capital fundraising and mergers and acquisitions precedes him, and as soon as I raise it, he says, "You're right, I get called on this a lot." And he doesn't mean by journalists. "No, by people interviewing with us because they're concerned about what I'm going to do," he admits candidly.

So where does his aptitude for growing, selling, and M&A come from? "Ever since I left IBM and went to a company called Viasoft," he begins. "It was a $6 million company and we turned it around, took it public, and I learnt very early on that I get excited about the structure of building something, growing something."

But what's the formula for success? "It's really simple, you invest in me, in the intellectual property, and you make sure that you have great technology." Great technology attracts great people, he adds.

And thus far, it has worked out pretty well for him. Hickey has applied said formula at Viasoft, NetPro and eEye Digital Security, which was acquired by BeyondTrust in 2012. eEye was Hickey's first pure-play security role, and he recalls that he very quickly realized "that if you really understand and get to know the [information security] sector, you'll have a career for life. This sector is not looking for people that just want a job."

High Hopes

So when Hickey joined BeyondTrust by way of the company's acquisition of eEye Digital Security, he had high hopes of taking the newly merged company to the "next level."

"I knew right away that what I'd like to do is sell to a private equity player. It was a group that I wanted to build and continue with," he explains. And sell to a private equity player he did – in September 2014, it was announced that an affiliate of private equity firm, Veritas Capital, would acquire BeyondTrust from private equity and venture capital firm, Insight Venture Partners.

"We sold the company, but there wasn't one change other than the fact that we have a new investor who's looking at it from the view that they want to build a really strong security software company to take public, and they want to do it the right way. It's a new partner with fresh eyes looking to build, and build out." And the right way, according to Hickey, is to "continue with the company, add to the top line, and invest back into the business.

"We invested a lot in the intellectual property, came up with some really solid solutions, and really started to add value."

The investment has been reflected in the numbers, which has seen margins grow to north of 35%. "If you look at our competition, even CyberArk or Qualys, they're in the high single digits or low teens," he compares.

With a strong alignment to M&A activity, I ask Hickey for his opinion on the current M&A landscape in the information security industry. "I think you're going to see a lot more consolidation in this sector. Customers have more vendors now today than they ever had. But I do believe, with all the pressure put on CIOs and CISOs right now – and the old adage, you never get fired for buying IBM – I think they're looking for people that have a platform, substantial revenue, and success."

As a result, explains Hickey, questions are posed about what kind of vendors CISOs really deal with and put their confidence in, which will result in a lot of consolidation. "You've got to believe that consolidation is healthy, and that innovation is not going away."

Innovation is, however, hard to come by in the bigger companies. "They acquire, they don't innovate, but that's just their business model – they know that innovating themselves would take longer." Information security, however, is a very healthy sector which relies on this very innovation, he adds. "We're being attacked and we don't even know it, it's 'if' not 'when', and there are even tools for hackers now," Hickey adds, clarifying the exact extent of the size of the (infosec) prize.

When the People Rule

And in order to truly compete for a decent slice of that infosec prize by staying relevant and staying ahead, you better have yourself a staff full of assets, Hickey tells me. "Just look at my team – Marc, Brent, Mike – they have a lot of passion for this industry. We've got guys and gals that are so driven, and that's hard to find in bigger companies."

But in a highly competitive industry with vendors fighting for the brightest talent, how does BeyondTrust attract – and more importantly, retain – talent? "You have to have a culture that is exciting and promotes clarity: tell people what's expected of them, and let them do it. Let them run their business, because when they have passion, they'll do it the right way," continues Hickey, who has a policy of hiring people "much smarter" than he is.

"Surround yourself with really bright, good people, and make sure objectives are exceedingly clear."

But that doesn't mean it's all smooth sailing, counters Hickey. "We fight like you wouldn't believe, but it's out of respect. You don't battle with somebody that you don't have a lot of respect for, you just kind of walk away."

The key to good people, he says, is building an environment and a culture that people want to be in, and of course, rewarding people appropriately. "People want to work where they're appreciated, where they feel like they have true input, and I hope that's what we've created here."

Hiring Hackers

I'm particularly keen to talk to Hickey about one specific member of his talented team: Marc Maiffret, the company's CTO, an ex-hacker with an impressive resume which has seen him testify before the United States Congress on matters of national cybersecurity and critical security threats three times.

Whilst no doubt an incredible asset to the BeyondTrust team, I ask Hickey whether he was ever concerned about hiring someone who had once donned a black hat. "When Marc was 16, the US government said to him: 'Either come help us, or we'll give you free rent,'" Hickey laughs. We can all read between the lines of that ultimatum.

"Today's hacker does it for financial or political reasons, true cybercriminals. Marc was different – he was that brilliant, and was doing it because he could. It wasn't malicious, just a little mischievous, and it was purely recreational, it wasn't to hurt his country. Marc then decided to build a product to stop guys like him. How many hackers were actually going out and starting a business to stop guys like themselves? You've got to be pretty confident, and that's how you know the caliber of person you're getting."

It's for these reasons, explains Hickey, that he actually views Maiffret's colorful history as a positive. "He brings such a passion and a love for what he does. You also have to look at the personality of who you're getting; give Mark three or four beers, and he'll start crying about how much he loves this company and the space." Well actually, Marc joined us for dinner that very night and I can confirm there were no tears, despite the flowing drinks. But his passion for the industry is undeniable, and as for his personality, he's an absolute diamond.

"Every case should be an individual judgement," adds Hickey, referring to policy on hiring ex-hackers. "You can't throw a generic cloth over something and say, I don't want to hire a hacker. Just look at the case, the timing, what were they doing, what they have done since. Ask what their ultimate goal is."

> If you really... get to know the [information security] sector, you'll have a career for life

In addition to his technical expertise, Maiffret "brings common sense to the equation. He can make boards understand technology by bringing it down to the right level so they can assist in policy. It's so unique to find someone who really understands the depth of the technology and what he could do with it, and then also understand the business."

So, having endearingly enthused about his entire staff for a considerable amount of time, I ask Hickey whether the apparent skills gap we talk about so frequently in the industry is perhaps exaggerated. "It's definitely a real thing," he says, "but there's a tremendous amount of talent that can be found, stolen, but also nurtured and grown." When I ask for more detail on 'stealing' talent, Hickey confesses: "We look for companies that aren't innovating like they used to, or ones that have been gobbled up, and I've got to tell you, when we find [a company] that has been acquired, oh, we're bad. We are all over those guys."

750 Miles from the Valley

BeyondTrust HQ is in Phoenix, Arizona, 750 miles east of Silicon Valley. Whilst BeyondTrust's finance, accounting and sales are all handled from Phoenix, R&D happens outside the Grand Canyon State. "You know, you do miss an awful lot being here, I will say that. You miss a little bit of the buzz, the edginess, and pushing-the-envelope type pieces. But what we gain from being away [from the Valley] is more focus on the solutions."

Hickey finds himself in the Valley on business every other week, for two or three days at a time, but is more than content being based in Arizona for nine months of the year. The other three – in the height of summer – are spent in his home in Coronado, California, a little island off of San Diego, which he very kindly offers me the keys to, if I ever fancy a vacation out there.

I get the distinct impression that Hickey is a man who has a very admirable work-life balance, and has passions outside of work that rival his passions within the BeyondTrust walls, including golf, fine wine, and family.

Thank You Snowden

So, what's next for BeyondTrust, I ask Hickey, the man who – on paper – always has his next move planned out. "I want to be seen as a true leader in the privileged space, data intelligence space, and the whole analytics piece.

"The days of having a vulnerability scanner without intelligence is a thing of the past. You have to give people good threat intelligence; boards and CISOs will demand it. So I really want to go after and take this privileged space, and be seen as just one of the true innovators and leaders."

And the privileged space is one that, since Snowden, has well and truly earned its place on the map. "I think we had 80% belief in the company that we're doing the right thing, then Snowden happened, and things started to take off.

"Snowden helped create a sector for privilege that is now arguably one of the faster-growing areas in security."

Once you lead and innovate in a space, Hickey says, "it gives you flexibility. If you do something really well, and build a good reputation, it allows you to get to the next level, and it gives you flexibility to do what you want to go do."

At this point, Mike Yaffe and Brent Thurrell, two of Hickey's senior leadership team, enter Hickey's office. "I'm sure this is real interesting and everything, but let's go get some drinks," says Yaffe. We laugh and Hickey rolls his eyes, it's clear to see just how well everyone at BeyondTrust gets on. I guess that's the culture that Hickey and I discussed earlier.

Kevin Hickey, it has been a pleasure. Now, let's drink wine.

ARE YOU SMARTER THAN THE ATTACKERS?

02 – 03 June 2015

REGISTER ONLINE NOW

www.infosecurity-intelligent-defence.com

Olympia. London.

Intelligent defence against cyber attacks

- Gain in-depth understanding of the latest vulnerabilities, exploits and threats
- Hear from leading security experts who are at the sharp end of technical research
- Access best practice advice on how to mitigate the effects of new vulnerabilities and exploits

Meet the Advisory Council

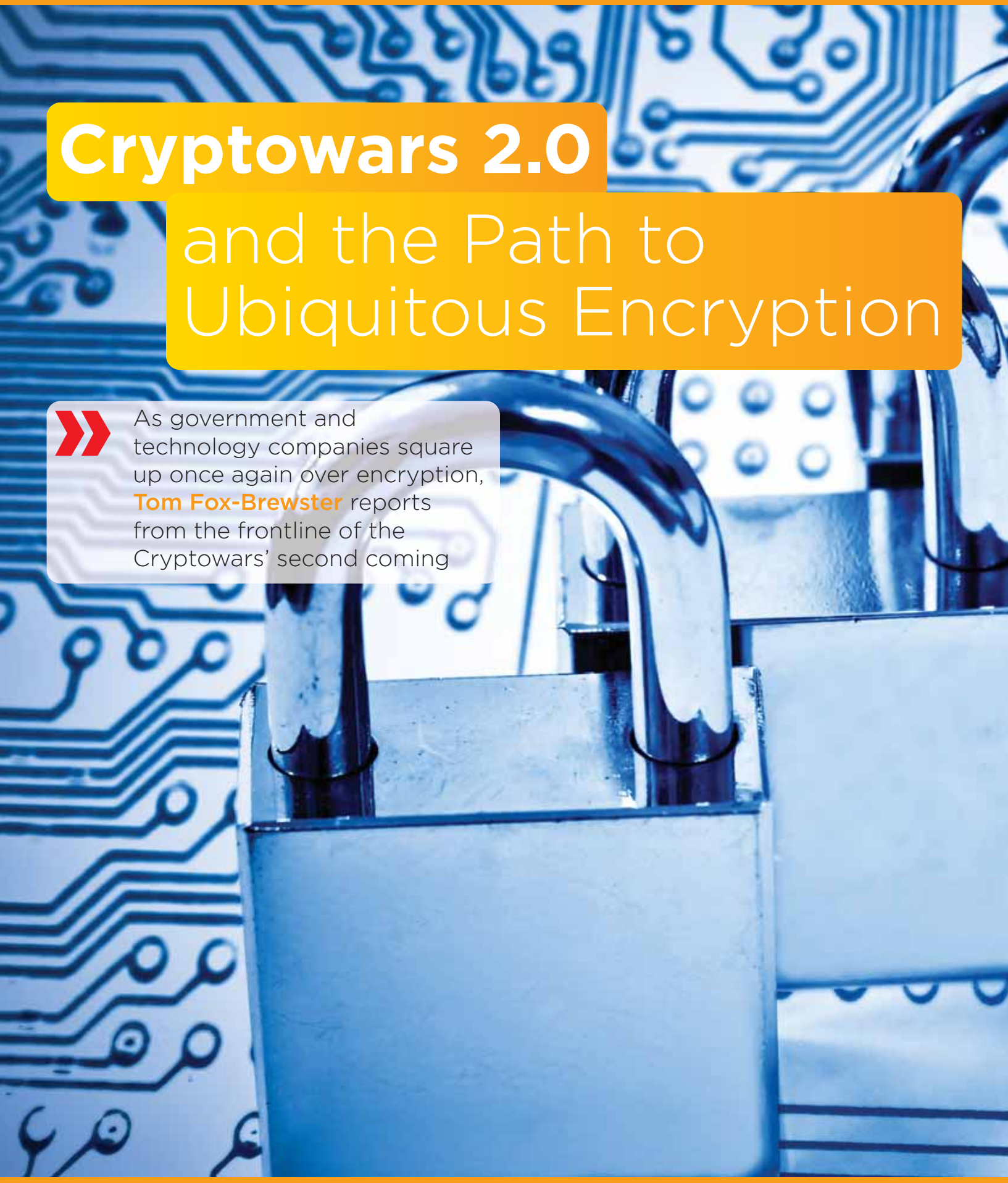
Dr Eric Cole, Jack Daniel
James Lyne , Trey Ford , Rik Ferguson

Find out more at:
www.infosecurity-intelligent-defence.com

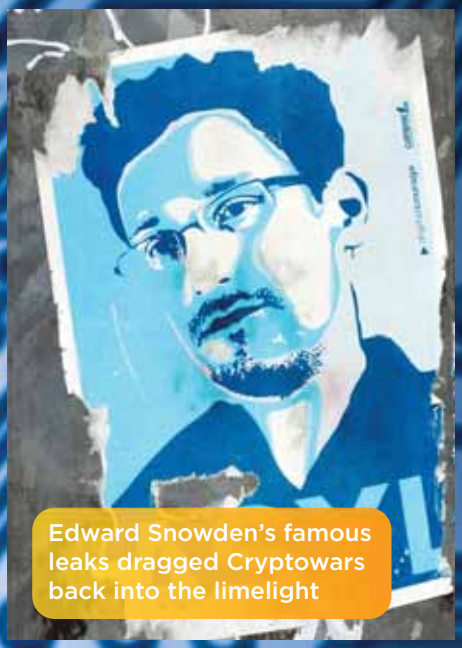
infosecurity® INTELLIGENT DEFENCE

European Technical Research Conference

Cryptowars 2.0 and the Path to Ubiquitous Encryption



As government and technology companies square up once again over encryption, **Tom Fox-Brewster** reports from the frontline of the Cryptowars' second coming



Edward Snowden's famous leaks dragged Cryptowars back into the limelight

Privacy is dead and we all need to deal with it. That statement was a shibboleth of those who would directly benefit from saying it, according to Jon Callas, world renowned cryptographer and co-founder of secure smartphone maker Blackphone. It's simply not true, he adds.

Who would benefit from a world with no privacy? Intelligence agencies and companies that trade people's data without affected individuals knowing are two obvious examples. But the tide is turning against them. The rise of cheap and widespread encryption across the web and internet-enabled communications has, in fact, pointed to a world where online privacy might be ubiquitous.

Watershed Moment

When historians look back at 2014, they'll likely see it as the year when this movement gained proper momentum. Just recently, WhatsApp added end-to-end encryption to its massively popular messaging service thanks to a collaboration with Open Whisper Systems, which had already created the much-respected TextSecure and RedPhone apps for private communications. Companies like Silent Circle and Blackphone have pushed on, trying to create financially viable businesses with their encrypted comms offerings. Much-used content delivery network CloudFlare decided to enable Secure Sockets Layer (SSL) web encryption across the sites it served, whilst notable tech experts like Chris Soghoian have been pushing for SSL across every website on the planet. Apple and Google, meanwhile, announced their respective mobile operating systems would encrypt users' data by default.

It was the actions of those two tech giants that irked law enforcement in America the most, however. FBI director James Comey told media he was concerned that Apple and Google were marketing a technology that would "allow people to place themselves beyond the law." Added to the Edward Snowden documents that revealed various attempts by US and UK intelligence agencies to break much-used cryptography, Comey's comments made it apparent that certain corners of government were willing to fight against widespread encryption. Privacy advocates the world over looked on dumbfounded. They felt it was a sign: Cryptowars 2.0 had begun.

Going Underground

The original Cryptowars, according to the account of Ross Anderson, professor of security engineering at the University of Cambridge, lasted roughly from 1993 till 2000. President Clinton was persuaded by the National Security Agency (NSA) to try to grab everyone's encryption keys, says Anderson: "We all fought back, from NGOs to Microsoft, and the policy was abandoned while Al Gore was trying to get elected. We thought we'd won, but it just went underground, as Snowden told us."

He points to one Snowden revelation in particular, the NSA decryption program known as BULLRUN, which has been covertly compromising cryptography in various ways. For starters, the NSA had spent at least $250 million on influencing companies' technical designs to try to ensure it could crack their protections, while GCHQ had explored ways to get access to Hotmail, Google, Yahoo and Facebook traffic. The NSA had also set up a ten-year program solely designed to crack encryption.

But the tech industry's response hasn't been to bow down to intelligence agencies. Instead, it has only bolstered encryption, hence the rush to push out end-to-end protected systems. And what they're doing is wholly legal, which leaves law enforcement with one of the toughest questions it has ever had to answer: how does it legally get access to data when users have total control over protections around their information?

Various countries are trying to pass access laws which would compel service firms – whether internet service providers like BT and Virgin, or internet firms like Facebook and Google – to do everything that's demanded of them. In the UK there's the Data Retention and Investigatory Powers Act 2014, which is heading for a judicial review after concerns were raised that the government had extended its powers to reach into foreign data centers and into webmail services such as Gmail.

But there are legal contradictions that police have to cope with and that bemuse critics of surveillance. For instance, privacy laws in the UK demand that firms should not hand over information on their own nationals to anyone outside the country, unless they have proven their ability to protect data. The Information Commissioner's Office has been demanding properly implemented encryption from private and public organizations. In the US, various laws, such as the Sarbanes-Oxley Act, require decent data protection. So on the one hand, governments are demanding encryption, whilst on the other they want easy access to data. As Callas notes: "There is no such thing as 'Government.'"

GCHQ has long sought to intercept traffic from several major tech giants

> We thought we'd won [the original Cryptowars] but it just went underground
>
> Ross Anderson
> University of Cambridge

The Rise and Rise of Encryption

With such apparent paradoxes and with various forces fighting their corners, how might the second Cryptowars be settled? The cryptographers certainly won't be backing down. Callas, who was also involved in the Dark Mail bid to create highly secure email, says crypto designers have to create systems that "actually work; they have to be effective." It's their *raison d'être*. "We're in the job of protecting people's communications because there are gazillions of people who have the right to talk to people," Callas adds. "They have business needs and personal needs and I believe they have a fundamental human right to defend themselves."

The tech companies will continue to improve encryption too, partly as part of a PR campaign in response to the Snowden leaks, but also because they are keen to place control of data into the hands of users so they don't have to make decisions on whether to work alongside governments. The technology itself will distance them from intelligence agencies as it'll prevent them accessing any data directly, though

there are still some weaknesses that could allow them to access users' communications.

From a technical perspective, though they will likely continue to break encryption, intelligence agencies don't have to spend all their resources subverting cryptography. They could, and have, sought to get to data before it's encrypted.

"It's easier, for example, to wait until a message has arrived and is decrypted by the recipient in order to read it rather than try to decode the message yourself. Don't think Bletchley Park, where messages were plucked out of the ether and decrypted; think of the technology you use in front of you being subverted to read your communications," says Professor Alan Woodward, a security expert and a visiting professor of the Department of Computing at the University of Surrey. It's believed GCHQ infected Belgian telecoms giant Belgacom with the Regin malware partly because it wanted to get at communications before they were turned into completely garbled nonsense.

The Long Arm of the Law

Law enforcement still has certain laws on its side if it does want to break encryption, even if they're limited. The UK Regulation of Investigatory Powers Act does allow law enforcement to demand that a suspect decrypts anything that has been seized, though it might be tricky to get certain sticklers to comply. In the US, citizens have claimed their Fifth Amendment rights, which protects against unfair treatment in legal processes, when such demands were made.

As subverting technologies becomes increasingly difficult and citizens can either flout the law or use it to their advantage, governments will likely have to rethink their strategy. Anderson wants to end the Cryptowars 2.0 early with a new treaty about law enforcement wiretapping that would let police forces in signatory states get access to communications data and content in other signatory states, with a number of safeguards. These would include judicial warrants, where an independent person has assessed the case and found probable cause for further investigation, rather than relying on a minister or intelligence agent to make the call.

WhatsApp is just one of many major tech brands to have begun introducing end-to-end encryption

There also needs to be transparency, including the eventual disclosure of all warrants after a fixed period of time, or when the suspect is charged or case dropped, says Anderson. There should also be jurisdiction, so that countries have to go through another's legal system if they want to get at data outside of their borders, he adds.

> These Cryptowars are probably un-winnable by either side, if there are actually any clear 'sides' in this debate
>
> Professor Keith Martin, Royal Holloway

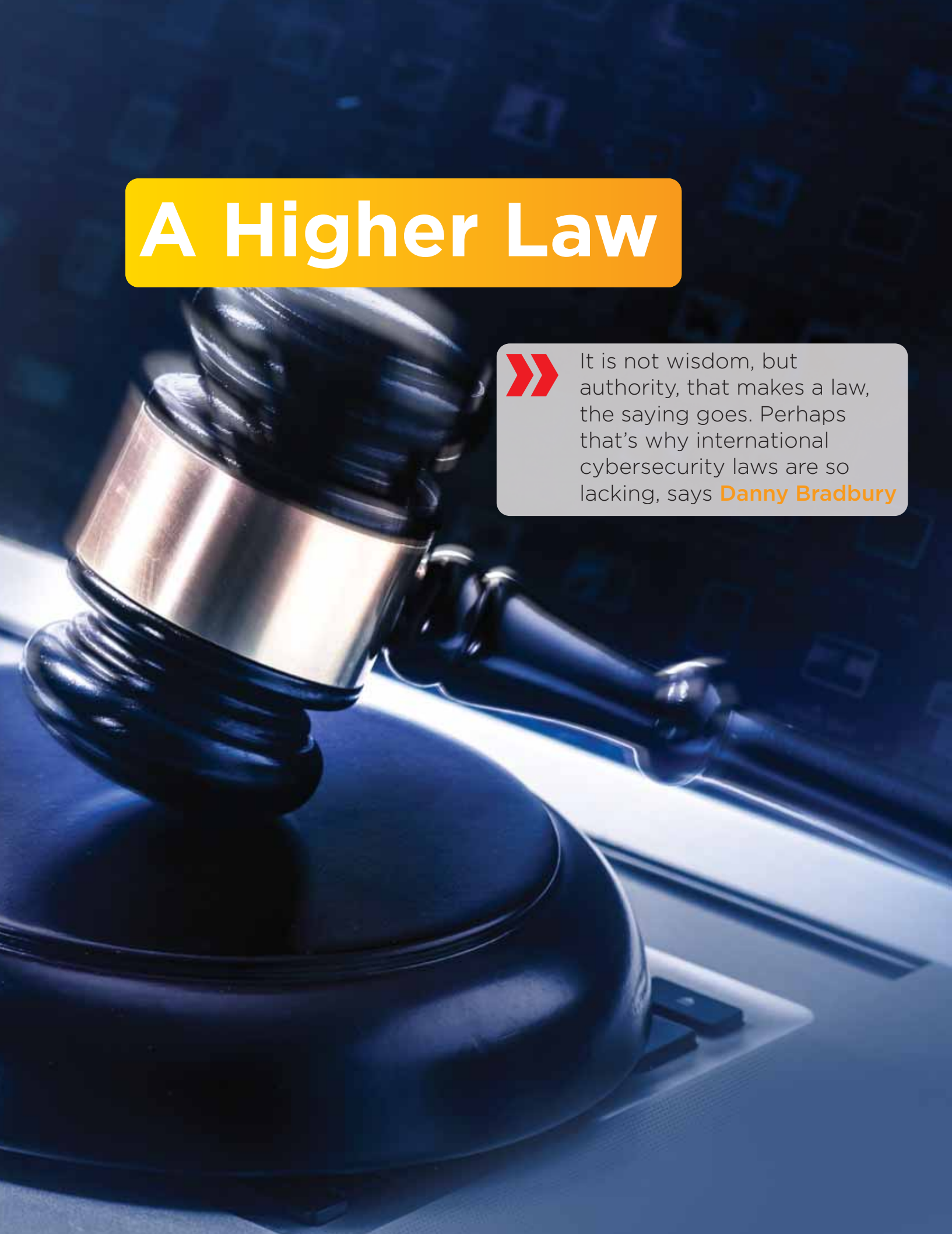
These are sensible suggestions, but some see no end to the back and forth between tech companies and global governments.

"These Cryptowars are probably un-winnable by either side, if there are actually any clear 'sides' in this debate – the battleground just continues to move around," says Professor Keith Martin, director of the Information Security Group at Royal Holloway.

Wherever individuals stand on the issue, they should remember not to place all their faith in encryption to protect their privacy. Just look at the many SSL weaknesses that received so much press last year, from the Heartbleed vulnerability to the Poodle flaw.

"It is certainly the case that there are more encryption products and services around. However, it is important to realize that encryption has its limitations. It is very good at making data unreadable while it is stored and/or communicated across a channel. But when that data is actually used, it normally needs to be decrypted and then exists in a readable state. Thus, use of encryption certainly makes it harder to access data – but it does not make it impossible to access," concludes Martin.

A Higher Law



It is not wisdom, but authority, that makes a law, the saying goes. Perhaps that's why international cybersecurity laws are so lacking, says **Danny Bradbury**

December 2014 was a big month for cybersecurity in Canada. The country passed legislation allowing it to ratify an international treaty on cybercrime a mere 13 years after it was first unveiled.

Things tend to move like molasses in the world of international law. That's a sticky problem for those tasked with bringing cyber-criminals to justice. With online thieves and exploiters often operating outside the legal jurisdiction of their victims, countries must work together to protect themselves against global threats. But is international cybersecurity law strong enough to bring criminals to justice? And if not, then what other work needs to be done?

The Law in Europe

There are several European directives that touch on areas of cybersecurity. The 2002 E-Privacy Directive requires European electronic comms companies to report data breaches, while the 2008 European Critical Infrastructures Directive states that critical infrastructure service providers must put electronic protections in place. The 1995 Data Protection Directive decrees that data controllers must adequately protect personal data, but this legislation will be superseded by the General Data Protection Regulation, which is expected to be adopted in 2015.

These directives have created some international consistency in cybersecurity across the EU, but far more work is needed. EU lawmakers admitted this in a preamble to proposed legislation now in the final stages of becoming law, which they hope will tie network information security law together into something more cohesive.

In March 2014, the EU voted through a Network and Information Security (NIS) Directive. Originally proposed a year earlier, the directive was designed to enforce an EU-wide cybersecurity strategy created at the same time. The proposal states that, "Existing NIS capabilities and mechanisms are simply insufficient to keep pace with the fast-changing landscape of threats and to ensure a common high level of protection in all the member states."

> Existing NIS capabilities and mechanisms are simply insufficient to keep pace with the fast-changing landscape of threats
>
> Proposal for EU Network and Information Security Directive, 2014

The directive, which at the time of writing was still being thrashed out by stakeholders, would force affected companies to report security breaches with a significant impact. Also included were instructions for national regulators to co-operate by providing early warnings to each other on cybersecurity risks, and for secure channels for sharing sensitive information.

The big debate at the end of 2014 was about whether the directive should affect only operators of critical national infrastructure, or whether providers of information services, such as social network and e-commerce companies, should also be affected.

The Budapest Convention

The directive will move the EU further towards a consolidated approach to cybersecurity, but only one international treaty currently addresses cybercrime more directly. The European Convention on Cybercrime, also known as the Budapest Convention, defines tactical operations for fighting cybercrime on a global basis. It is this legislation that Canada is now able to ratify, which puts the North American country on a list including the US, France, and Germany.

Published in 2001, the Budapest Convention was a long time coming. Its roots date back to 1976, when participants at the Council of Europe Conference on Criminological Aspects of Economic Crime in Strasbourg discussed ways to define

2015 should see the passing of the new EU General Data Protection Regulation

Efforts to involve Russia and China in worldwide cybersecurity legislation have been fruitless: Neither Russia nor China have signed or ratified the Budapest Convention

cybercrime. This was a forward-thinking crowd: the wooden-cased Apple 1, one of the first home computers with an actual keyboard, shipped that year.

Little happened then until 1989, the year when the fundamental language of the web, HTTP, was created. The Council of Europe created its own list of recommendations for punishable cybercrime acts, which was adopted the following year. Seven years later, the Council began negotiations on the European Convention on Cybercrime. Introduced in 2001, it finally came into effect in 2004.

Assessing the Law

So does the Budapest treaty do its job? There are still notable problems prosecuting cyber-criminals, warns Steve Durbin, managing director of the Information Security Forum (ISF): "If you're talking about cybercrime, and you talk to Interpol, they'll describe an immense amount of frustration on their part in tracking perpetrators down, and then doing something with them if they do find them," he says. "So, it's about the willingness of nation states to observe and collaborate and prosecute cyber-criminals."

Countries that ratify the Convention agree to implement its policies in domestic law. These policies span key areas: fraud and forgery, child pornography, copyright infringements, and security breaches. However, neither Russia nor China – two large sources of cyber-criminal activity – have signed or ratified the treaty.

Still, there have been some significant wins, thanks in part to co-operation facilitated by the Budapest treaty. In November, law enforcement units from the US and over a dozen countries arrested 17 individuals in a bust targeting black markets operated via the Tor network.

Ulf Bergström, head of communications and external relations at Eurojust, the judicial co-operation unit, argues that international agreements are crucial when targeting cybercrime with operations like these: ''It is paramount in cybercrime to involve the judicial authorities, prosecutors and investigations from the start to ensure that evidence is gathered in a way so that it is admissible later in court.

"You must also sort out where you will prosecute, as this is a cross-border operation; at the same time, you must balance the citizen's rights," he continues. "So, clearly, without justice, there will be no success in fighting crime.''

Military Activity

Commercial cybercrime isn't the only thing that international law must consider, though, according to legal experts. Military attack and defense is

becoming an increasingly important part of the equation.

"There is real doubt about whether the Convention reaches sovereign state activity, and as we know, this is the major area of great concern to those of us that want a peaceful, conclusive and fair cyberspace," argues Mary Ellen O'Connell, professor of international dispute resolution at the University of Notre Dame's Kroc Institute for International Peace Studies.

O'Connell is particularly concerned about the use of Stuxnet, the virus that disrupted operations at the Iranian Natanz nuclear facility, now believed to have been a US/Israeli project: "I am also concerned about how the Chinese are using the internet for military advantage," she warns.

If Budapest doesn't shed legal light on these kinds of state-sponsored cyber-activities, then what does? Robert Clark, an attorney in cybersecurity and privacy law at the US Military Academy's Army Cyber Institute, says that the Pentagon has mapped laws used in conventional warfare to the cyber domain. He refers to the Law of Armed Conflict (LOAC), which draws on treaties such as the Geneva Convention and Hague Regulations for warfare, and covers basic principles such as proportionality and military necessity.

In a 2011 report to Congress on cybersecurity defense policy, the Pentagon called for the inclusion of LOAC as part of a strategy including "the use of all necessary means" to defend its interests in cyberspace. "LOAC is just as adequate as it is for the other domains: land, air, sea and space. In all these domains, including cyber, LOAC can be easy, hard, and everything in-between," says Clark.

> Interpol... describe[s] an immense amount of frustration in tracking perpetrators down
>
> Steve Durbin
> ISF

O'Connell argues for a binding treaty on nation state engagement specifically for cyberspace, governed by an independent body like the International Telecommunications Union (ITU), with its rich understanding of the internet. Clark is unconvinced: "China and Russia were leading the pack to come up with a cyber-treaty convention, and the reason we objected is because it also went to our core basics of freedom of information and freedom of speech. They wanted to include aspects of regulating and suppressing freedom of speech as part of this core cyber convention."

Instead of a pervasive treaty on cyberspace engagement, the US has moved to bilateral talks, but these have been difficult. Direct discussions with China on cybersecurity recently stalled after five members of the Chinese military were indicted on hacking charges in the US. Meanwhile, Russia and China have been working towards signing a bilateral treaty on cyberspace engagement rules.

In 2011 the Pentagon called for the Law of Armed Conflict (LOAC) to be applicable to incidents in cyberspace

State-Sponsored Theft

Part of the problem with China is the high instance of IP theft alleged to be emanating from that country. The five aforementioned Chinese military officers were accused of hacking firms including Westinghouse Electric, US Steel Corp, and SolarWorld, in an effort that US attorney general Eric Holder said was designed to advance the interests of Chinese state-owned firms.

When states sponsor or organize the theft of corporate secrets, that is classed as espionage, Clark points out, arguing that it isn't illegal internationally. Countries normally prosecute such activities under domestic law. That's a useful tactic when the spies reside in your cities, he points out, but less so when they're a continent away, doing it via keyboard.

The only other option is to address it privately, says Gregory Nojeim, director of the Freedom, Security and Technology Project at the Center for Democracy and Technology: "Sometimes it becomes a diplomatic issue, in which case the relevant officials will be raising the matter with the foreign governments," he explains. "I would imagine that sometimes the State Department raises it with foreign ambassadors here."

Like purely commercial online criminal behavior, state-sponsored activities are developing at breakneck speed. Politics moves more slowly, especially when multiple countries with different agendas are all working on the same treaty. For now, it seems that most of the meaningful discussion around state-sponsored cyberspace activity is happening as many hacking operations do: behind closed doors, in secret.

Computer Says "No":

Will We Ever be Rid of DDoS Attacks?

With DDoS attacks reportedly increasing in size and complexity in 2014, **Phil Muncaster** canvasses the industry on where the problems lie and how we can respond

The distributed denial of service (DDoS) attack has been on the CISO's radar for years now. But 2014 saw a huge surge in attack size and volume, causing misery for organizations across the globe. In the third quarter of the year alone, DDoS prevention firm Akamai said it dealt with 17 attacks greater than 100Gb/s, with the biggest standing at a whopping 321Gb/s. With cyber-criminals constantly adapting new techniques to improve their effectiveness, what can organizations do in response? And what does 2015 hold in store?

What's a DDoS?

At its most basic, a DDoS is an attempt by an attacker to overwhelm a targeted computer resource with a flood of traffic from multiple compromised computer systems – usually part of a bot. The distributed nature of the attack makes it difficult to stop those botnet machines without blocking legitimate traffic, resulting in a service outage for the victim and its customers, albeit usually temporary.

There are numerous different types of DDoS, but two of the most common are application layer attacks and infrastructure (or network) layer attacks. The former typically inundates a service with application calls, while the latter overloads a service by using up all of its bandwidth. Akamai's stats reveal that the total number of attacks increased 22% from Q3 2013 to Q3 2014, with a 389% increase in attack bandwidth. However, while infrastructure layer attacks jumped by 43% over the period, app layer efforts decreased 44%.

Hitting Firms Where it Hurts

Before working out what level of response is needed, organizations need to

understand why they've become a target, according to Quocirca director and analyst Bob Tarzey. "Launching a DDoS will not in itself make you any money as a cyber-criminal. There's not an obvious way to monetize these attacks, apart from extortion," he tells *Infosecurity*, adding that this is a relatively unfavored option compared to other illicit money-making schemes, given the time, effort and cost involved for cyber-criminals.

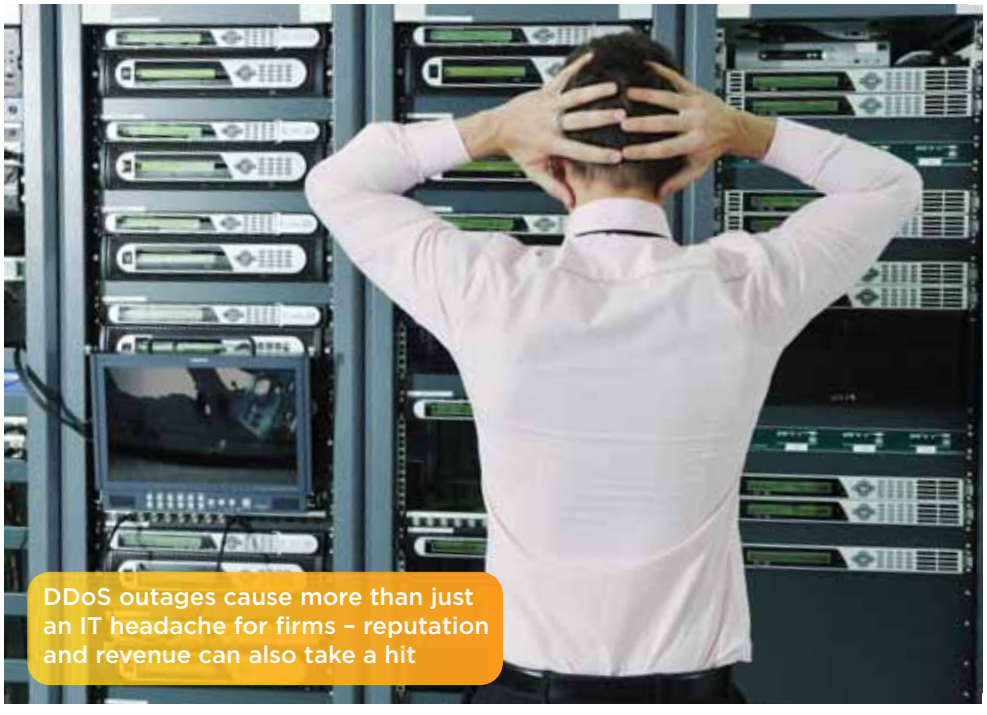
Arbor Networks' *Worldwide Infrastructure Security Report*, released in 2014, has some interesting insights. It reveals that instead of criminal extortion (15%), DDoS attacks are most likely to be motivated by political or ideological disputes (40%). The rise of Anonymous has certainly had a major part to play here, and 2014 once again saw the online collective cause its fair share of outages – most notably in the #OpWorldCup blitz against FIFA World Cup sponsors.

It also emerged recently that potentially state-sponsored actors have been DDoS-ing pro-democracy Hong Kong sites such as that of the anti-Beijing paper *Apple Daily*.

Hong Kong saw a 111% rise in attacks from September to October 2014 as a result, according to Arbor Networks. Interestingly, 26% of attacks spotted were put down to criminals simply demonstrating their DDoS capabilities to potential customers. A further 18% were due to competitive rivalry between organizations, while 16% were launched merely as a diversion to enable a more serious data exfiltration attack.

The impact on organizations, of course, depends upon a variety of factors. A fleeting attack from Anonymous is not likely to have the same impact as a major, well-resourced campaign from a state-sponsored entity, for example.

> There's not an obvious way to monetize [DDoS] attacks, apart from extortion
>
> Bob Tarzey
> Quocirca



DDoS outages cause more than just an IT headache for firms – reputation and revenue can also take a hit

However, for those organizations which make their livelihood from the internet – including online gaming, e-commerce sites, or even cloud service providers – it could lead to a worrying drop in earnings, negative publicity, and loss of customers to rival firms.

More Sophisticated?

Just as with the rest of the ever-evolving threat landscape, DDoS attackers are constantly changing their *modus operandi* to circumvent existing threat mitigation systems. To this end, 2014 first saw an explosion in NTP amplification attacks. This was signalled by a US-CERT warning in January which claimed attackers were exploiting a vulnerability in older versions of NTP servers to overwhelm victim systems with UDP traffic.

Incapsula research in March claimed to reveal a major shift towards this strategy, with attacks as big as 180Gb/s spotted. However, thanks to a concerted effort by organizations to patch and update their NTP servers, the attack methodology began to lose favor. In fact, NTP attacks dropped from 14% of all DDoS in Q1 to just 5% in Q3, according to Arbor Networks.

Yet as this strategy began to wane, so the cat-and-mouse game evolved again and so-called SSDP attacks grew, from just three known events in the whole of Q2 to a substantial 29,506 the following quarter. These attacks use source port 1900 and may be harder to stop with patching as they exploit a vulnerability in home CPE devices, which users typically do not get around to upgrading with newer firmware. Some 42% of all attacks greater than 10Gb/s used SSDP reflection during Q3 2014, according to Arbor.

Attackers have now also begun to use public cloud infrastructure to launch DDoS campaigns. In July, researchers revealed that hackers were exploiting a vulnerability (CVE-2014-3120) in open source search engine Elasticsearch to break into Amazon EC2 virtual machines and launch their attacks using a new variant of the Linux DDoS trojan Mayday. In fact, new DDoS malware is

> More can be done by sharing information in near real time on the nature of the attacks
>
> Jim Fox
> KPMG

a constant thorn in the side of those tasked with mitigating these attacks, especially as easy-to-use toolkits are becoming increasingly widely available.

Discovered in September, the Spike toolkit is the latest of these and is said to be able to build even bigger DDoS botnets by targeting a wider range of internet-enabled kit, such as routers and internet of things (IoT) devices.

Response Strategies

So how do we respond to the growth in DDoS attacks? Two main strategies are open to organizations, according to Bloor senior analyst Fran Howarth.

"One of the easiest ways to try to prevent a DDoS attack is to overprovision your infrastructure, especially those parts that are internet-facing. Organizations should also look to ensure that infrastructure is geographically widespread and that anycast, a technique that allows multiple servers to share the same IP address, is deployed," she explains. "This, however, can be an expensive option and is not for everyone. An alternative is to subscribe to cloud-based services that will handle the traffic overload in the cloud before it even reaches your network."

However, while there are certainly firms out there that can help, the industry as a whole has been slow to address the threat. "I still believe there is a long way to go," argues Howarth. "There are many vendors and service providers with their own offerings, but I see little evidence of any co-ordinated, concerted effort to develop and standardize. We are, though, starting to see a greater emphasis placed on regulation."

KPMG cyber security director, Jim Fox, believes all industry stakeholders can do their bit: "More can be done by sharing information in near real time on the nature of the attacks and a more co-ordinated response between target firms, internet service providers, security vendors and government," he tells *Infosecurity*. "Ultimately, governments need to work to disrupt the organized crime groups undertaking those attacks, and that will require difficult and painstaking international action."

What Lies in Store

So what of the future? More regulation is likely, according to Howarth. She says that under amendments to FFIEC rules, US financial institutions must now have DDoS mitigation technologies in place, although no individual tech was specified.

"With DDoS attacks on the rise, and increasing in complexity, size and sophistication, more organizations will be hit and more regulation is likely," she says. "We are also seeing more co-ordinated attacks against specific industries, which is likely to continue."

DDoS attackers will continue to evolve their methods to outwit the security vendors into 2015 and beyond, for example with SYN floods and application layer attacks. A report by DDoS mitigation firm Black Lotus also recently claimed that more countries, like Vietnam, India and Indonesia, would emerge as major sources of attack traffic thanks to their sheer number of infected endpoints, especially mobile phones.

According to KPMG's Fox, cyber-criminals will "continue to find more and more obscure protocols and vulnerabilities to amplify the effect of their attacks. We may also see more aggressive or disruptive attacks which aim to take down target systems by directly exploiting security vulnerabilities – or target the routing infrastructure of the internet itself."

Hacktivist groups such as Anonymous often attack targets with DDoS campaigns

It's not all doom and gloom, though. For Quocirca's Tarzey, there could come a time when all but the most sophisticated DDoS efforts can be dealt with by the majority of organizations: "I'd argue that anyone with a good spam filter never really sees any spam, but ten years ago it was a real problem. They're still sending the spam out but we've got the problem under control. [In time] we'll have the network locked down well enough to defend against the obvious DDoS attacks."

Tarzey adds that, "There's more at stake from being online today. It's the reason why the industry is more focused on the issue. This is a good thing because it means the industry is responding. So watch this space."

The Cyber-Threat of Things

There is an increasing landscape of risks facing well-connected businesses, and security practitioners must act now to mitigate them, explains **Wendy M. Grossman**

By the end of Laura Poitras's documentary about the Snowden revelations, *CitizenFour*, Edward Snowden and Glenn Greenwald are so worried about surveillance that they sit side by side and write each other notes on paper sheets carefully shielded from the camera and discuss only in vague monosyllables. It's not paranoia if they're really spying on you.

The incoming constellation of technologies known as the internet of things (IoT) is bringing with it new security concerns that only a few years ago would have sounded like paranoia but are increasingly realistic. In November, a Reddit user posted a story about a boss's computer that was infected with malware after plugging an infected e-cigarette into the USB port to recharge.

"The funny thing about it," says Rik Ferguson, vice-president of security research for Trend Micro, "is that it's not a new thing. Production line malware has been built into hardware like digital photo frames and others for many years now. The oldest example I could find was 2008." What matters more, he says, "is how you manage any devices being connected."

The predicted number of devices around the world that will be online-enabled within five years is around 50bn

> As a business you should be looking at how you mitigate the risk in the data center
>
> Rik Ferguson
> Trend Micro

Lagging Behind

The underlying problem, says Adam Westbrooke, product director for UK-based Ovo Energy, is that manufacturers build to customer requirements: low cost, ease of use, and high functionality. Adding security tends to interfere with at least two of those – but the risks associated with breaches are wide: escalating attacks, unchecked access points to more complex systems, and hidden surveillance. He cites, for example, a recent survey of cheap tablets that found many are released with developer access still enabled and even spyware installed. All of these build on existing vulnerabilities.

The head data scientist for Massachusetts-based BitSight, Stuart Layton, says that one consequence of his company's efforts to create objective ratings of the security effectiveness of other companies is that, "People are just beginning to realize how poorly their security has been configured up until now. We're trying to tell people so they can make changes."

At this early stage of the IoT, Layton is seeing what experts have been warning from the beginning: devices of all types accessible via the open internet – webcams in companies, printers, industrial-grade network switches, and mail servers, many with manufacturer-installed backdoors that are thoroughly documented in manuals that are easily accessible.

"What's kind of alarming about the internet of things is that the technology industry, despite being in technology, has a pretty bad track record on maintaining the security of devices," Layton explains. "Small companies won't update, users won't be aware how connected they are, and they pose a real security threat to themselves and anyone connected to them."

The key to change, he adds, is ensuring you know what your public-facing network looks like, reviewing policies governing traffic passing over your network, and regular self-scans to ensure nothing unexpected has been able to connect in or out.

Device or Data?

However, Ferguson suggests that focusing on the devices themselves – as in Black Hat talks – is to some extent misguided. Instead, he says, "What hackers are going after is the data," which, he adds, means the cloud. "In large part, as a business you should be looking at how you mitigate the risk in the data center as well as the devices connected to the corporate network." Even with something as personal as a heart rate monitor, the risks lie primarily in how the data is transferred, stored, and processed. "These are all data center questions," Ferguson summarizes.

Despite that, some risks invoke the scene from *CitizenFour*. In mid-2014, the consultancy NCC Group demonstrated compromises of smart TVs and electronic hotel door locks. The researchers made three main points. Firstly, manufacturers assume that only other machines, not humans, will communicate with these devices and therefore security doesn't matter. Secondly, manufacturers in the embedded world still think 'security by obscurity' is a reasonable strategy, forgetting that internal schematics and technical manuals including default passwords are all easily accessible on the internet. Thirdly, vulnerabilities present in devices when first deployed – such as the decision to run everything on some smart TVs as root – are likely to persist for years. Who patches a car – or a light bulb?

"I think you have to make the assumption that a lot of these devices should be untrusted and treat them accordingly," says Rob Horton, NCC

CELEBRATING 20 YEARS

Join Europe's biggest free-to-attend information security conference & exhibition

infosecurity® EUROPE

02-04 JUNE 2015 | OLYMPIA | LONDON | UK

Securing the connected enterprise

Collect **CPE/CPD** credits

WHY YOU CANNOT MISS INFOSECURITY EUROPE 2015

98.1% of visitors attending Infosecurity Europe in 2014, were satisfied to completely satisfied

96.6% of visitors are likely, or more than likely to attend in 2015, of which 81% are more than likely to return

84.1% of visitors are very likely to recommend participating in Infosecurity Europe to a colleague

97.2% of exhibitors were satisfied in 2014 and 80% have already rebooked to participate in 2015

ROI £447,528,560 of future orders expected to be placed with exhibitors as a direct result of Infosecurity Europe 2014

REGISTER YOUR INTEREST NOW
www.infosec.co.uk

Part of infosecurity GROUP Organised by Reed Exhibitions

Patching cars may well become routine in the IoT era

Group's European managing director. He advises that, whenever a new device is connected, security practitioners should assess whether it introduces insecurities into the network that provide an entry point and what the impact of a compromise would be.

"I know of a company where the video conferencing system would allow you to dial in and it would automatically pick up, but the TV wouldn't necessarily turn on," Horton explains. The resulting scenario was very like last year's season-ending episode of the TV show *The Good Wife*, where a law firm gained the advantage over its opponents by listening in on an apparently disconnected conference room.

"If I were a cyber-criminal, would I target lots of different companies, or would I go for law firms? They're aggregators of really sensitive information such as mergers and acquisitions. Your threat as a company comes from many different aspects."

Escalating Risk

Despite the spooky nature of this complex and less predictable environment, Kim Larsen, a senior client executive for Verizon, argues it isn't really new: "Machine-to-machine communication, which is the foundation of the internet of things, is something that's been going on for a long time."

On the other hand, he agrees that the IoT can exacerbate existing risks. One often cited data point in the 2014 annual *Verizon Data Breach Report*, for example, is that organizations commonly take up to six months to detect a data breach.

When even the office coffee machine presents a threat, clearly the parameters of corporate IT are shifting

"In the internet of things environment that could be very bad," Larsen says. Both manufacturers and purchasers of such systems therefore need to ensure that security is built in at the outset rather than applied afterwards. The desktop computer model – release and update – will not work in this environment. SCADA systems are a good example of what not to do; legacy systems newly connected must change their threat model.

Production line malware can be found in a disturbing array of consumer electronics, from e-cigarettes to digital photo frames

Larsen continues: "This is why the companies who do this for internet of things devices need to be very much aware that cyber-threats are a huge issue they need to mitigate from the beginning and not try to solve afterwards." Among the risks he lists is manipulating sensor data in ways that damage the system – for example by allowing the water pressure to get too high, or creating power spikes and denial-of-service attacks.

Risks like these are beyond what most security practitioners are used to. As Piers Wilson, head of product management for Tier3, a Sydney-based company specializing in security monitoring solutions, puts it, "The effects will be real. The coffee machine will overheat, healthcare will stop monitoring, your car will stop. So the implications are going to be real things rather than just flows of data and credit card information. A part of the physical world will change."

This is a particular problem for organizations where IoT technologies will be an integral part of delivering the business. These include healthcare, logistics, delivery services, education, and manufacturing, where incorporating sensors into existing automated production lines will be the next stage of development. The key for Wilson will be ensuring that systems are designed to deal with failure scenarios and that good monitoring will catch anomalous behavior that might indicate problems.

Security By Default

The ideal would be to build secure products, write secure software, and deploy secure systems. Decades of software development, however, has shown how difficult a proposition that is.

Wil Rockall, a director in the cybersecurity advisory team for KPMG, highlights this issue when he says that, "It would be a real shame if we went and, through lack of foresight, designed those systems to operate exactly the way we operate enterprise IT systems – inherently insecure products upon which we put layer upon layer of security products and then products on top of that to compensate for the weaknesses – rather than design them as inherently secure as we can."

> 95% patching sounds impressive, but 5% of one billion devices is a large number
>
> Wil Rockall
> KPMG

However, he adds, "There are always going to be bugs and problems. It's hard to write really secure software, so we have a chance to really think about those things and do it intelligently rather than rush and blunder in with the same models."

A complicating factor is the sheer volume of devices analysts expect will be deployed: we're counting in billions. At that rate, the law of truly large numbers kicks in. As Rockall says: "95% patching sounds impressive, but 5% of one billion devices is a large number that makes it attractive to attack if you're a criminal or a terrorist."

A possible way to remedy that, he suggests, might be a legislative shift in allocating liability. "Who owns a piece of internet of things technology? Does the fridge manufacturer retain liability for all the things the fridge does? Do you have to pay for the two tons of yoghurt it orders?"

Frank Palermo, senior vice-president of the Millennial Solutions Group for Massachusetts-based IT services company Virtusa, favors being able to turn off or isolate misbehaving devices. In cars, for example, the entertainment system should not be hooked into safety-critical systems such as braking or steering.

Wilson notes that an added difficulty is that these technologies will arrive in the workplace without involvement or approval from the IT department, who are not the people historically tasked with buying items like coffee machines. "Technologies like that are not seen as IT projects."

Taking control will be hard. Despite the risks, Trend Micro's Ferguson warns that security practitioners will have no more success keeping connected devices out of the workplace than they did previous consumer technologies like mobile phones, tablets, or social networks. His advice: manage, rather than deny, their use.

"It's an evolution for security departments," he says. "Stop being the department of no; start being the department of how."

WWW.INFOSECURITY-MAGAZINE.COM HAS A BRAND NEW LOOK

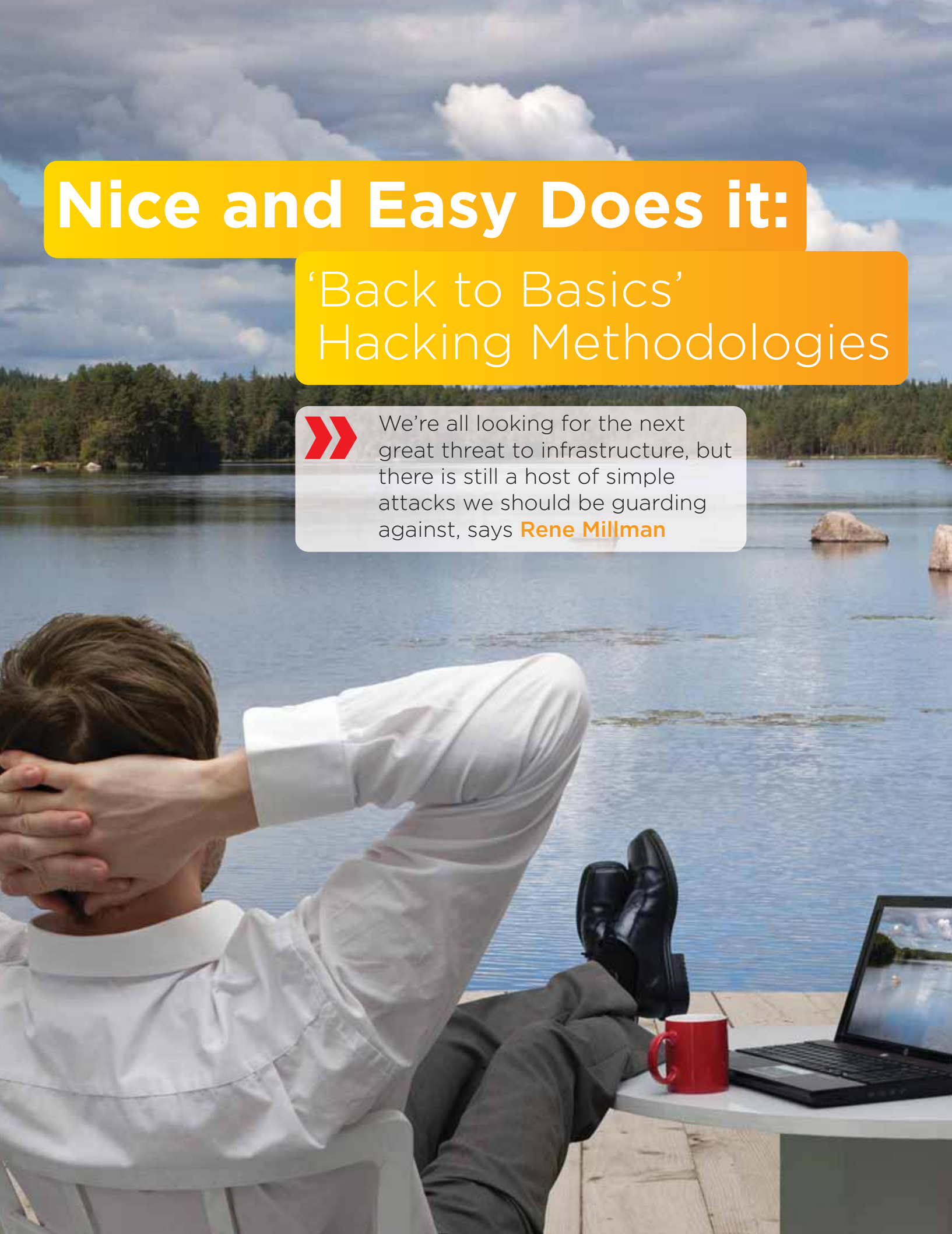
GIVING INFORMATION SECURITY PROFESSIONALS EVERYTHING THEY NEED TO DO THEIR JOB IN ONE PLACE WITH GREATER EASE

NEW FUNCTIONALITY INCLUDES:

- IMPROVED NAVIGATION AND SEARCH FUNCTIONALITY - GIVING USERS ACCESS TO MORE RELEVANT INFORMATION THAT IS EASIER AND FASTER TO FIND
- UNIQUE CPD MANAGEMENT TOOL NOT AVAILABLE ANYWHERE ELSE
- AUDIENCE POLLING TO CROWDSOURCE OPINIONS
- COMMENT TO ENCOURAGE GREATER INDUSTRY DEBATE AND COLLABORATION
- ENCHANCED MEMBER CONTENT INCLUDING: THE LATEST INDUSTRY REPORTS, WHITEPAPERS, WEBINARS AND EDUCATION OPPORTUNITIES

WWW.INFOSECURITY-MAGAZINE.COM

info security
STRATEGY | INSIGHT | TECHNOLOGY



Nice and Easy Does it:

'Back to Basics' Hacking Methodologies

We're all looking for the next great threat to infrastructure, but there is still a host of simple attacks we should be guarding against, says **Rene Millman**

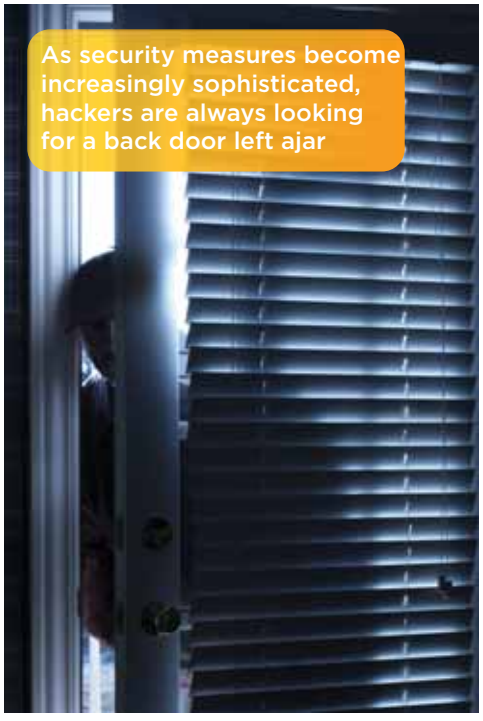
The security industry likes to think it is in an arms race with cyber-criminals. These hackers are busy dreaming up the next new way of breaking into infrastructure and, as an industry, we try to find ways to defend ourselves from ever more esoteric dangers.

To a large extent this is true, but this does sometimes mean we overlook many of the threats we think we have already overcome. In the same way we have come to think of diseases such as tuberculosis as being defeated (it hasn't and it's still a major problem in some parts of the world), basic hacking practices can still yield results for criminals intent on stealing from organizations.

It makes sense for hackers to try something easy first when looking to gain access to infrastructure. The quick wins for these criminals can sometimes be overlooked by firms when it comes to deploying an IT security strategy.

Finding the Easy Way In

The path of least resistance is attractive to criminals. "Hackers are beginning to realize that security measures are becoming increasingly sophisticated," says Boudewijn Kiljan, EMEA chief technology officer at Wave Systems. "This is why we are seeing fewer 'full frontal' attacks, and more that seek to go in through a credible sidedoor, such as an enterprise employee."



> We are seeing fewer 'full frontal' attacks, and more that seek a credible sidedoor
>
> Boudewijn Kiljan
> Wave Systems

Kiljan adds that this type of attack is becoming more prevalent, as this 'middle man' provides the gateway to a world of useful and lucrative information.

Richard Braganza, senior consultant at security consultancy firm Context Information Security, says that, in his experience, the path of least resistance usually involves going for the low-hanging fruit – in other words, the easy pickings that effortlessly bypass defenses and go unnoticed.

He gives the example of WiFi. When organizations set up corporate wireless networks they will tend to use the strongest security provided by Microsoft, as the security fits nicely with Windows domains. "This may sometimes be a mistake," says Braganza. "That is unless special measures are taken."

On the face of it, this looks secure as you have to enter the same credentials to get onto the wireless network as you would use normally to access the rest of the corporate network.

"It ticks all the boxes for users and IT to think the WiFi is secure. And therein lies the problem. This default use of Windows' strong enterprise security for WiFi actually leaves the company completely wide open to anyone outside the building," Braganza says. He adds that a user does not check who the WiFi network belongs to: "Anybody could set up a fake WiFi network with the same name and ask for user credentials. Once the attacker has the user credentials they can use them on the real WiFi network and, hey presto, they now have a foothold on the corporate network."

Getting Social and Getting In

But it is not just the simple attacks on computers and networks we are still worried about; no amount of technology can adequately defend against social engineering attacks. Defcon ran a 'social engineering' capture the flag contest last year and the majority of ten major US companies targeted were happy to hand out information which would be useful reconnaissance for future attacks.

"A worst-case scenario to illustrate this would be the Target compromise where the refrigeration company they used was identified and targeted as a way into Target's network, ultimately allowing hackers to breach point-of-sale terminals and steal details of millions of credit cards," says Paul McEvatt, senior security architect at Fujitsu's Security Operations Centre.

Social engineering has become the mainstay of modern cyber-attacks, whether directed en masse in phishing campaigns or specifically targeted in so-called 'spear phishing' attacks, according to Kevin O'Reilly, senior consultant at Context Information Security.

"The reason is that, as technology evolves and security holes in systems are closed, the weakest link in the chain remains the same: the human at the keyboard," he says. "Piquing the curiosity or engendering trust with a carefully worded email is the most universally reliable way of eliciting the clicking of a link or the opening of a weaponized document leading to the installation of a malicious backdoor on a system."

Malware writers may look to use web browser or email attack vectors – those that the enterprise has the least control over, says Kiljan. One of the most high profile cases of this type of attack was in relation to the RSA breach, which broke through the RSA's SecureID token technology.

Carefully worded phishing emails can easily socially engineer recipients into clicking bogus links

"The breach was caused by an email attachment, which was likely opened by an employee due to the promise of interesting information," says Kiljan. Once the attachment was opened, it acted like a stepping-stone for malware to begin to infect the device and retrieve sensitive information. Upon creation of the connection, the hacker can gain remote access to all information stored or connected to the device and, at the end, to the IT infrastructure.

"This type of attack can occur in a distinct window, from when the vulnerable connection is first made to when developers can counter the attack with a counter-threat or patch," adds Kiljan.

Something Old, Something New

Perhaps the main issue here is that while technology progresses in order to combat the latest threats, why can't these protect against the more basic threats? Are the tighter defense mechanisms of more modern operating systems doing enough to deter cyber-criminals?

Modern operating systems have two problems they must deal with when trying to build a secure operating platform. Jeremy Demar, director of threat research at Damballa, says the first problem is that these operating systems are not completely new creations: "Even when a new version of your favorite one comes out it likely has a lot of code written decades ago," he says.

The second issue is that users demand new features, functionality and backwards compatibility. "A good example of legacy code in modern systems is the Shellshock vulnerability," says Demar. "This vulnerability first existed in code written in 1989."

> As technology evolves... the weakest link remains the human at the keyboard
>
> Kevin O'Reilly
> Context Information Security

He adds that CVE-2014-6332 is a perfect example of what happens when you try to remain backwards compatible. "This exploit works on Internet Explorer from version 3 to 11; the code is only still around for backwards compatibility. Many times when an operating system tries to create proper defenses, users get upset and quickly find ways to turn it off. A good example of this one is the introduction of User Account Control (UAC) in Windows."

Tackling the Problem

There is very much a need for security professionals to do more to tackle basic threats. Paul Glass, senior associate at international law firm Taylor Wessing says that, "To a degree, more can be done by security professionals, and the more sophisticated tools now available can prevent many low-level hacking approaches." He adds that, "Risk assessment as to what data actually needs to be protected, and putting in place controls to achieve that without hampering the business, is key."

Glass says that these steps need to be accompanied by education and awareness of employees, as IT tools are only part of the picture: "For example, spoof emails that look as though they come from another employee but actually contain a malicious link are almost always easily identifiable by employees, but will often not be caught by IT tools. GCHQ estimates that about 80% of

The easiest pickings for hackers are the low-hanging fruit – attacks that bypass complicated defenses

known attacks would be defeated by embedding basic security techniques, and education is a key part of that process."

A Threat to Consumers and Enterprise

Criminals threaten both consumers and enterprises, and while both attacks are similar in that they involve persuading the end user to click on a link or open an email attachment, the difference is in the malicious payload.

"For consumers, it tends to be a more crude threat aimed at the masses with a low expectation of click-through for a backdoor trojan that is only sophisticated enough to do its basic job without creating too much noise," says Context's Kevin O'Reilly.

"For the enterprise, the lure is often slicker with a more intelligently worded email appearing more trustworthy or with more context, leading often to a more advanced exploitation method (perhaps a rare and therefore more valuable zero-day vulnerability in a web browser or plugin) and almost always leading to a more advanced backdoor threat."

Glass says that, at the enterprise level, there is usually a bigger prize, so the time put into more advanced social engineering can be worth it for a hacker. He adds that, "This is particularly the case if the target has access to large volumes of personal data, valuable commercial assets, or large volumes of credit cards or bank accounts, and a hacker can remain undetected, slowly extracting data, over a long period of time."

Glass says that education remains key at an enterprise level; also critical are access to data (restricting access to only those who really need it) and the ability to quickly identify when security is compromised and take action. "As Target found out, having advanced security tools is of little use if the IT security team doesn't use those tools to identify a threat."

The Key Skills for New Recruits ...Point..

Hard Tech Skills Remain the Priority

The new year promises to be a challenging one for organizations recruiting new personnel within information security. Last year saw a number of high-profile threats, attacks and breaches at the forefront of the news including Heartbleed, Shellshock, Microsoft's SChannel flaw and the Sony hack, which continues to be played out. Last year, according to PwC's *Information Security Breaches Survey*, 81% of large organizations had a security breach, and the cost of said breaches in the UK was nearly double 2013 levels.

As such, the need for new recruits in the information security industry has never been higher. A considerable skills shortage across all levels in the industry currently exists, from graduates and junior positions, to CISOs and heads of security. This looks likely to remain the case throughout 2015 as more organizations realize that cybersecurity has become a persistent, all-encompassing business risk and look to mitigate this through hiring additional security personnel.

For the vast majority of our clients seeking new recruits within their security teams, a strong technical understanding is currently the most important attribute for the majority of roles. Having spoken with a number of other CISOs and hiring managers, I would argue this is generally the case within the wider security industry at the moment.

This issue is more pertinent for less experienced or entry level professionals, where the need for a good technical understanding overwhelmingly supersedes softer skills and business knowledge which can be gained through training and in-post experience. Graduate positions advertised invariably stipulate a degree in IT, engineering or maths, with further education or relevant certifications within information security a distinct advantage.

If we consider trainee or junior positions where professionals have the opportunity to move into the security sector from elsewhere, again the vast majority assume a technical background or require hands-on IT experience. Vulnerability assessors and pen testers, security programmers, network or system security analysts, IAM administrators, NOC and SOC analysts, incident response analysts and junior security consultants are all roles that offer an opportunity to move into the industry, but are far more readily available to those with an existing technical background.

The majority of current security training and development courses available (IISP, (ISC)², SANS, CREST) also require delegates to have a good technical understanding prior to attending, and whilst internal training and development is now increasing, hiring managers continue to favour new recruits who have a fundamental knowledge of technology to those without.

For management and leadership roles, the emphasis on deep technical understanding does lessen, with more prominence on transferable business and softer skills. Here we can see a greater crossover of applicants from outside of the technical sectors who have an understanding of security principles and highly transferable business skills.

Indeed the role of a CISO these days sees the technical considerations as only a small aspect of overall responsibilities, working much more at the strategic level within the business. By and large in my experience, however, those at the management layer of security within organizations will have a technical background, albeit historic, from a hands-on perspective.

Not having a strong technical background does not mean you cannot enter the sector – some excellent opportunities are available to those with little or no technical understanding, notably within areas such as risk and regulatory compliance, sales support, security awareness and training, as well as recruitment.

However, I would argue that in the current climate where organizations remain understandably risk-averse in their recruitment strategy, having a strong technical background allows new recruits to explore a far higher number of avenues.

As cybersecurity is a profession developing momentum, and with security training, career development and entry paths continuing to mature, I can see no reason why this shouldn't change in the future, which will be a positive move for everyone.

AUTHOR PROFILE

Chris Dunning-Walton is the owner of InfoSec People Ltd, a specialist recruitment business focusing on the UK information security sector, launched in 2008. Chris has over 11 years' experience providing value-add recruitment solutions up to executive level to some of the UK's biggest employers, as well as a host of information security SMEs.

.....Counterpoint....

Time for a Softly-Softly Approach

As an independent consultant in the field of information security I have seen a lot of changes over the years. From infosec being an area that was often overlooked by businesses, it is now one of the fastest growing areas in technology. This change has led to an infosec 'skills gap' where many companies are citing they cannot hire anyone to fill their vacant infosec roles. Indeed, I am regularly asked by various companies if I am aware of anyone looking to change career and, if so, whether I could point those people to the company's vacancy.

Yet, at the same time, I talk to many professionals who lament that they cannot break into the information security field. Many cite that they feel they are not technical enough to get into the area, or that they do not have enough experience.

Many believe that to be successful in infosec you need a very strong technical background. The argument being that, as infosec is so reliant on technology, you need to be strong technically to understand not only how that technology works, but also how it fails, so that you can better secure it. While this may be true in a number of specific infosec roles, such as penetration testing, security/system administration, malware analysis, and development of security tools, I contend that this is not true of all roles.

The headlines have recently been full of security-related stories which cast an aura of highly technical adversaries breaking through companies' defenses with ease. Yet, if we look at the root causes behind these breaches, or indeed read the excellent *Verizon Data Breach Investigations Report*, we see that many breaches are not that technical and are in fact caused by simple issues such as the human factor, lack of training, ineffective operation processes such as patch management, or good old lack of security awareness.

None of the above areas requires strong technical skills to address and, indeed, as information security is becoming more of a mainstream concern for many businesses, strong technical skills, to the detriment of other softer skills, may in fact turn out to be a disadvantage. For companies to have effective information security, the area has to become embedded as a key component of overall business activity.

Responsibility for information security is now too important to be left solely in the hands of the technical experts. Instead, everyone from the board right down the organization's hierarchy must share that responsibility. In order to do so we need to be better able to communicate to business stakeholders why they need to care about information security. This involves many soft skills such as being able to present complex infosec concepts in simple terms to employees from various business backgrounds.

We also need to be better able to ascertain information security risk and how those risks can impact on the business. Too often I see reports going to senior management not being actioned upon because they are littered with too much technical detail and not enough on the business impact. As an industry we need to better communicate with key decision makers and not just focus on the technical issues.

As a result, the key requirements I look for in new recruits to the industry is a passion for the topic and the ability to communicate clearly and effectively. Indeed, some of the most successful people I have worked with come from non-technical areas.

Many other respected professionals within the field will also claim they do not have a technical background. Yes, technical skills are important and we will always need specialists in the more technical aspects of our industry, but technical skills are no longer the be-all and end-all for a successful career in information security. Technical skills can be taught and improved upon, whereas the soft skills required to communicate effectively with others are harder to teach.

Over time, technology becomes dated, as do the related skills. As an individual progresses through their career, they will also find they move more and more away from pure technology roles. Passion, curiosity and the ability to communicate are skills that will last throughout one's career and will also make us more effective infosec professionals.

AUTHOR PROFILE

Brian Honan is an independent security consultant (BH Consulting) based in Dublin, Ireland, and is recognized as an industry expert on information security. He is COO of the Common Assurance Maturity Model and founder and head of IRISSCERT. Honan also sits on the technical advisory board for a number of innovative information security companies and is on the board of the UK and Irish Chapter of the Cloud Security Alliance.

» MARKET ANNOUNCEMENTS

Managed File Transfer Solutions

Pro2col recently released the latest edition of its free *Ad Hoc / Person to Person File Transfer Comparison Guide*. Featuring industry-leading vendors including Accellion, Thru, Cryptshare, Egress, Ipswitch and more, the guide covers solution basics, business strategy and technical details.

The easy-to-read guide enables SMEs, enterprises and value-added resellers to see at a glance which solutions best fit their requirements. James Lewis, managing director of Pro2col commented: "The third version of the A*d Hoc File Transfer Comparison Guide* is our best yet. It includes the leading technologies in this space and provides useful information on which solutions to consider. For those wanting further assistance, Pro2col provides a range of other value-add services to guide end-users and resellers alike from needs analysis through to eventual implementation."

To download this free resource visit Pro2col's web site at www.pro2col.com

ESET Launches Next Generation of Business Security

ESET recently announced the upcoming launch of its next generation business products, including: ESET Endpoint Antivirus and Endpoint Security for Windows and OS X, ESET File Security for Microsoft Windows Servers and ESET Remote Administrator.

Protect endpoints better than ever with fast and effective real-time scanning, plus an enhanced exploit blocker and advanced memory scanner. The new GUI can be completely hidden from users and managed exclusively via the new and improved ESET Remote Administrator.

Based on consultations and in-depth interviews with IT professionals, ESET Remote Administrator now has a web-console which allows a security overview of an entire network plus access to data visualization with extensive drill-down capabilities. ESET Remote Administrator has had a complete overhaul to offer a more user-friendly and effective experience.

ESET File Security now provides support for virtual environments and offers native clustering of file servers. Take advantage of the award-winning scanning available in ESET Endpoint Antivirus and Endpoint Security developed specifically for Windows Servers.

Launching in Q1 2015, ESET's business products are going to protect essential business data like never before.

LockLizard Releases Document DRM for the Browser

LockLizard has released a web viewer enabling users to view PDF DRM protected documents through a web browser. LockLizard delivers a highly flexible, granular and secure document DRM solution for PDF documents that enables document publishers to control who can view documents, for how long, where and when. Web Viewer extends document delivery by enabling protected PDF documents to be viewed on any operating system or device without the need to install any software or plug-ins. Web documents can be locked to specific IP ranges so that they can only be viewed from, for example, a work location, and documents can be made to instantly expire after a number of views, days, or on a fixed date. LockLizard is used worldwide by Fortune 1000 companies, governments, small and large publishers, training companies and research institutes, preventing unauthorized use and misuse of their information. To learn more visit www.locklizard.com

Protegrity Announces Data Protection and Monitoring in Hortonworks Data Platform

Protegrity USA Inc., provider of data-centric enterprise data security solutions, recently announced an expanded partnership with Hortonworks to strengthen and expand the availability of data-centric protection and monitoring in the Hortonworks Data Platform (HDP). Protegrity Avatar for Hortonworks extends the capabilities of HDP native security with Protegrity Vaultless Tokenization (PVT) for Apache Hadoop, Extended HDFS Encryption, and the Protegrity Enterprise Security Administrator, for advanced data protection policy, key management and auditing.

Protegrity Avatar for Hortonworks is currently available exclusively to Hortonworks customers; with a per-node maintenance fee, users receive direct end-user access to Protegrity resources and software releases. The growing relationship underscores the importance of data protection in the modern data architecture, and the need for security solutions that preserve the ability to operationalize and utilize sensitive data.

"Hortonworks customers have asked for frictionless data protection within their modern data architecture. We're excited to expand our relationship with Protegrity and increase the ease at which our customers can now access and deploy," said Bob Page, VP Partner Products at Hortonworks. For more information and to download the free Protegrity Avatar for Hortonworks, go to www.protegrity.com/products-services/protegrity-avatar-for-hortonworks

Publication Helps IT Security Managers Understand Current Security Issues

The third issue of the Wick Hill *Guardian* is now available online from Wick Hill or as a mailed-out printed version. With its aim 'to advise, not advertise', the Wick Hill *Guardian* is a great read for IT security managers looking to understand more about existing and future security issues, as well as suggesting the type of solution best suited to deal with them.

Barry Mattacott, Marketing Director at Wick Hill commented: "The *Guardian* features authoritative articles from some of the world's leading experts in IT security. It's an informative and entertaining read, which will help IT security managers navigate their way through today's rapidly changing IT landscape."

Leading companies who have contributed features include: WatchGuard, Kaspersky Lab, Check Point Software Technologies, Barracuda Networks, macmon secure, VASCO Data Security, and of course Wick Hill.

The wide range of security topics covered includes the importance of gaining visibility into today's widely dispersed networks if you want to stay secure; whether or not to use encryption; and issues around mobile device security. There is also a free audiobook on network access control.

To view the Wick Hill *Guardian* online or request a mailed-out hard copy, please visit www.wickhill.com/guardian

AlgoSec Streamlines Connectivity Management for Data Center Migrations

The AlgoSec Security Management Suite v6.7 simplifies and streamlines end-to-end security policy management for large-scale server migration and decommissioning projects, while ensuring service delivery and business continuity.

Key new features include:

- Simplify Large-Scale Server Migration Projects: Through AlgoSec's built-in workflows, the user simply selects the servers to be migrated, and AlgoSec then automatically identifies all the applications that are affected by the planned migration. AlgoSec then generates the necessary change requests for the underlying network traffic flows, all while ensuring the integrity of the security policy and network access.
- Visualize Application Connectivity: The new dynamic, graphical map provides unprecedented up-to-date visibility of all applications and their connectivity requirements. The map also highlights blocked connections and color-codes business applications based on their vulnerability scores for easy troubleshooting and risk analysis.
- Simplify and Automate Connectivity Provisioning for Shared Applications: Users can now create templates that automatically apply the appropriate connectivity flows for shared applications such as antivirus, backup, DNS etc. to cut management overhead and simplify change management.
- Ensure Compliance with More Regulations: New compliance reports include the Health Insurance Portability and Accountability Act (HIPAA), the Internet Banking and Technology Risk Management Guidelines (IBTRM) of the Monetary Authority of Singapore (MAS) and NERC CIP version 5.0.

London Fire Brigade Protects Itself From Potential Liability Using Egress Switch

Egress Software Technologies recently announced the uptake of its flagship encryption platform, Egress Switch, by London Fire Brigade. The Switch platform enables London Fire Brigade to manage the secure exchange of sensitive electronic information with its network of third parties, including London's local authorities and the Met Police. In doing so, Switch is helping London Fire Brigade to ensure the appropriate level of protection is applied to all confidential information shared with these external organizations, and also addresses the potential liability for the Brigade for negligent disclosure or publication of personal information.

Vanessa Skinner, London Fire Brigade's deputy manager and safeguarding lead, explains: "During a recent review of London Fire Brigade's safeguarding processes and systems, our ICT security staff identified the organizational benefit, particularly in line with local authorities, offered by the secure electronic transmission of confidential information to third parties. As a result, we deployed Egress Switch to meet this need."

PFU iNetSec Smart Finder Instantly Identifies and Isolates Previously Undetectable Attacks

Organizations attacked by APT malware haven't always been able to detect attacks via traditional antivirus, signature-only-based IPS technologies or sandbox-based technologies. Today's attacks often disguise themselves as routine business communications, such as email transmissions or web traffic, and can lie dormant for long periods of time.

To address this problem, PFU Systems recently released the latest version of its iNetSec Smart Finder, the first comprehensive, easily-deployable endpoint visibility and network access solution integrating advanced intrusion prevention system (IPS) technology to automatically detect and immediately block APT attacks and remote access trojans designed to steal data from SMB and enterprise networks.

Carmine Clementelli, network security product manager at PFU Systems said: "iNetSec Smart Finder discovers and neutralizes these threats by dynamically adapting to changing network conditions. It analyzes and stops malware by detecting behaviors associated with APTs and malicious programs, including communications patterns produced by running scripts within a company's network. iNetSec Smart Finder is now an all-in-one solution that combines full network visualization of all wired and wireless devices and applications used, with the addition of new IPS features."

Linoma Software Releases Milestone Update for GoAnywhere Services

Linoma Software (www.goanywhere.com) recently announced the release of GoAnywhere Services version 4.0. The popular enterprise managed file transfer software now features a streamlined interface in addition to new collaboration and file sharing capabilities. All administrator and user components have been migrated to HTML 5 for a more modern and functional interface. The secure mail module has also been overhauled to appear and perform like a typical email client for employees needing to send large or secure file attachments. The star of version 4.0 is GoDrive, an on-premise enterprise file sync and Sharing (EFSS) solution that puts IT administrators back in control of file management. GoDrive combines:

- Familiar tools like drag-n-drop and image previews, making the employee adoption quick and easy
- Detailed audit logs which give management and compliance officers the peace of mind that all activity is well documented
- Proven security features of GoAnywhere Service's administrative tools, with the addition of device authorization and remote wipe capabilities

GoDrive files and folders are easily shared between users with advanced collaboration that includes file revision tracking, commenting, a recycle bin, media viewing and synchronization with Windows devices.

Google Chrome Provides FIDO U2F Security Key Support

Google recently announced an extra layer of security for Google accounts based on FIDO U2F support added to the Chrome browser, the first public deployment of FIDO U2F protocols and a major step in increasing internet security. FIDO U2F is an emerging open authentication standards initiative with strong support from more than 120 end-user and vendor companies in the FIDO Alliance.

In conjunction with this new functionality within Chrome, Yubico introduced the FIDO U2F Security Key, a new, secure two-factor authentication device designed to let users securely log-in to Google accounts and any number of service providers who have or will adopt the FIDO U2F protocol.

Stina Ehrensvard, CEO and founder, Yubico Inc., commented: "This news can't be overstated for anyone who desires better protection against hackers; whether consumers, security professionals, internet privacy advocates. Having a leading Internet browser adopt FIDO U2F signals the arrival of new and stronger options for authentication and security."

The new FIDO U2F Security Key is a specially designed YubiKey that relies on high-security, public-key cryptography. All it takes to authenticate is to touch the button on the key after it has been inserted into a USB port and the FIDO U2F Security Key provides a unique public and private key pair for each application it protects. Only those keys can correctly complete the cryptographic challenge required for authentication and a successful login.

Acuity Launches Latest STREAM Solution for Governance Risk and Compliance

Acuity Risk Management, the governance risk and compliance (GRC) software specialist, recently announced the release of version 4 of its popular STREAM Integrated Risk Manager software.

The configurable, scalable and easy-to-use software has been improved and extended in V4.0 with a range of new features including a report builder for custom reporting, a new API for third-party data sources and new 'risk delta' functionality for identifying and prioritizing the control improvements that will provide the greatest risk return on investment.

STREAM is used world-wide for automation of risk registers; integrated management systems, including ISO 27001, PCI-DSS, Cyber Essentials, ISO 9001; risk and control self-assessments, and to provide a business risk perspective on technical security data from scanning and monitoring tools.

Accompanying the STREAM V4.0 release are several additions to the library of pre-configured content available for use with STREAM, including the NIST Cyber Security Framework and ISO 28001:2007 Security Management Systems for the Supply Chain. Visit www.acuityrm.com for a free single-user copy of STREAM V4.0.

DataLocker Launches DL3 FIPS Edition

With individuals storing record amounts of data and files on external hard drives, the potential for data theft, loss or compromise is high. To address this, DataLocker, a leading developer of encryption solutions, recently released its DL3 FIPS Edition (FE), a new, FIPS 140-2 validated, military grade 256-bit AES encrypted, high capacity, external hard drive. Built on the proven foundation and success of its predecessor, the DataLocker DL3 FE provides unmatched usability and security with USB 3.0 speeds and unrivaled dual crypto processors.

"With DL3 FE, data is fully encrypted the instant that it is saved and with the highest level of cascading dual encryption. Data undergoes two passes of 256-bit encryption, the first pass being in XTS mode, the second pass in FIPS 140-2 validated CBC mode. Locked down and secured, every single bit of data on DL3 FE is double encrypted for added security," said Jay Kim, founder and COO, DataLocker.

DL3 FE adds a layer of military-strength encryption to storage devices that is easily secured and managed by the user without installing complicated software. Easy to use and platform independent, users can simply access their data with a personal passcode on the device keypad.

Go Hack Yourself... Really

..Opinion..

Organizations are very focused on building security defenses in an attempt to stop attacks, mostly from the outside. But IXIA's VP Fred Kost reckons they should spend more time taking on the role of the attacker and trying to defeat the very defenses they have worked hard to put in place

Let's face it, curiosity often gets the best of us. The desire to click on a file folder, such as the one named 'Finance', log in to an unauthorized application, or generally poke around the network in discovery mode is intriguing. Almost daily we hear about hacking stories and wonder how they did it. As it turns out, tapping into this could be a great way to bolster an organization's security posture and understand its ability to withstand attacks.

Typically, most organizations leave security to the IT security professionals. Organizations hire firms to conduct penetration tests to assess security technologies, processes and their readiness for attack detection and response. Is there an unpatched server on the network that is running a critical business function, or does the helpdesk give out credentials inappropriately when called?

Almost always, these pen tests identify some kind of risk or exposure. Additionally, organizations can use outside services or products to conduct vulnerability scanning. This is intended to find the holes before an attacker is able to make their way into the network. Both approaches have benefits and can help bolster security defenses.

Put on Your Black Hat

But what if, instead of just looking externally and hiring outsiders to do some of these security assessments, an organization were able to turn their internal employees – or at least some of them – loose to become a black-hat wearing, cyber version of James Bond?

Empower your own insiders to engage in exploratory mischief to find the holes and vulnerabilities in your network and security program. Imagine the value that an insider could provide from their security testing activities. For one, insiders understand the business and know where the 'good stuff' is located. They see it daily, but now they are empowered to click and attack.

Also, insiders are familiar with your defenses or policies and can work around them to abuse them in ways that an attacker would do if they were to get inside, creating havoc on your network and the data you are trying to protect. And while they may not normally try these activities, your immunity or amnesty program will allow them to help the organization find the holes and gaps.

A Combined Approach

As part of the 'attack yourself' exercise, organizations can complement the people aspect with additional tools or software to help uncover weaknesses. These tools can help companies get beyond the point of looking for software vulnerabilities to actually identifying weaknesses by using techniques like fuzzing, where unexpected and intentionally incorrect inputs are provided to try to cause a device to fail or to allow an attack to succeed.

In addition, these tools can simulate real world applications and attacks to test what the network can withstand beyond the human onslaught.

Could taking advantage of these tools actually help improve your defenses before the attackers find a hole? Could this exercise of hacking yourself actually make organizations more accountable and possibly expose the true strength of network security?

A retailer who passes a PCI DSS audit, for example, may believe they are secure enough to meet compliance requirements and therefore protected. But have they really done a thorough security assessment?

If an organization truly puts on the black hat and tries to breach its systems and their activities succeed, it may create more work in the near term. However, in the end, it will make their networks truly more secure, raise their understanding of their security, and help them identify opportunities for improvement.

AUTHOR PROFILE

Fred Kost is vice president of security solutions at Ixia and is responsible for managing the company's security and applications portfolio. He has over 15 years' experience in the information security field and speaks frequently on the subject. He has also held leadership positions with companies such as Cisco, Symantec, nCircle, Blue Lane Technologies and Recourse Technologies.

Slack Space

E-Cigarettes Smoke Out Security

It's a new year, and plenty of people are trying to kick it off right by, say, quitting smoking, or implementing a gym routine. Unfortunately, the former could be hazardous to your (IT) health: a batch of e-cigarettes from China was found to have malware hard-coded into chargers, in a move that sent at least one company's anti-malware protection up in smoke, as it were.

Reddit user 'Jrockilla' described the issue: "They finally asked the executive, 'have there been any changes in your life recently?'. The executive answered, 'well yes, I quit smoking two weeks ago and switched to e-cigarettes.' And that was the answer they were looking for. The made-in-China e-cigarette had malware hard-coded into the charger and when plugged into a computer's USB port the malware phoned home and infected the system."

It just goes to show that the ever-expanding universe of connected gadgets provides a rich playground for nefarious types. What's next: a fridge with mal-intent? A TV that watches you back? A fitness tracker that uploads more than workout stats? How about any and all of the above?

"While laptops have increasingly sophisticated protection against malware attacks, mobile phones, tablets and wearable technologies do not yet," said Phil Barnett, EMEA general manager at Good Technology. "Malware can spread to these devices very quickly and cause risk to consumers and businesses alike."

He added that, "Any company that allows its data to be stored on a mobile device needs a security and risk management policy that takes into account the diverse and expanding number of sources of potential threats."

You've Got to Know When to Hold 'Em…

Poker, as we know from *Casino Royale*, American Westerns and, of course, Kenny Rogers, can be serious business. Like losing your gold kind of serious (or potentially the GDP of a small island nation, in Mr Bond's case). Part of the game is bluffing, tells and ticks. You've got to know when to hold 'em and when to fold 'em. But what do you do against an opponent that has none of these behaviors?

When the (micro)chips are down, think twice if your opponent goes by the name 'CPR+'

According to a research paper, a computer algorithm has 'solved' poker – specifically, heads-up limit Texas Hold 'Em, which is a two-person, bet-limited version of the game (no going 'all-in' here). What this means is that, given an opponent's bet and the three community cards displayed during the game, the computer can pretty much be guaranteed to take one's money.

Granted, the authors of the algorithm admit that it is "weakly" solved, meaning that it can largely determine every possible outcome given the cards dealt – but not every time.

Still, CFR+, as the algorithm is known, is capable of solving extensive-form games that are several orders of magnitude larger than previously possible.

"Poker is a family of games that exhibit imperfect information, where players do not have full knowledge of past events," the researchers said. "Whereas many perfect-information games have been solved (like Connect Four and Checkers), no non-trivial imperfect-information game played competitively by humans has previously been solved."

So if someone wants to bring his buddy the computer along for poker night – know when to fold 'em.

And file this last tidbit under the 'obvious' tab: "Furthermore, this computation formally proves the common wisdom that the dealer in the game holds a substantial advantage."

Amtrak Goes Off the Rails

The famous revelation in the 1980s that the Pentagon was using part of its not inconsiderable military-industrial budget to buy astronomically priced toilet seats forever solidified the image of no-oversight and waste in the weeds of government bureaucracy. Now, fresh intel shows that the US Drug Enforcement Agency has paid hundreds of thousands of dollars for Amtrak passenger data that it could have gotten for free.

Ah, data collection. It's the new $1000 toilet seat when it comes to US government spending.

An Amtrak inspector general report discovered by Senator Chuck Grassley, the senior Republican on the Senate Judiciary Committee, shows that since 1995, a former Amtrak employee has been selling passenger data to the DEA, for the total sum of $854,460.

The Amtrak employee was a "secretary to a train and engine crew" – and has since been let go. Even so, Grassley said that it "raises some serious questions about the DEA's practices and damages its credibility to co-operate with other law enforcement agencies."

Amtrak collects a range of information in the process of selling tickets, as many online retailers do, including credit card numbers, addresses, travel itineraries, emergency contact details, and in some cases, passport numbers and dates of birth.

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

Parting Shots

All the usual New Year fuss about 'fresh starts' and 'self-improvement' can grate on more cynically minded individuals. Each year is just an arbitrary period of time, these people are quick to point out. What do you really expect to achieve by buying that pair of gym shoes in the January sales? We all know they'll end up dust-coated under the stairs, probably around the same time that the 'Teach Yourself Japanese' book ends up in the charity shop window.

Well-intentioned as many of our New Year's resolutions start out, lots of us have a habit of assuming that the transition of one 12-month period to another will somehow give us new powers overnight. We'll be more active; more adventurous; more charitable; less like our old selves… all the time forgetting that these things take time, dedication, hard work and, often, a fundamental change in mindset.

But a new mindset is exactly what is needed. In order to avoid repeating yesteryear's mistakes, and really instigate positive change, complacency is off the menu.

For information security, 2014 was an *annus horribilis* – and the transition to 2015 presents an opportunity for businesses to take a long hard look at their security practices and really re-assess their approach. After all, if the last 24 months have taught us anything, it's that the old methods aren't adequate, and haven't been for some time.

This fact was brought home harder than ever in 2014. Sony Pictures took a major hit in November, and however skilled and well-resourced the adversaries, fundamental mistakes were made by the entertainment giant. Leaks reveal that passwords for Sony accounts were stored in a folder labeled, unambiguously, 'Passwords'. Sony Pictures chief executive, Michael Lynton, deployed a password that included the word 'Sony', his initials, and a one-digit number. This kind of practice does not hint at a high level of security awareness within the organization.

Target, meanwhile, was finally ruled negligent by a Minnesota court in December for a data breach in which 40 million customers' payment card details were leaked. The diagnosis? Poor network sequestration whereby a HVAC contractor's access credentials enabled hackers to gain access to sensitive data. An early warning system that detected anomalous activity was even ignored for a time.

All businesses should expect to be breached, because there is no truly impenetrable security. Simple login credentials, if stolen, are enough to cause critical damage to a business. But though breaches are now considered inevitable, that does not exempt companies from shouldering the blame when incidents do occur if the highest safeguards were not in place.

Victim-blaming is a terrible thing, given that the perpetrators of online and computer-enabled crime are the real scourge of this digital age. But we cannot be naïve, and unfortunately, as cybersecurity is still in its infancy, companies that do fall victim are going to be held up as examples and subjected to serious scrutiny and criticism – regardless of whether we agree with this or not.

So how can you or your company avoid having your dirty laundry aired in public in 2015? Use the new year as an opportunity to address the fundamentals. This goes for everyone in the organization's decision-making hierarchy.

Instead of forging ahead with the decision to keep deploying the latest, shiniest next-gen solutions, think simple. What is it you are trying to protect? And where is that vital information stored? How is it accessed? Who has access? Has the nature of that access changed, and if so, has your security policy changed to reflect that?

Given that data is the key asset, it's important to figure out where that data is, and where it is going. Also think about how it is protected. Answering these questions is the first step on the road to assessing whether your security policy is up to scratch.

We shudder to think that weak passwords are still deployed at the highest level. But it still happens. Maybe it's time to reconsider whether the venerable username and password combo is adequate.

Consider also the increasing shift to virtual environments and mobile business models. Is your mobile-working policy fit for purpose, and do you really know how much data is leaving the organization?

Assess not only the state of your security, but also your emergency response plan. If a breach is detected, it's important to have the right measures in place to minimize impact. And finally, keep communication flowing within the business to keep on top of the problem. Finger-pointing and assigning blame is going to be the least of your concerns in the face of the potential damage of a breach that is allowed to happen through shoddy security. Make sure cybersecurity is a business-wide responsibility.

> Use the new year as an opportunity to address the fundamentals

Will those new gym shoes be gathering dust come spring? Possibly. But while you can put off running a marathon for another year with few repercussions, neglecting your New Year's cybersecurity resolutions could have far-reaching and serious implications.

Mike Hine, Deputy Editor

HAVE YOUR SAY

in the

National Security Survey

and WIN great prizes

Share your views on the current trends and security needs by completing the National IT Security Survey. As a Thank You for taking part we are offering some truly great prizes. Plus, on completion of the survey you will receive either a mobile PowerBank or Bluetooth speaker*, or you can opt for a donation to charity on your behalf. We will also send the survey results to every participant when the survey closes.

As an IT professional we are very interested in discovering your security plans and concerns for the coming year. Here is a great opportunity to share your views on the immediate future of IT security.

Support and sponsorship from some of the biggest names in Network Security allows us to offer some exceptional prizes, including:

- 6 x Beats by Dre Headphones
- 4 x GoPro Cameras
- 3 x Sonos Play HiFi systems
- 1 x Parker Duofold pen

Complete your survey at:

www.nationalsecuritysurvey.com/ismag

*Random Selection

beats by dr.dre

SONOS

PARKER

GoPro

Sponsored by

Barracuda KASPERSKY lab VASCO THE AUTHENTICATION COMPANY WatchGuard WICK HILL

WICK HILL

Telephone: 01483 227600

email: info@wickhill.com

WICK HILL

infosecurity®
EUROPE
• 02-04 June 2015 • Olympia • London •

Intelligent security
Protect. Detect. Respond.
Recover.

You can't put a price on high-quality education

REGISTER for the world's biggest **free** Infosecurity Education Programme!
www.infosecurityeurope.com

CELEBRATING 20 YEARS
02-04 JUNE**15**
OLYMPIA**LONDON**UK

REGISTER FREE NOW

- Access to the experts and industry leaders
- Learn from inspirational speakers
- Network, share, collaborate and build relationships
- Discover new and innovative security solutions
- Earn CPD and CPE credits by attending the free education programme

Engage with Infosecurity Europe on Twitter: @infosecurity #infosec15

Managed by:
infosecurity™ GROUP

Part of:
Reed Exhibitions®