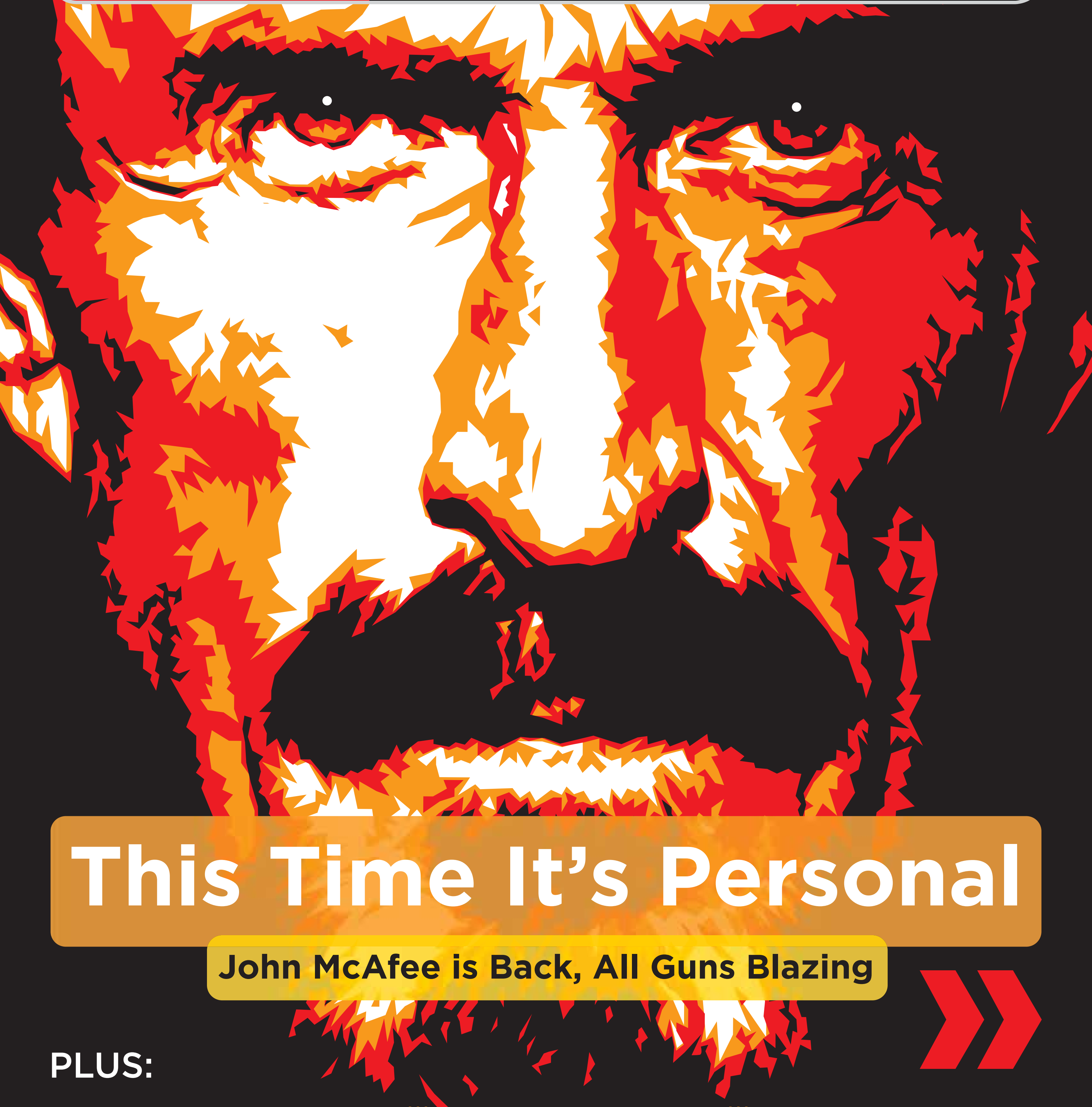
Q3 /// 2015 /// VOLUME 12 /// ISSUE 3

STRATEGY /// INSIGHT /// TECHNOLOGY

infosecurity



This Time It's Personal

John McAfee is Back, All Guns Blazing

PLUS:

WINDOWS SERVER 2003 EOL /// THREAT INTEL SHARING /// SECURING SMART CITIES

Contents

July/August/September 2015

REGULARS

OPINIONS

INFOSECURITY

EDITOR & PUBLISHER
Joseph O'Halloran
joseph.ohalloran@reedexpo.co.uk
+44 (0)208 4395648

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:
James Ingram
james.ingram@reedexpo.co.uk
+44 (0)20 89107029

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

Rosalia Lazzara
rosalia@showtimemedia.com
+44 (0)1462 420009

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

DIGITAL MARKETING CO-ORDINATOR
Karina Gomez
karina.gomez@reedexpo.co.uk
Tel: +44 (0)20 84395463

PRODUCTION SUPPORT MANAGER
Andy Milsom

ISSN 1754-4548

Disclaimer of warranties and limitation of liability
Reed Exhibitions Limited uses reasonable care in publishing materials available in Reed Exhibitions Limited's *Infosecurity* magazine and websites. However, Reed Exhibitions Limited does not guarantee their accuracy or completeness. Materials available in Reed Exhibitions Limited's *Infosecurity* magazine and websites are provided "as is" with no warranty, express or implied, and all such warranties are hereby disclaimed. The opinions expressed by authors in Reed Exhibitions Limited's *Infosecurity* magazine and websites do not necessarily reflect those of the Editor, the Editorial Board or the Publisher. Reed Exhibitions Limited's *Infosecurity* magazine websites may contain links to other external sites. Reed Exhibitions Limited is not responsible for and has no control over the content of such sites. Reed Exhibitions Limited assumes no liability for any loss, damage or expense from errors or omissions in the materials or from any use or operation of any materials, products, instructions or ideas contained in the materials available in Reed Exhibitions Limited's *Infosecurity* magazine and websites, whether arising in contract, tort or otherwise. Inclusion in Reed Exhibition Limited's Infosecurity magazine and websites of advertising materials does not constitute a guarantee or endorsement of the quality or value of such product or of the claims made of it by its manufacturer.

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

Placing Down a Stake In Constantly Moving Ground

As the Rolling Stones once said: please allow me to introduce myself. I'm Joe O'Halloran and it's my pleasure to be stepping into the shoes of Eleanor Dallaway for the next year during her maternity leave, building on the phenomenal job that she has been doing here, as editor and publisher, for so long.

After more years than I'd like to mention reporting on IT security, and even working for a leading vendor of security products and services for over five years, I feel qualified to say that there are not many sectors quite like this one.

And what better time to reflect on this than during the peace and calm following Infosecurity Europe 2015? Twenty years is a good birthday to celebrate, and the industry's premium event certainly lived up to expectations.

The undoubted star turn of the event was John McAfee. The industry legend and pioneer – he is both, whatever your opinion on him – did not disappoint, blazing in and leaving a trail, not of devastation, but of devastatingly good soundbites in his wake. Read some of these on page 18 where we interview security's *enfant terrible*.

At a reception at the show, McAfee braved delegates with a no-holds-barred Q&A. He was grilled on a number of topics, mostly surrounding privacy. But he wasn't asked about the meta-narrative developing during the event around the 'logical' need to re-allocate resources from preventing incidents to dealing with their aftermath. It wasn't just the specialists in response pushing this line – in fact one delegate at a session proclaimed that AV is dead. It's amusing to think of how McAfee, one of the fathers of antivirus software, would have responded to the assertion.

But is it dead? Has detection and prevention suddenly become so unimportant? These are important questions. After all, the threat landscape sure isn't diminishing. In June 2015, the latest threat report from John McAfee's old firm reported a 165% increase in ransomware attacks in the first three months of the year, while increases in Adobe Flash malware soared 317% compared with Q4 2014.

Believing AV is dead is a huge and potentially dangerous assumption, said industry stalwart Jack Daniel as he was inducted into the Infosecurity Europe Hall of Fame. Daniel warned that any advocates of the 'detection in marked demise' doctrine, who felt compelled to simply rush headlong into response, had better be pretty darned good at protecting their infrastructure.

Leading provider of network security and DNS services, OpenDNS, warned at the show that the increased demand for the use of internet of things devices in the enterprise is opening new avenues for faster exploitation. The risks from such wide penetration are increasing even in some of the world's most regulated industries.

> “Despite the plethora of technologies and services, fundamentally, security is about people

Even sanctioned IoT devices are now increasingly operating outside the control of IT departments because they rely on cloud-based and hosted network infrastructures. Many companies are basically under-prepared for their use.

Also at Infosecurity Europe, PwC introduced its *2015 Information Security Breaches Survey*, which found that almost three-quarters of small UK businesses, and 90% of large organizations, have experienced a security breach, roughly a 10% increase for both on last year. PwC also discovered that the nature and type of threats that organizations now face have changed, with data leaks and attacks from unauthorized outsiders of most worry – almost 70% of large UK organizations were attacked by unauthorized outsiders in 2014, up from 55%.

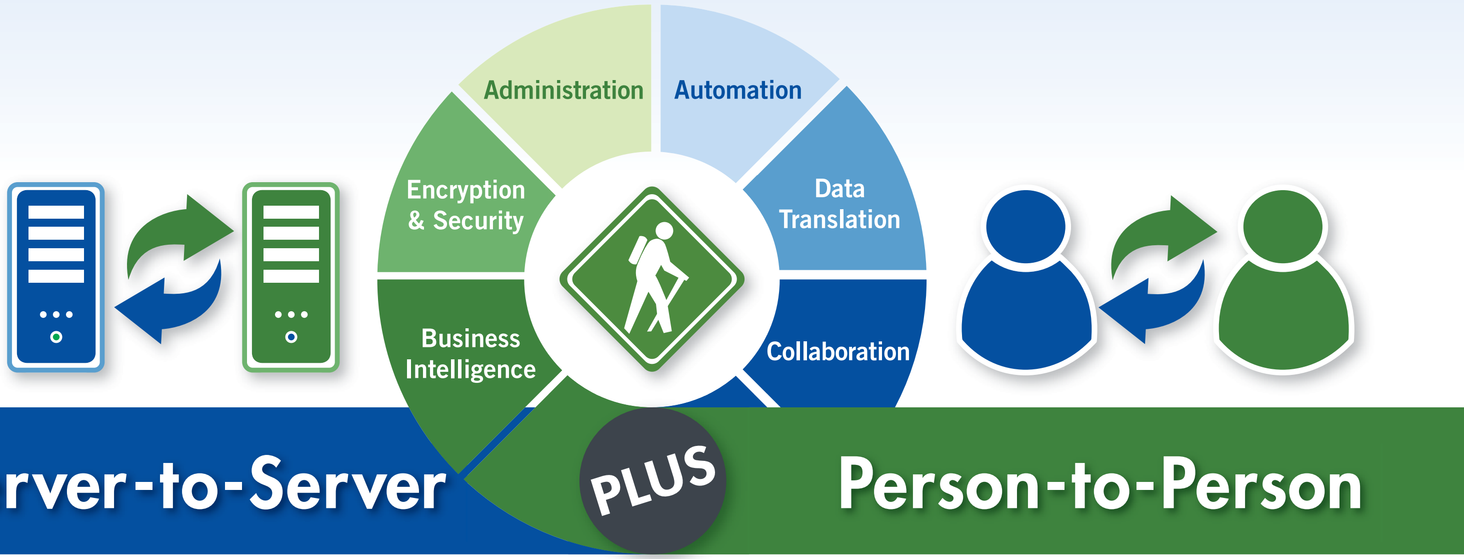
Richard Horne of PwC explained that, “Dealing with breaches is now a fact of life.” Yet what he did not do was advise making a drastic move away from protection. Instead, he suggested, “People are starting to realize that cybersecurity is not about fixing technology; it's about fixing the way we use technology.”

This is a huge point. Despite the plethora of security technologies and services that were on display at Infosecurity Europe, fundamentally, security is indeed all about people. It's all about the nature of the attacker, what their motivations and objectives are, and the character of people whose human nature makes them fall prey to such attacks. It's about the policies and procedures that we, as people, want to implement in our businesses, and how we go about making them happen. It's all about us.

I hope you enjoy this issue of *Infosecurity* Magazine – full with stories of how people define and deploy security practices.

Joe O'Halloran, Editor

Secure File Transfer



Server-to-Server

Person-to-Person

Simplify File Transfers with GoAnywhere™

GoAnywhere Managed File Transfer automates and secures file transfers with your customers, vendors and enterprise servers.

Through a browser interface, GoAnywhere MFT allows your organization to connect to almost any system (internal or external) and securely exchange data using a wide variety of standard protocols.

GoAnywhere MFT can parse XML, CSV and XLS files to/from databases, and includes the ability to encrypt file transfers using Open PGP, SFTP, FTPS, AS2, HTTPS and AES.

Visit GoAnywhere.com for a free trial.

> “GoAnywhere MFT monitors queues and automates encrypted file transfers (SFTP, FTPS, HTTPS).
>
> We currently have 45,000 scheduled and ‘triggered’ transfers running daily.”
>
> *One of the Largest*
> *North American Railroads*

Try it for FREE

GO ANYWHERE™

GoAnywhere.com 800.949.4696

a managed file transfer solution by

LINOMA SOFTWARE

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

Business as Usual

The NSA has experienced its biggest legislative setback in nearly 40 years – but there's a fishy smell to it, reports **Danny Bradbury**

Two years after Edward Snowden blew the whistle on the NSA, Congress has passed a law to rein in its powers. But will it really matter?

The USA Freedom Act finally passed on 2 June. It curtailed bulk data collection at the NSA, which had been vacuuming up metadata about domestic US phone calls and storing them in vast databases. This is the biggest legal ruling on surveillance since the mid-1970s, when the Church Committee was formed to investigate intelligence activities within the US government, following Watergate. It found a widespread telegram interception program, Operation Shamrock, dating back to 1945, whereby the NSA enlisted three US communications carriers to secretly provide it with copies of all telegrams sent to foreign parties. This also enabled it to gather information about US citizens on a secret watchlist.

The outcome was the 1978 Foreign Intelligence Surveillance Act (FISA), which established an oversight procedure, and the Foreign Intelligence Surveillance Court (FISC) whose jurisdiction is activities relating to foreign intelligence.

A Long History of Surveillance

The Church Committee, recalled investigator L Britt Snider in 1999, "caused the NSA to institute a system which keeps it within the bounds of US law and focused on its essential mission." Then came 9/11: one of whose outcomes was a culture of

1945 – Government approaches telcos to secretly provide telegrams for national security purposes

1952 – NSA formed

1975 – Church Committee formed to investigate intelligence activities in the US

1978 – Foreign Intelligence Surveillance Act (FISA) passed to provide more oversight on foreign intelligence activities

secret surveillance of US citizens, and, ultimately, the biggest exposé in history.

In 2001, President Bush signed an order allowing the NSA to monitor international telephone calls and email messages without warrants to search for terrorists. The agency, criticized by the 9/11 Commission for its adherence to strict oversight, began collecting information without applying for FISC approval.

It later transpired that the NSA had conspired with AT&T, BellSouth and Verizon to gather a vast database of domestic telephone call records. In 2013, the *Guardian* uncovered a court order requiring communications giant Verizon to give the NSA metadata from calls within its systems, both domestically and to other countries. That order was obtained by the FBI from the FISC, part of an ongoing bulk telephone metadata collection program authorized by the court in 2006.

The US government was then able to use these records to search all telephone numbers that directly communicated with a target, and also search any numbers that were in contact with those numbers (a second 'hop'). Then, by conducting another third 'hop', NSA officials could determine who constituted a target. Making things worse, Section 215 of the Patriot Act, passed in 2001, made it easier for intelligence agencies to gather this and other information. It amended FISA, making it easier to gather information from both US and non-US

President Reagan signs Executive Order 12333, which provides extensive information collection privileges to the US intelligence community

1981

9/11 attacks on US. Patriot Act becomes law. Section 215 grants extensive information collection privileges to the US intelligence community. President Bush authorizes the warrantless collection of data about international telephone calls and emails under Stellar Wind program. NSA launches secret program to gather domestic US call data from telcos

2001

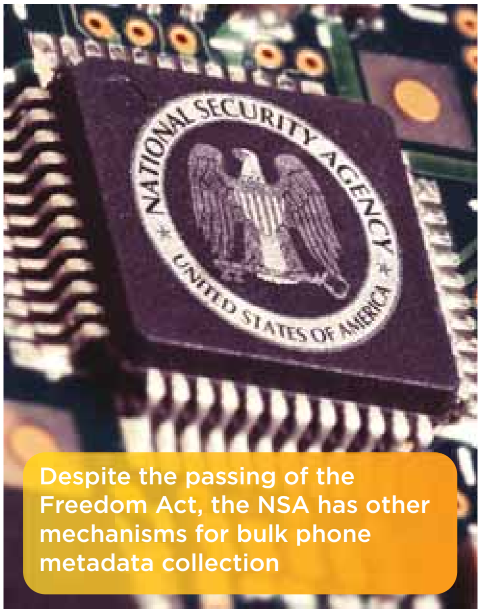
citizens, and expanded the scope of surveillance orders.

Court Decision

Jim Sensenbrenner, who penned the Patriot Act, said in 2013 that bulk collection of call record metadata was "never the intent" of the legislation. Yet only weeks later, the American Civil Liberties Union sued director of national intelligence, James Clapper, and others in the government. The Union argued the program must be stopped and records purged, as such activities violate the first and fourth amendments. Its case was finally successful in May 2015.

By that point, Section 215 was nearing its end-of-life, due to 'sunset' on 1 June; Congress was busily working on extension legislation. The USA Freedom Act had already been voted down once in the 113th Congress.

A watered-down version of the bill, sponsored by Sensenbrenner, was under negotiation. It would extend the Section 215 provisions, but with significant caveats designed to quash the bulk collection of telephone metadata.



Despite the passing of the Freedom Act, the NSA has other mechanisms for bulk phone metadata collection

A Red Herring

The Act failed to pass by midnight on 31 May, leaving the intelligence community with dramatically reduced surveillance powers. Congress panicked. On 2 June, the bill was passed. The new legislation curtailed several collection methods. It targeted the collection of business records under Section 215, but also National Security Letters, which the FBI can use to demand customer records from organizations including telcos, while preventing them from informing customers.

The law also placed restrictions on the use of 'pen registers', devices that monitor specific phone lines. These were used to gather bulk metadata information until 2011, following a FISC-approved order in 2004. The USA Freedom Act requires that these collection methods be used with specific selectors to limit the number of records gathered. It also appoints an amicus as an independent voice in FISC hearings, which have hitherto been held in secret.

On the face of it, this sounds like great privacy reform, and a vindication of Edward Snowden's whistleblowing. But privacy advocate and Resilient Systems CTO Bruce Schneier is highly critical: "It's definitely vindication, but it's also a red herring. It's both at the same time."

Retired NSA agent Kirk Wiebe, who worked at the agency from 1975 to 2001, has concerns about the act itself, and the adjustments voluntarily made by Obama in February 2014. He criticizes Obama's 'two hops' limit: "Although collection is limited to two hops, what if the first hop from a suspected/known criminal or terrorist is the IRS? That would mean everyone who ever called the IRS is two hops from the bad guy and subject to collection," he said. "So while pure bulk collection may end under the Freedom Act, 'bulky' collection is still possible."

> You're not allowed to collect surveillance data on people without probable cause. That separates us from East Germany
>
> Bruce Schneier
> Resilient Systems

Plenty More Fish in the Sea

The act may have helped to quash bulk phone metadata collection using the mechanisms listed, but there are others. One of these is Executive Order 12333, a Reagan-era presidential order which carries similar powers to a federal law. Written 20 years before the web existed, this law permits the gathering of metadata and message content. Former NSA agent turned whistleblower, William Binney, is particularly concerned about section 2.3C of the order, which authorizes intelligence agencies to collect "information obtained in the course of a lawful foreign intelligence, counter-intelligence, international narcotics or international terrorism investigation."

All of this creates a huge opportunity for incidental data collection about the communications of US citizens, he warns: "If you get any US data you can keep it and

FISA court authorizes bulk metadata collection program involving Verizon

2006

Stellar Wind terminated (according to government officials)

2011

Despite the additional scrutiny placed on intelligence agencies post-Snowden, some advocates worry that very little will change

distribute it, as long as you're looking for a terrorist or a dope dealer."

"The NSA does that under that criteria, but they keep all the data they collect," he adds. "Then the FBI and the CIA come in and look at the data internally in the US databases for anything that they want. There's no oversight to that."

EO 12333 isn't the only way to obtain information on US citizens, warns Julian Sanchez, a senior fellow and privacy rights watcher at the Cato Institute. Section 702 of the 1978 FISA legislation also grants data collection powers, he points out. It is less egregious than Reagan's order, still requiring a FISC review of data collection, although FISC plays no role in actually approving the target.

"At last count there are 90,000 targets under the authority. To my mind that fits as cleanly as anything could the definition of a general warrant," says Sanchez. "All of those communications are intercepted, including the communications of Americans."

Trawling for Data

Sanchez suggests that searching incidentally-collected domestic information stored in 702-related databases is a way of gathering information without a warrant, in what has become known as a backdoor search. This is what was taken out of the USA Freedom Act's final version. "The proposal was that, if you wanted to search these databases for American communications, you'd have to take the same steps as if you did it directly. That was unfortunately removed."

James Lewis, director at the Center for Strategic and International Studies, has a different perspective: "The Freedom Act is useful because the NSA used to authorize itself, and that isn't how it's supposed to work."

But ultimately, nothing much will change, he suggests: "It will change some of the procedures around collection and make the NSA and FBI jump through some additional hoops, but for communications surveillance, I don't think it changes very much."

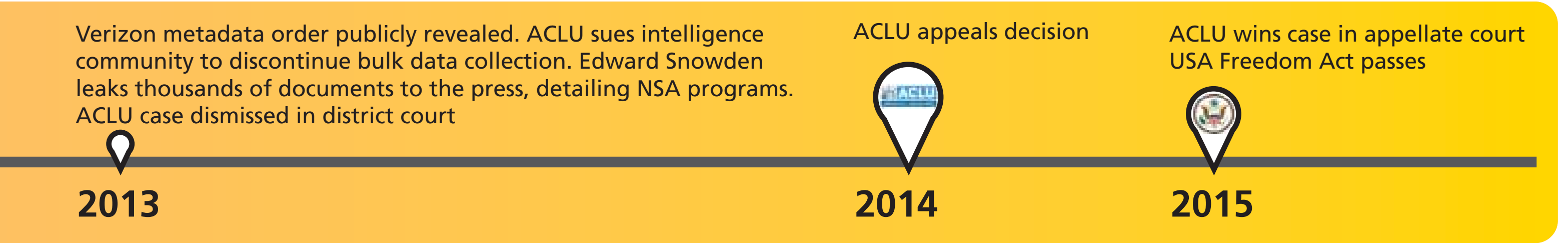
The USA Freedom Act also curtails some mechanisms already ruled illegal by appellate court, including the direct collection of bulk call metadata directly by the NSA. However, it still leaves the data in the hands of the phone companies, and allows it to be queried by the NSA using targeted selectors.

This worries Gene Tsudik, a professor in the computer science department at the University of California, Irvine. "This stuff represents a treasure trove of information, and an attractive target for attacks," he says. "I believe that if metadata has to be kept for some time, it is best to split it in a way that neither NSA nor the phone company can make sense of it, without cooperation."

There are cryptography technologies for that, but there are no provisions for this as it stands. In any case, the NSA is still legally capable of collecting bulk metadata and (in some cases) bulk content on foreign targets which generate significant amounts of data on US citizens inside the country.

Should bulk data collection be a part of the US surveillance machine? "Against innocent people? No," says Schneier. "That's not what democracy does. You're not allowed to collect surveillance data on people without probable cause. That's not one of the things we do. That separates us from East Germany."

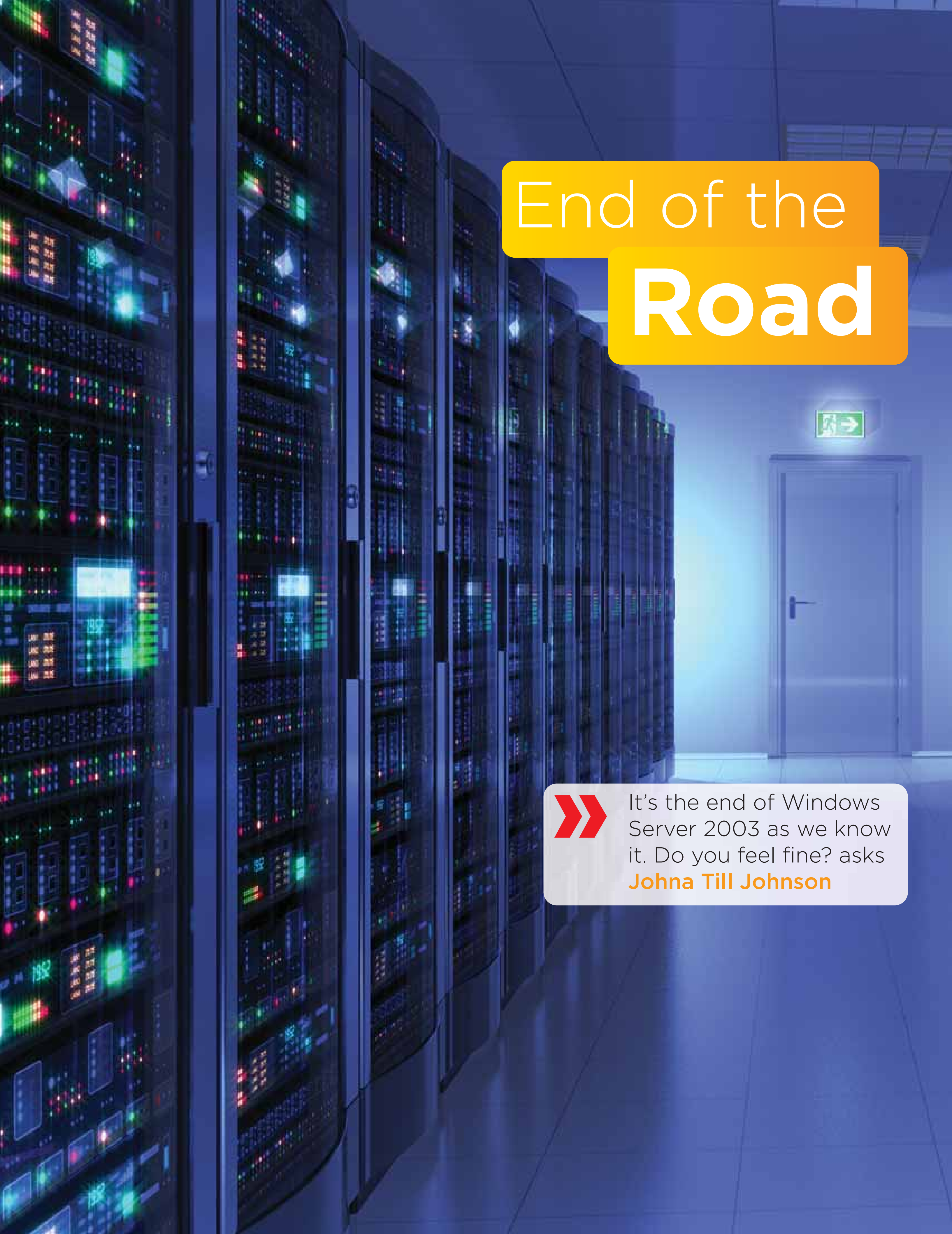
The battle between privacy advocates and surveillance hawks in the US has been long. And difficult. And it isn't over yet.



Verizon metadata order publicly revealed. ACLU sues intelligence community to discontinue bulk data collection. Edward Snowden leaks thousands of documents to the press, detailing NSA programs. ACLU case dismissed in district court

ACLU appeals decision

ACLU wins case in appellate court
USA Freedom Act passes



End of the Road

It's the end of Windows Server 2003 as we know it. Do you feel fine? asks **Johna Till Johnson**

Unless you've been living under a server rack for the past three years, you'll be aware that on 14 July Windows Server 2003 reaches its end-of-life. Microsoft will no longer provide general support, bug fixes, or security patches for the OS. The company will no longer even report on security flaws in WS 2003, and will cease to update or support the endpoint security tools offered for it.

If you're among the estimated near two-thirds of organizations (according to App Zero) that still have WS 2003 in your enterprise, it's not too late to take action. You have more options than you may realize, but it's imperative to tackle the problem now.

There are three main issues that will hit on 15 July. First is security; unsupported WS 2003 machines will create a huge vulnerability in your enterprise. As of early June, there have been 25 documented WS 2003 vulnerabilities in 2015, compared with 26 in total in 2014. These range from denial of service (DoS) vulnerabilities to buffer overflow to code-execution issues. So far, they've been patched, but that's not going to happen going forward.

And hackers know it: they're already going into high gear locating vulnerable servers.

"We've seen an uptick in scans, of hackers trying to take inventory to find out who's running these systems," says Chris Strand, senior director of compliance and governance at endpoint and server security firm Bit9 + Carbon Black. So the chances are extremely high that your systems will be hit in the 30 days immediately post end-of-life.

But it gets worse. The second major issue is compliance. Virtually every organization is subject to regulation – such as PCI, HIPAA, or Dodd-Frank – and most regulations require vulnerabilities to be patched within 30 days of discovery, something that's not possible if patch updates aren't happening. Moreover, if an organization is running outdated or unsupported software, it can be subject to additional fines and penalties. So regardless of whether your systems are actually compromised, you'll fail your next compliance audit.

Finally, there's the issue of cost. The cost of supporting an obsolete OS is high and will keep on rising, based on everything from the extra work required to keep the system running to the outmoded hardware it's likely running on. And for enterprises large enough to negotiate a custom support agreement (CSA) with Microsoft, fees can be exorbitant, starting at $1500 per server per year, and compounding annually. (And note that CSAs are only available to organizations that already have a remediation plan in place).

Supporting the WS 2003 operating environment will continue to be a slow drain on your resources, consuming time and effort you could have devoted to something else. The bottom line is that inaction is both dangerous and expensive. This is one deadline you can't afford to ignore.

> "We've seen an uptick in scans, of hackers trying to take inventory to find out who's running these systems
>
> Chris Strand
> Bit9 + Carbon Black

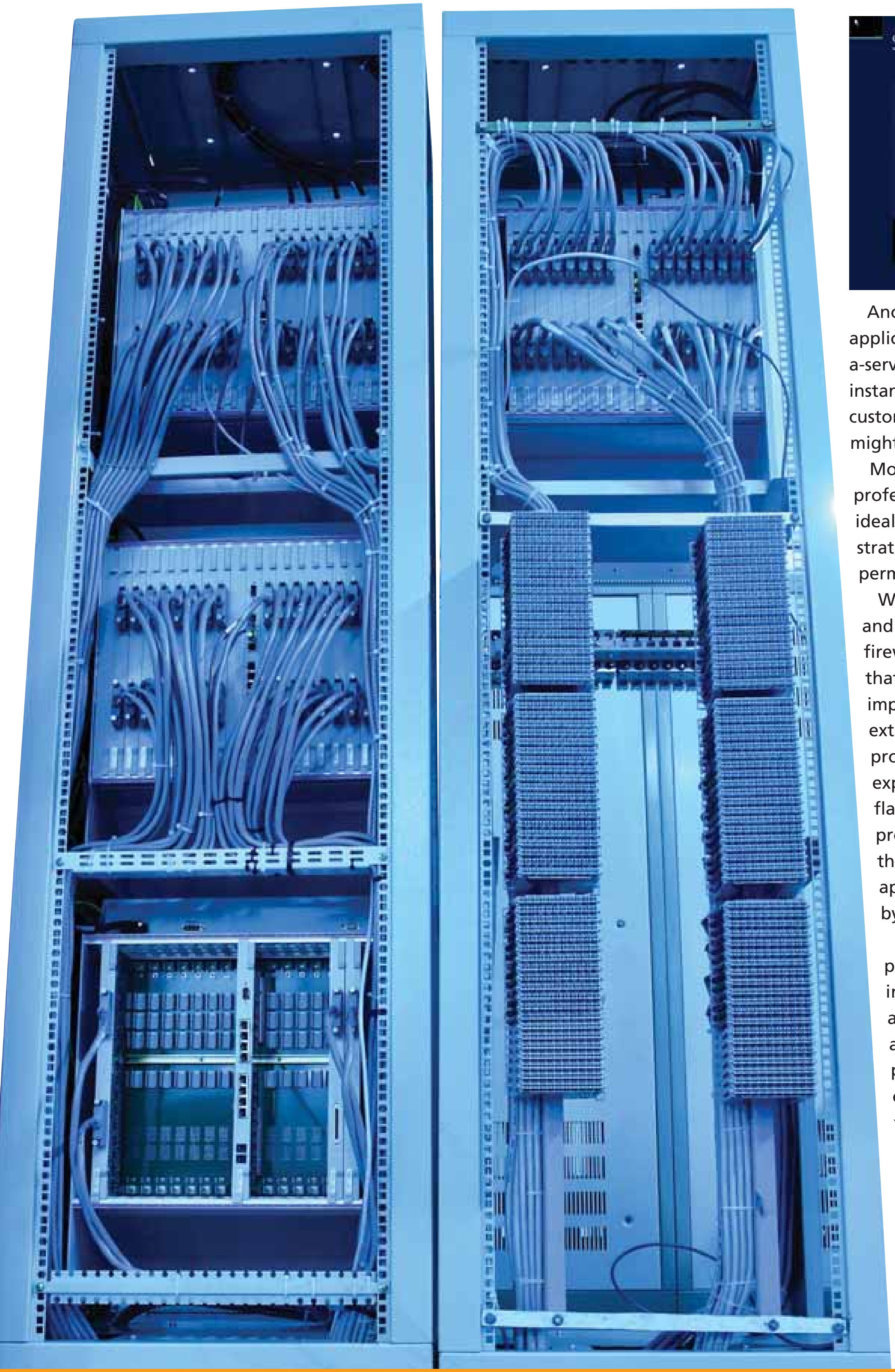
What's The Plan, Stan?

There are several remediation strategies for the WS 2003 end-of-life issues. The most obvious fix is to migrate applications off it. But to where? One option, of course, is to migrate to later OSs, most likely WS 2012.

Another is to take the opportunity to move to the cloud, specifically Microsoft's Azure. The challenge is that there may not be enough time. Re-architecting applications to run on a different OS (or porting them to the cloud) takes planning and effort. Apps still running on the old system are often hard to uproot, rewrite, or replace for a variety of reasons: close customization to the OS; a lack of application vendor support; or a lack of in-house staff to do a rewrite. So unless you have relatively few applications, migration is probably not a near-term solution.

Options for WS 2003 EOL Remediation

- **Server migration** – Migrate your applications to up-to-date servers, most likely WS 2012. Consider this if you have a limited number of servers and do not yet have a cloud strategy in place.
- **Cloud migration** – Migrate your applications to IaaS cloud services, most likely Azure. Consider this if you have a cloud strategy in place, and application migration makes sense in that context.
- **Application replacement** – Replace your applications with more modern ones, including SaaS. Consider this if you have a cloud strategy in place, and application replacement makes sense in that context.
- **Segmentation** – Move your WS 2003 machines behind firewalls and gateways, or in an extreme scenario, take them offline entirely. Consider this if there is a limited set of users accessing applications, but remember you won't be protected against app-layer threats or compliance concerns.
- **Augment with defense in depth** – Add defense-in-depth technology to your security arsenal. Look for products that can provide real-time monitoring, centralized logging and enforcement, compliance, and the ability to integrate into your strategy going forward. Plan a gradual migration away from WS 2003 over the next six to 30 months.



Migrating to WS 2012 is one option facing IT teams

Another approach is to replace your old applications entirely, relying on software-as-a-service (SaaS) or other solutions. For instance, rather than porting your elderly custom CRM application to WS 2012, you might opt to transition to, say, Salesforce.

Moving to SaaS is an option that IT professionals should seriously consider, ideally as part of an overarching cloud strategy. But once again, timing doesn't permit this approach as a quick fix.

What's left? You could attempt to isolate and protect systems by segmenting behind firewalls, load balancers or other systems that can filter connectivity. This will improve security from low-level and external attacks, but will be less able to protect from application-level attacks that exploit previously undiscovered OS-level flaws, or threats propagating within the protected space. This approach also has the weakness of making systems and the applications they support less reachable by the lines of business.

At the extreme, systems can be placed off-net entirely. This could apply in some healthcare, manufacturing, and other scenarios, for example when a system controls a machine tool or a piece of lab equipment via a dedicated or embedded 2003 server. However, the number of systems that can actually operate off-net is shrinking fast as systems increasingly depend on connectivity.

What's left? Fortunately, many security vendors have developed security products that use 'defense-in-depth' techniques such as virtual patching, application control, endpoint control, and ongoing monitoring to keep the servers protected beyond the end-of-life deadline.

Beefing up security by implementing such systems has two advantages. First, it buys you time to develop a more overarching strategy that covers not only WS 2003 but all your computing platforms. Most likely this will involve some combination of infrastructure-as-a-service (e.g. Azure), software-as-a-service, and private cloud. Since it's a big shift, you'll want to take your time planning and executing this strategy.

Second, moving towards a defense-in-depth strategy will increase your overall security stance. If you're still relying on protecting your systems by strengthening your perimeter, your security architecture is seriously out of date. Moving to a defense-in-depth approach will more effectively protect your entire enterprise, not just your obsolete WS 2003 machines.

Technical Considerations for Keeping Servers Protected Post End-of-Life

- **Ongoing monitoring** – The product you select should monitor systems in real time, not just daily or hourly.
- **Logging and provable enforcement of policies** – Your solution should be able to demonstrate to your auditors that threats have been stopped and vulnerabilities have been remediated.
- **Reporting** – You should be able to generate easy-to-read reports from your systems that can validate that the system is doing what it's supposed to be doing.
- **Integration into your broader security architecture** – It's important to think about your security architecture and roadmap: which solutions you have in place today, and which you'll be putting in place tomorrow and next year. Make sure your solution is compatible with both your current needs and your go-forward requirements.

Microsoft may negotiate costly custom support agreements with large organizations to extend support for WS 2003

Putting It All Together

So if you've still got apps running on WS 2003, what should you do? The answer depends on your environment. If there aren't many, and they aren't a critical part of your environment, you can migrate them to WS 2012 or Azure. Or, you can replace them with a SaaS solution, assuming your WS 2003 environment is sufficiently contained for this to be feasible in the few days remaining.

If your environment is more extensive than you can handle via migration or replacement, you can segment the servers (or take them offline entirely), assuming this doesn't affect usability. Note, however, that this is strictly an interim fix: you're still liable from a compliance standpoint, and you're still vulnerable to some forms of attack.

You could also invest in defense-in-depth solutions that provide both protection and compliance validation. This approach buys you time, and also moves you in the right direction from a security standpoint.

Assuming you opt for a solution other than migration or replacement, how much longer should you plan to keep your WS 2003 machines operational? The answer once again depends on how heavy your dependence on WS 2003 is. If your environment is extensive, you should accelerate your migration or replacement strategy, because securing and managing an obsolete OS (and its associated applications and hardware) is likely costing you quite a bit. If your environment is more limited and/or self-contained, you may be able to support the servers for longer.

A good rule of thumb is 30 months on the outside. That is, regardless of your situation, you should be off WS 2003 by 2018. Many of the security vendors won't commit to supporting the platform beyond 2018, and even if they did, it's almost certain that your hardware and overall architecture will be obsolete.

And remember, that's the *outside*: if you can wrap up a migration or replacement strategy by the end of 2015, so much the better. You'll have more time, energy, and resources to focus on doing something truly innovative for your organization.

Taking action doesn't necessarily mean an emergency forklift upgrade. There are plenty of options for buying yourself time and staying protected and compliant.

Better Together

Information sharing can be a win-win for public and private sectors, **Phil Muncaster** discovers, but there are still hurdles to overcome

Last year, pro-unionists looking to keep the United Kingdom from disassembling secured victory in the referendum on Scottish independence with a simple message: better together. It's a message that governments on both sides of the Atlantic are looking to spread to private sector organizations struggling to contain the sheer volume and sophistication of modern cyber-threats.

Combining forces by sharing key threat intelligence between public and private sectors should be a no-brainer: a clear win-win. But it has been complicated in our post-Snowden world by fears of over-sharing information with intelligence agencies that indiscriminately devour private data. Then there are the ever-present concerns over possible legal action or shareholder ire if threat information indicating a data breach leaks into the public domain. It's certainly not an easy sell for governments, and the patchwork of disparate frameworks, directives and legislation is growing ever more complex before our eyes.

At its very best, effective information sharing between public and private sectors should be a two-way street. On the one hand, government agencies and related parties would receive intelligence from a wide variety of endpoints on the ground to help them in ongoing investigations against state-sponsored hackers, hacktivists and financially motivated cyber-criminals. On the other hand, data flowing the other way – from the likes of GCHQ, the NSA and Europol – could be critical for CISOs and IT leaders hoping to pre-empt major attacks on their organizations and better fortify themselves against data loss.

Preventing such attacks and the data breaches which inevitably follow could save organizations millions. The most recent Ponemon *Cost of Data Breach* report put the average figure globally at $3.5m, 15% up from the previous year. The UK government, meanwhile, claimed in its *Information Security Breaches Survey 2014* that the average cost for small businesses had risen from £35-65k to £65-115k, and for large firms from £450k-850k to £600k-1.15m.

What's in Place

In the United States, the Department of Homeland Security's (DHS's) Office of Cybersecurity and Communications, the National Cybersecurity and Communications Integration Center, and US-CERT are heading up an over-arching strategy to "automate and structure" info-sharing techniques worldwide, both across industries and between public and private sectors. They're doing this by promoting the use of three community-driven technical specifications – TAXII, STIX and CybOX – which, according to US-CERT, are designed to "enable automated information sharing for cybersecurity situational awareness, real-time network defense and sophisticated threat analysis."

The DHS's Enhanced Cybersecurity Services, meanwhile, is a voluntary info-sharing program focused specifically on critical infrastructure operators. The DHS also works with sector-specific Information Sharing and Analysis Centers (ISACs) in industries including aviation, emergency services, health, nuclear, real estate, financial services and oil and gas.

In the UK, the coalition government created the Cybersecurity Information Sharing Partnership (CiSP) back in 2013. Now part of CERT-UK, it has 950 organizations and 2500 individuals signed up to receive real-time threat updates from the Fusion Cell, a joint industry and government team which creates alerts, advisories, regular summaries and bespoke threat analysis. There are also pilots under way to continue its work at a local level via Regional Organised Crime Units (ROCUs) established within the police force.

At a European level, there's no single framework on info-sharing – legal or otherwise – spanning all sectors, although there's a breach notification obligation on the part of telecoms firms to report to their regulators and at an EU level to ENISA. Data protection authorities also need to be notified if private data is impacted. Aside from the CiSP in the UK, there are other voluntary frameworks in member states such as MISP in Luxembourg, and NDN in the Netherlands.

> The public sector must… ensure that the threat exchange will be a lively two-way street
>
> Joerg Fritsch
> Gartner

A Problem Shared

But merely having such programs, whether they have legal backing or are voluntary, doesn't necessarily mean they'll be effective. The type of information shared can have a major impact on how useful it could be to the other party. Breach-related data such as timing, tools, techniques, procedures, and targeted sector can be incredibly useful, according to head of CERT-EU, Freddy Dezeure.

"More and more frequently the cooperation also involves the sharing of context in order to make prioritization of the information easier and to make the information actionable," he tells *Infosecurity*. "A lot of work is currently under way to make sure that organizations speak the same language when sharing information with each other."

For Jasper Graham, senior vice president of cyber technologies and analytics at Darktrace and former NSA technical director, information needs to go beyond mere file hashes and IPs.

"The tactics, techniques, and procedures (TTPs) have to be presented in a format that can be digested by everyone," he tells *Infosecurity*. "The way hackers are going about attacking particular systems, or a notable increase in attacks across a certain industry vector could show a shift in the black market and a need for a particular data type. It is important to understand these shifts especially when working to stay a step ahead of the attackers."

Bumps in the Road

Despite the proactive work being done by governments and other industry groups in this area, there remain serious concerns to address on both sides of the Atlantic before wholesale information sharing between public and private sectors can be achieved. These include doubts over how much information should be shared with agencies like the NSA and GCHQ, given the Snowden revelations of mass surveillance.

Then there are more practical concerns, such as privacy and anti-trust laws and the lack of a "single, well-accepted, machine-readable standard" for information exchange, according to Gartner research director, Joerg Fritsch.

"To give some examples, the public sector has to classify all information that would be good enough to support or threaten national security as 'SECRET'; it cannot freely share this data. That includes data about threats to privately held critical national infrastructure where no security cleared staff and infrastructure that is accredited to store classified data are present," he explains.

There are a number of emerging standards and architectures but no working and scalable blueprint, he adds, claiming that the current best channel is secured email – which is hardly scalable.

Fritsch also argues that another challenge facing current systems is that many

An executive order signed by Obama in February lays a framework for intel-sharing with federal agencies

emerging standards and frameworks seem to be driven by defense contractors, a fact which is keeping private sector participation low.

"If this is so, then it will stay a niche market tailored to the information sharing of players at selected CNI and governmental CERTS; it will hardly be a two-way system," he adds. "I expect that the benefit for the CNI operator may be moderate."

What Next?

A much-anticipated EU Network and Information Security (NIS) Directive – which would mandate greater information sharing, among other security measures – has yet to be finalized, but Fritsch is guarded about its chances of success.

"The public sector must for one get its act together to find out how it will ensure that the threat exchange will be a lively two-way street," he argues. "Secondly it still must become more effective and understanding how an appealing public-private threat exchange partnership will be possible. The NIS direction is a good first step, but it does not solve anything yet. It is still very early days."

In the US things are also heating up at a legislative level. An executive order signed by president Obama in February is designed to lay the framework for improved information sharing with federal agencies. In particular it will create new Information Sharing and Analysis Organizations (ISAOs) – which, unlike existing ISACs, will be more horizontal – and calls for common standards to share data more easily.

Elsewhere, much controversy still surrounds two pieces of legislation passing through Congress, which critics have branded surveillance bills in disguise: the PCNA and NCCPA. The PCNA in particular has been slammed by rights groups because it could allow law enforcement to use the data it collects to investigate crimes outside of cybersecurity. The bill also allows companies to hack back against assailants as a defensive measure, which could undermine current laws like the Computer Fraud and Abuse Act.

"The ideal solution would... [allow] for the quick delivery of indication and warnings data... then correlat[e] that information with existing data

Jasper Graham
Darktrace

Acronym Buster

There are a head-spinning number of acronyms when it comes to info-sharing initiatives and organizations. Here's a quick jargon decoder:

CS&C *Office of Cybersecurity and Communications* – US agency responsible for enhancing the country's cyber infrastructure

NCCIC *National Cybersecurity and Communications Integration Center* – US federal body set up to share information among public and private sectors

ECS *Enhanced Cybersecurity Services* – Department of Homeland Security voluntary information sharing program to assist public and private entities

TAXII *Trusted Automated Exchange of Indicator Information* – A standard whose goal is implementing secure and automated cyber-threat information sharing

STIX *Structured Threat Information Expression* – Project to create a standardized language to represent structured threat information

CybOX *Cyber Observable Expression* – Standard providing a mechanism for capturing, characterizing and communicating threat information

PCNA *The Protecting Cyber Networks Act* – Draft US government bill to encourage more private sector-government sharing

NCCPA *National Cybersecurity and Critical Infrastructure Protection Act* – 2013 bill that brings cybersecurity under the domain of the DHS

ISAC *Information Sharing and Analysis Center* – Vertical-specific forum allowing members to share security information impacting the industry

ISAO *Information Sharing and Analysis Organization* – Hubs for sharing information between private sector and government; outcome of Obama's February 2015 executive order

CiSP *Cybersecurity Information Sharing Partnership* – UK government info-sharing initiative available to all UK registered companies

For Darktrace's Graham, a 14-year veteran of the NSA, governments and private sector need to agree on what data to share, how it can be used, and how it can be shared in a timely manner.

"From a very high level, the ideal solution would be a system that allows for the quick and easy delivery of indication and warnings data that then correlates that information with existing data from other companies to identify commonalities such as overlapping attack infrastructure, vectors, and exploitation methods," he explains.

"This information would allow for the quick rollout and implementation of defenses within industry and government. Additionally, it will help to form a better picture of who is conducting the attack."

There will inevitably be more challenges along the way. But if governments can agree on legally binding rules for information sharing, in consultation with all stakeholders, then perhaps before too long public and private sectors can really start to see the benefits of more openness.

Demystifying Threat Intelligence

'Threat intelligence' could be the answer to defeating dangerous cyber-threats. But what does it really mean? asks **Adam Schoeman**, senior analyst at SensePost

'Threat intelligence' has become a catchall term for a vast array of different technologies, methodologies and ideas. Meanwhile, the use of different prefixes has become little more than a marketing tool. But if we can't classify threat intelligence products by naming conventions, how can we evaluate them? Perhaps some of the industry's biggest research firms can help.

What the Analysts Say

For Forrester, threat intelligence is not a single product or service, but a framework constructed around high-quality information sources and skilled analysts. In Five Steps to Build an Effective Threat Intelligence Capability, Forrester shows that five distinct focuses need to be combined to harness it effectively: laying the foundation; establishing buy-in; staffing the team; establishing sources; deriving intel.

Gartner defines threat intelligence as, "evidence-based knowledge… about an existing or emerging… hazard to assets that can be used to inform decisions regarding the subject's response to that… hazard." At first glance, this could be a definition for a single black-box product, but it's likely that it would actually need to exist inside a framework in order to contextualize the knowledge that originates from third parties.

To understand if a potential adversary has the opportunity, capability or intent to attack an asset, the asset itself needs to be understood. This is difficult to achieve from a black box point of view, where the system has no knowledge of the environment in which it is deployed.

In all these definitions, there is one constant: threat intelligence cannot simply be deployed in a way that adds value as a black box system. Any threat feed that is built to be scaled across many organizations must, by definition, deliver generic insights. Without local contextualization, an information feed can never truly be described as threat intelligence.

Product Proliferation

There is an explosion of threat intelligence products on the market today, but they can all broadly be split into three groups – feed-, research- and platform-driven products.

Feed-driven products convert traditional security logs into an information feed. Generally, the provider gathers information through an array of collection points (often referred to as 'sensors') and transforms that information into a consumable feed.

Research-driven products rely on analysts to distil information into a research report that can be delivered to a specific audience. Although they follow the same steps as feed-driven products, they are built on the premise that human analysts will rigorously interrogate the information that they retrieve, generating value for the target audience.

Platform-driven products do not provide threat intelligence per se, only a way to house and share it. There aren't any definable steps in delivering information, since the platform is always available, and any data stored within it must be added by the end-user.

Applying Threat Intelligence

Threat intelligence products have evolved rapidly, creating offerings that have huge visibility. Yet there is still a significant piece missing: localized knowledge of the target environment.

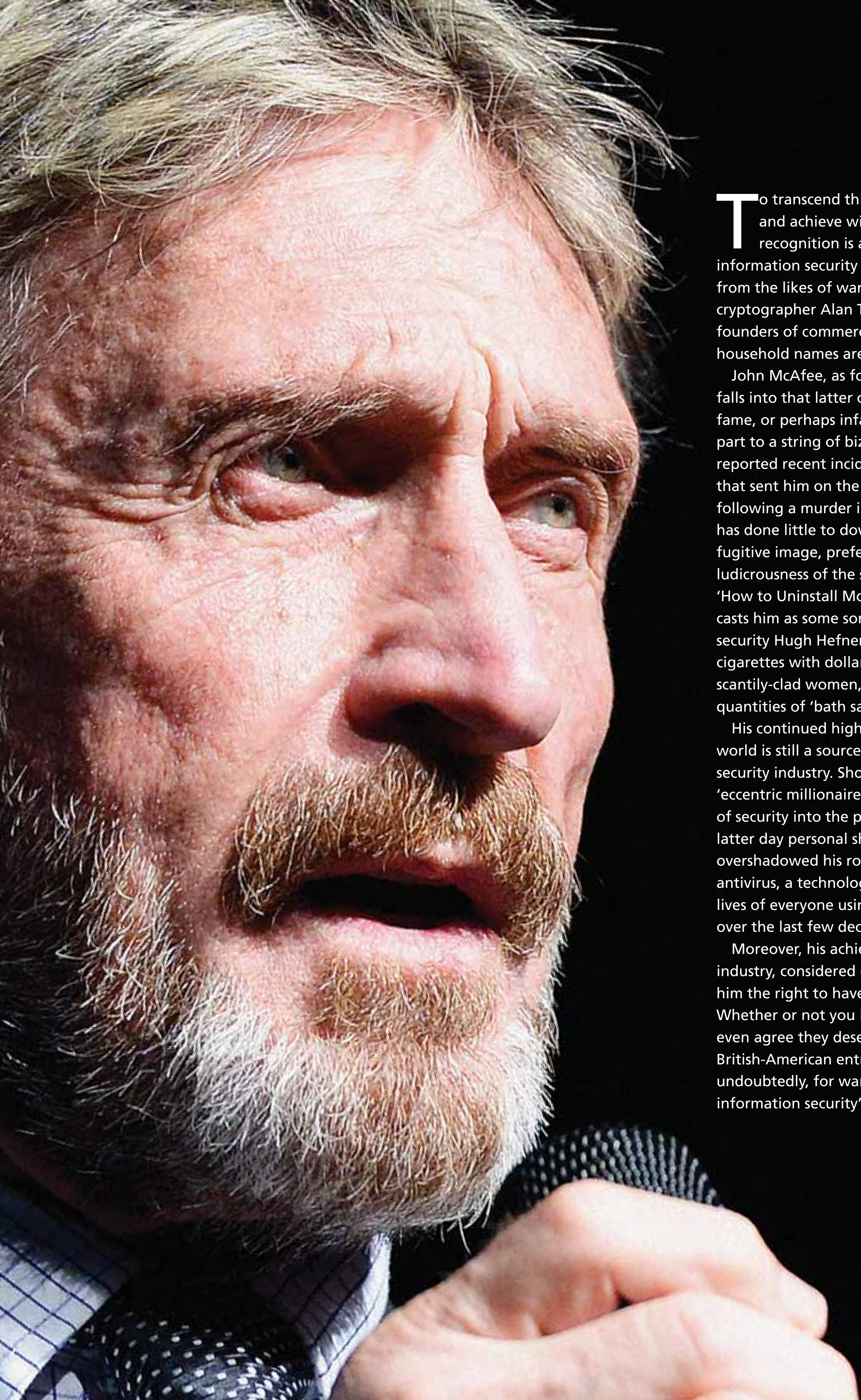
While feed and research-driven products have the potential to add value, such as offering an outsourced information gathering or analyst function, they lack the ability to contextualize knowledge with local information. This dramatically limits their ability to deliver actionable intelligence to organizations.

It could be possible to overcome this limitation on the end-user side through rigorous evaluation of threat intelligence products before purchase, and then using internal analysts to mutate the incoming intelligence to better suit the consumer architecture. However, there would be a significant cost involved.

An alternative would be for a consumer to have direct access to a threat intelligence provider's backend storage and transform functions so that they could pull out intelligence based on their localized knowledge. Unfortunately that's unlikely to be possible when these products deliver generic information to numerous end users rather than harvesting local knowledge about individual environments.

Return of the Mac

» Suited, booted and back on the speaking circuit, John McAfee is a man with a bone to pick. **Mike Hine** lights the fuses at Infosecurity Europe



To transcend this industry's boundaries and achieve wider fame and recognition is a rare feat for information security professionals. Aside from the likes of wartime hero and cryptographer Alan Turing, and a few founders of commercial security enterprises, household names are few and far between.

John McAfee, as founder of McAfee Inc, falls into that latter category – but his wider fame, or perhaps infamy, is attributable in part to a string of bizarre and widely-reported recent incidents in his personal life that sent him on the run in Central America following a murder investigation. McAfee has done little to downplay his bad boy, fugitive image, preferring to revel in the ludicrousness of the situation. His self-made 'How to Uninstall McAfee Antivirus' video casts him as some sort of information security Hugh Hefner, gun-toting, lighting cigarettes with dollar bills, surrounded by scantily-clad women, and snorting copious quantities of 'bath salts'.

His continued high profile in the wider world is still a source of some concern to the security industry. Should this self-proclaimed 'eccentric millionaire' be carrying the torch of security into the public sphere? McAfee's latter day personal shenanigans have overshadowed his role as a pioneer of antivirus, a technology that has touched the lives of everyone using a personal computer over the last few decades.

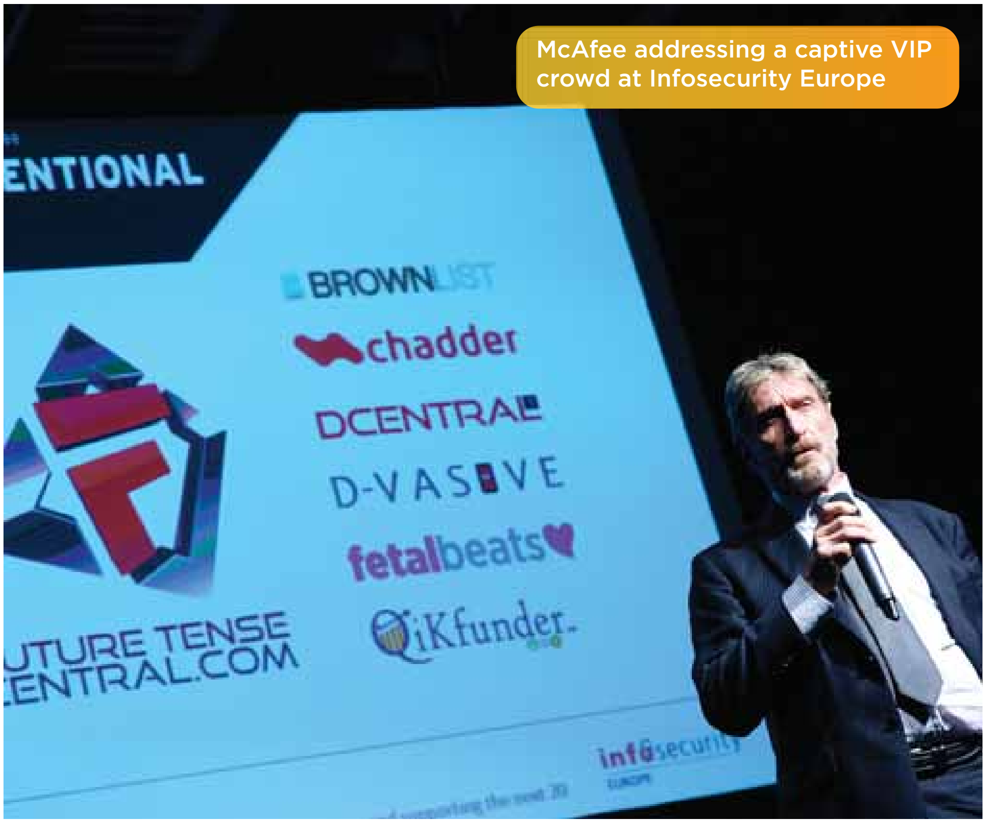
Moreover, his achievements in the industry, considered objectively, have earned him the right to have his opinions heard. Whether or not you like those opinions, or even agree they deserve an audience, the British-American entrepreneur is undoubtedly, for want of a better phrase, information security's rock star.

It's some surprise, therefore, when I meet the man for interview at Infosecurity Europe. He's smartly dressed, softly spoken and unfailingly polite to all who drop by for a chat or selfie. Far from the unhinged individual he is sometimes portrayed as, McAfee comes across as a man who's on top of things. Aged 70, and not looking bad for it, perhaps this dapper appearance signifies a man who has turned a corner. And he's heavily involved in the industry again, leading his latest venture Future Tense Central, launched two years ago, and masterminding a range of new apps designed to put privacy back in the hands of users.

Indeed, a primary occupation of McAfee's thoughts these days is what he regards as relentless corporate and government surveillance – a topic he speaks fiercely but eloquently on as we sit down to chat. In particular, he scorns applications that ask for excessive permissions, especially on smart mobile devices.

"Take, for example, Bible-reading applications – in America they're very popular. At night you can say, 'read to me Genesis Chapter Three'. That's all it does. But every single one of them asks for permissions to read your emails, your text messages, to access your contacts, the camera and the microphone. It's not that they're trying to spy on you to get bad information, they just want to watch what you're doing, what you're buying, so they can use that information to sell you stuff. Given the fact that facility exists, hackers can enter. You are open to malicious use of those applications."

"A person is risking an entire life [by using technology]. We need to address this



McAfee addressing a captive VIP crowd at Infosecurity Europe

The idea of seemingly innocuous applications opening up new threat avenues for data to leak out of is a profoundly troubling thought for security professionals. But, McAfee argues, this is not just a problem for the security world. It's a societal problem, which requires a step-change in what we expect, and demand, of corporations and governments.

"First and foremost we have to take responsibility for our own lives – we can't expect the government to keep us secure," he says. "There is no magic button that you can push, if there is a burglar in your house, and a policeman will materialize. Protection is not something the government offers. We have to take responsibility for our own security before we can change the government."

Such rhetoric, taken out of context, might sound like an extract from the NRA manifesto. (And, indeed, McAfee is seemingly attached to his firearms). But it's emblematic of how seriously McAfee takes individual privacy and security that he sees it in such terms – a matter of life and death, if not for actual individuals, then for a way of life.

"We cannot make privacy extinct; our society cannot function without privacy. Every moment of every day when you meet someone you choose what to reveal. If we do not have that ability society will collapse. If everyone knows everything about every one of us, we will have chaos. We will have constant judgment and therefore constant conflict."

Perhaps a prescient example of McAfee's dystopian visions is the hack of online dating site AdultFriendFinder, which he cites as a particularly horrifying example of the breakdown of privacy. The service suffered a major breach in May, exposing the information of up to four million users. Aside from personally-identifiable information like email addresses, usernames, dates of birth, postcodes and IP addresses, sensitive details such as sexual orientation and predilections for extra-marital affairs were included in the mass of data stolen.

"It's a horrible thing. Can we not see what is happening? A person is risking an entire life [by using technology]. We need to address this. We need to address privacy first and foremost. When we lose [it], when the camera comes into our bedrooms and gets between the moments shared with those we love, then all is lost."

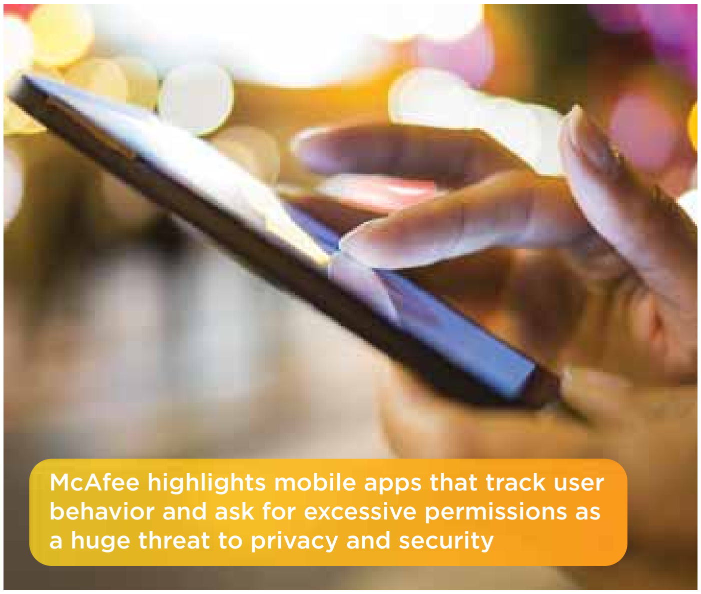
When he says that this is a problem for 'us' to address, McAfee does not mean the security industry alone. In fact, the antivirus pioneer is deeply skeptical of the sector's ability to look at the bigger picture: "I think there's more wrong than right in the security industry – because it's a business like anything and the purpose of business is to make money and survive. If you have a product you want to make an excuse for selling. We can't do that anymore; it's too risky."

He highlights the aforementioned mobile devices as the great looming threat to corporations. Yet even as security vendors worldwide are busily developing solutions, such as containerization, targeted at protecting corporate mobile devices, McAfee suggests all such projects are in vain: "It will not work because people will not conform to the restrictions that are necessary for that."

But stopping mobile devices entering the workplace is not going to work either, he says: "We have become so habituated to their convenience that people would just quit and go somewhere else. I think the world will eventually have two separate issues. You'll come to work and you'll have your pad and your mobile device and you can do what you want, and you'll have no connection between that device and what you do at work. Without that there will be no security either for an individual or for a corporation."

> I think there's more wrong than right in the security industry – because it's a business like anything and the purpose of business is to make money and survive

In the meantime, McAfee is working on solutions that aim to combat the threat of applications and utilities that collect, and therefore threaten to leak, large swathes of user data. Future Tense Central has launched a number of projects that target mobile security. One app, D-vasive, he argues is, "Probably the most secure application for mobile devices, which allows you to lock down your microphone, your camera, your Bluetooth, your Wi-Fi, so that no one can listen to you or watch you."



McAfee highlights mobile apps that track user behavior and ask for excessive permissions as a huge threat to privacy and security

He is also partnering with a company called Starxx, which he describes as offering "the most secure instant messaging platform for the enterprise that has ever existed."

But perhaps the most intriguing of McAfee's new projects is something he calls 'social encryption', for which he is partnering with "one of the founders of Napster and a gentleman who helped architect *Grand Theft Auto*." Social encryption, he explains, "is based on the concept that shared knowledge is something that simply cannot be acquired by anyone. If you and I have a year's worth of shared experience, no one can tap into that and get into the mind of what we have experienced. It's a very sophisticated algorithm that has a layer of abstraction that is, I believe, completely impermeable. It cannot be broken into."

That's one big claim; indeed one that no security advocate would ever make lightly. McAfee agrees.

"I understand how bizarre that sounds. I'm the last person who [would say that]. If you have a switch on a microphone that turns it on, and it disconnects itself from the rest of the hardware, it cannot be tapped into. It is unbreakable. We now have enough sophistication in software to emulate that to extremely high degree.

"Say we want encrypted communication. If I said to you 'Hey remember when Sally got drunk and threw up, in that place we were staying, and her fine?'. Encryption is then developed via communication based on the shared knowledge, and an algorithm is developed. There's no information that was passed between us, other than Sally got drunk and threw up, so the out-of-band communication offers no information to anyone who is trying to snoop. Once the encryption algorithm is run it is virtually unbreakable. It has too many layers of abstraction and the entropy is so infinite that it would be years before we could get supercomputers able to hack into it even after two or three years of processing."

It may sound bizarre and a bit obscure, but McAfee assures us the math is in place and has been verified by the usual authorities. Like everything in the wonderful and frightening world of John McAfee, it's bound to arrive in style and grab attention. He's back.

» MARKET ANNOUNCEMENTS

infosecurity
EUROPE
02 - 04 June 2015 | Olympia | London | UK

Intelligent Security: Protect. Detect. Respond. Recover.

At Infosecurity Europe 2015, keynotes and educational sessions stepped up to the challenge proposed by the event's theme – 'Intelligent Security: Protect. Detect. Respond. Recover' – delivering actionable, cutting-edge security advice. Experts explained the necessity for a holistic approach to security, offering attendees advice on a range of protection and response methods, from intel-sharing and self-evaluation of infrastructure to software controls and network monitoring. Every attendee of Infosecurity Europe came away with new insight on how to protect their systems and respond to attacks.

TOP TEN KEY TAKEAWAYS

1. Understand your business and link information risk back to business objectives and business impact
2. Define the level of risk your organization is comfortable with
3. Demonstrate the return on information security investment by linking to strategic goals
4. Understand which information assets are important to your business to drive an intelligent security strategy
5. Make security relevant to the user by tailoring and refreshing awareness messages to drive behavioral change
6. Implement a robust, fully documented incident response plan, and test and audit it on a regular basis
7. Apply the learning from security incidents to enhance security posture and improve security controls
8. Think like a hacker
9. Collaborate and share intelligence with industry peers to strengthen defence against cyber adversaries
10. Balance prevention, detection, response and recovery according to the risk profile and tolerance for incidents of your organization

WHO ATTENDS?

65%	of 2015 visitors are involved in making vendor decisions
48.4%	of attendees have specific security projects in the next 12 months
40.4%	of visitors represented companies of 1,000+ employees
85.2%	Authorize, specify or influence security decisions
42%	have served for over 10 years in security
32.2%	have served 3-9 years in security
12.9%	were female
87.1%	were male

These statistics refer to the Infosecurity Europe 2015 attendees.

Find out more: www.infosecurityeurope.com

At the Show

GCHQ: UK Firms Must Fight ‘Power, Money and Propaganda’ of Cyber-Attacks

GCHQ’s cybersecurity boss warned at Infosecurity Europe that money, power and propaganda are motivating hugely damaging online attacks against UK organizations. Director general of cybersecurity, Ciaran Martin, argued that while much of the past decade was spent talking about “what might happen,” it’s now a case of “what is happening … on a daily basis.”

The bad news is that GCHQ is seeing organizations of all shapes and sizes being targeted today – by nation states, financially motivated gangs and hacktivists.

“We’ve been genuinely surprised by the extent and variety of UK organizations subject to intrusions,” Martin revealed, adding that a useful way of approaching cybersecurity is to “think about what makes you attractive as a target.”

There are simply too many incidents to worry about “stopping attacks always and everywhere” – so the key is to focus on “what you care about most,” he argued.

GCHQ documents including the *10 Steps to Cyber Security* and the CERT-UK co-authored report on *Common Cyber Attacks* are particularly useful, Martin claimed.

Martin also distanced the agency from the controversy surrounding allegations it has participated in mass surveillance of its citizens, claiming GCHQ uses its legally assigned powers “carefully.”

At the Show

Pen Testers Lack Code-Level Exploit Savvy

The growth of so-called “black box” technologies has led to a worrying lack of awareness among many security professionals about the fundamental computing principles that underpin key disciplines.

So argued Sophos global head of research, James Lyne, during his keynote presentation at Infosecurity Europe 2015.

Lyne, who is also a director of technology strategy at teaching institute SANS and a contributor to the Cyber Security Challenge UK initiative, claimed that these tools have made us all more “tech savvy” than ever before.

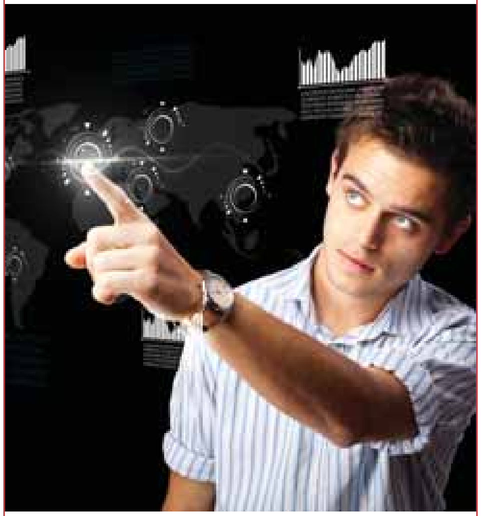
Yet paradoxically, this has “disconnected” and “abstracted” security professionals from the lower level workings and principles of computing.

“This is a missed opportunity for forensics and a missed opportunity to be better pen testers,” he argued.

“It’s important that the industry has skilled individuals … so we can take on the cyber-criminals, who are eternally fantastic at learning and sharing information with each other.”

At the Show

Focus on People Not Tech for Best Threat Intelligence



Effective security controls, network-level visibility and talent are vital underpinnings to good threat intelligence, but IT teams need intellectual rigor rather than whizz bang tools to get the best results, according to a collection of CISOs and industry analysts.

Speaking at Infosecurity Europe 2015, the panel of experts discussed strategies for how actionable intelligence can provide robust cyber defense.

Wendy Nather, research director for 451 Research, and FCC Group CISO Gianluca D’Antonio argued that despite its image as a high tech discipline, good threat intelligence ultimately requires human input to interpret and analyze data in a meaningful way.

“People talk about the technology but analysis needs the human brain to understand the potential impact [of threats],” said D’Antonio.

The idea of “context” is often bandied about by threat intelligence vendors, but frequently to refer merely to adding in “extra details” which on their own might not provide the right kind of insight, explained Nather.

Security Needs to be Seamless

At Infosecurity Europe 2015, deputy editor Mike Hine sat down with Dr Hugh Thompson - professor at Columbia university, chairman at RSA Conference, and chief security strategist at Blue Coat. With all that on his plate it's amazing Dr Thompson found the time to fly over to London at all. But make it he did. Here are some highlights from their conversation:

Tell us a bit about Blue Coat's current work

We're dedicated to being an architecture platform that allows companies to rapidly onboard other technologies. This involves working with other vendors, and building a platform that supports the broadest range of protocols, as well as STIX and TAXII. We want to be integrated into the ecosystem and let people choose best of breed, whatever that may be.

What is the importance of collaboration?

Security companies that win in the marketplace are the ones that listen to their customers. What are the customers asking for? They want all the stuff to work together. We are very customer-focused and because of that we work with other companies that have the same mindset. Working with other vendors that have a common set of customers is a great proposition.

What do customers typically want to know?

In security we really suffer from a lack of metrics around effectiveness and risk. There's a lot of discussion now around threat intelligence. As a concept it's a terrific thing; but how do we automatically take action based on that knowledge? There is some threat intelligence that's very useful to a human being, but for us to advance quickly the far more important ability is automation. That conversation isn't happening as much as it needs to be.

Are security skills lacking?

There is a set of skills that are now becoming very important around incident response, forensics and analytics, people that can solve puzzles. There is a skillset shortage in that for sure. Having been on the other side, teaching at Columbia, there are a lot of people coming through the ranks that are interested, but there's an insufficient supply to the marketplace.

What is the major challenge facing the security industry right now?

We've entered this era where everyone has access to so much free, cool technology, that even if it's mildly annoying to use compared with what corporate IT is offering, the latter is going to be bypassed. We have the challenge of not compromising on security, but innovating in a way that security becomes useful and seamless and transparent. At Blue Coat, we see the ability to make decisions behind the scenes in a way that the user never has to get involved as really important and liberating. A great example is with the last release of the iPhone and the touch sensor. The interesting thing is that it was built up as a big security thing, but it isn't. It's a convenience feature, but it vastly increases security at the same time. That's the next generation, increasing joy of use and security at the same time – that's the next battleground for security.

At the Show

Blue Coat Research Highlights Human Threat Vector

At Infosecurity Europe 2015, Blue Coat revealed results from a study into the online behavior of 1186 UK employees, highlighting how ill-prepared organizations could be for the threat of social engineering. Overall, 54% of respondents would connect with strangers on social media and 56% had no access controls on social media.

Females are more aware; over half set up privacy settings, in contrast with just 36% of males. While 62% of 18-24 year olds take effective precautions checking the identities of strangers before connecting, this group also tends to share more work information on social media. Surprisingly, 18% have never had IT security training.

"On one hand the results are amazing," Dr Hugh Thompson told *Infosecurity* at the event, "But for a security professional that has to deal with failures in the company, probably not so surprising. Despite the fact security is in the news every day, people are still making poor choices with technology."

At the Show

IoT Opens Door for Attackers

Leading provider of network security and DNS services, OpenDNS, warned at Infosecurity Europe that the increased demand for internet of things (IoT) devices in the enterprise is creating new attack vectors.

The IoT market is predicted to grow from $655.8bn in 2014 to $1.7trn in 2020 with a compound annual growth rate (CAGR) of 16.9%. Devices, connectivity, and IT services are expected to make up the majority of the IoT market in 2020, with devices (modules/sensors) alone representing 31.8% of the total.

OpenDNS director of security research Andrew Hay said that IoT devices were moving to the corporate environment just like smartphones and tablets did.

He added that many companies are basically under-prepared for their use. Indeed, OpenDNS research also showed that nearly a quarter of respondents had no mitigating controls in place to prevent someone from connecting unauthorized devices to their company's networks.

In a call to action, Hay advised that it was critical that those charged with protecting networks get out in front of a growing issue. He added that IoT-enabled devices should be regarded and managed like any other equipment connected to the internet and closely monitored to provide warning signs of an attack.

Call for New ICO Powers as Watchdog Misses Thousands of Breaches

Security experts have called for changes to the data protection framework after new research revealed a huge disparity between the number of breaches reported to the Information Commisioner's Office (ICO) and the volume of stolen device incidents handled by police over the past year.

Security and communications firm ViaSat UK submitted freedom of information requests to all UK police forces and found that they dealt with at least 13,000 device theft cases between March 2014 and March 2015.

In comparison, data protection watchdog ICO investigated 1089 breaches over the same period. This could mean thousands of breaches are going unreported, assuming many of the devices stolen had sensitive corporate data on them.

"We must remember that 13,000 thefts is the bare minimum: considering that not all police forces could share this information, the real figure is likely to be many times greater. As a result, thousands of individuals' private data could well be on borrowed time," said Chris McIntosh, CEO of ViaSat UK.

"It's clear that this discrepancy isn't due to the ICO but the framework it has to operate in. As it stands, the ICO simply doesn't have the tools and powers it needs to ensure that either all threats are reported, or that risk is minimized."

At the Show

Rise in UK Cybersecurity Incidents as Average Costs Soar

Almost three-quarters of small UK businesses, and 90% of large organizations, have experienced a security breach, roughly a 10% increase for both compared with the same time last year. This is one of the key findings from the *2015 Information Security Breaches Survey*, commissioned by HM Government, conducted by PwC, and launched at Infosecurity Europe.

Not only are more companies feeling the pain of breaches but the average costs associated with security incidents are also rising sharply.

The survey of 664 IT pros and senior business leaders asked respondents to put a monetary cost on their worst security breach of the year.

For a large organization this price has more than doubled since 2014, now ranging between £1.46m and £3.1m, up from £600k to £1.15m a year ago. The average cost to small businesses, meanwhile, ranges from £75k to £311k, up from £65k to 115k.

Experts from PwC explained that the nature and type of threats that organizations now face have changed. While malicious software was once the highest concern for companies, it is now data leaks and attacks from unauthorized outsiders that should be keeping company execs up at night. Almost 70% of large UK organizations were attacked by unauthorized outsiders last year, up from 55%.

At the Show

Certes Networks Unveils CryptoFlow Solutions at Infosecurity Europe 2015

A rise in mobile devices plus changing working practices means that more data than ever is flowing both within an organization and outside and unencrypted data is fast becoming a major security concern.

Certes Networks therefore took the opportunity to make the EMEA launch of its next generation, borderless security encryption solution at this year's Infosecurity Europe. The CryptoFlow App solution is the industry's first user-aware and application-aware solution for protecting sensitive data traffic and provides safe enterprise apps for all users, regardless of device, network or location.

Protecting data in motion often requires a complex assortment of SSL, IPsec tunnels, application layer controls and multiple network configuration challenges. However, CryptoFlow VPNs use the power of network virtualization to build simple, abstract encrypted flows across the network, which means that encryption can be managed from end-to-end without touching the network or applications.

"Given the escalation in serious breaches over the past couple of years, it is clearly time for new thinking. CryptoFlow App is a big step forward for the industry as it allows enterprises to secure networked applications with a simple policy interface by matching users to applications with the desired security profile, based on both business compliance and data protection needs," said Paul German, VP EMEA, Certes Networks.

Join the ESET Beta Program

Version 9 of ESET's award winning Smart Security and NOD32 is now available in beta form, offering new features including:

- Banking & Payment Protection which automatically detects when users visit a banking or payment site, and ensures that any transactions are processed in a secure environment
- Reputation Evaluator to further help guide the user safely through the Web by blocking cloud-based files and URLs based on reputation and risk level
- Enhanced Botnet Protection with added support to allow the prevention of malicious botnet traffic coming to and from the users' system
- Improved update process, now more flexible and transparent, and with new protection features added automatically as they become available

Version 9 is fully compatible with the forthcoming Windows 10 OS. Find out more and join the beta program at: www.eset.com/int/beta/edition2016/

Radware Launches New Device Fingerprinting Technology

Radware, a global leader of application delivery and application security solutions for virtual, cloud and software defined data centers, recently announced enhanced protection from threats posed by advanced bots through its Attack Mitigation System. This major enhancement gives Radware customers the ability to track end user devices without the need for an internet protocol (IP) address. Fingerprinting technology is used to precisely identify application users or website visitors who have a history of malicious behavior, and are often part of a botnet.

Device fingerprinting implemented in Radware's Attack Mitigation System suite uses dozens of characteristics of the device in a unique way to identify and distinguish it from all others. Using proprietary tracking, Radware can generate device reputational profiles that combine both historical behavioral information aiding in the detection and mitigation of threats such as distributed denial of service (DDoS), intrusions and fraudsters alike.

"We have reached a point where the IP address has limited effectiveness as a means of identifying and blocking illegitimate users. With the proliferation of devices driven by the internet of things (IoT) and users operating multiple mobile devices more than ever before, the challenge of device identification continues to increase exponentially. Our device fingerprinting technology gives online businesses a powerful tool in combating the threats posed by the difficulties of accurate device and user detection," said Ben Desjardins, director of security solutions for Radware.

At the Show

VASCO – Security Meets Convenience

Infosecurity Europe 2015 proved to be a busy show for VASCO, with plenty of interest in its range of mobile and cloud security apps and its transaction security solutions. With today's trend for constant connectivity, and the rise of BYOD, VASCO showcased DIGIPASS for Mobile.

DIGIPASS for Mobile is unique in that it balances the need for stronger mobile security with user demands for convenience, by delivering frictionless two-factor authentication, an e-signing experience and built-in application security. It ensures that any application running on a mobile platform is self-protected in all aspects of application runtime.

DIGIPASS for Mobile hasn't just attracted the attention of visitors to Infosecurity Europe 2015. Caesars Entertainment Corporation, the world's most diversified casino-entertainment provider, recently implemented it to enhance its network security – without compromising the convenience of its corporate users. This follows the recently released 2015 *Verizon Data Breach Investigations Report* which identified that 95% of web app attacks use stolen credentials, such as stolen user-names and passwords. By implementing stronger authentication methods – like DIGIPASS for Mobile – companies can significantly reduce the chances that hackers will succeed with a mobile data breach.

Generated one-time password:

410537

Wick Hill Named Distributor for KnowBe4

Wick Hill recently announced that it has been appointed UK distributor for US-based KnowBe4, providers of the world's most popular integrated security awareness training and simulated phishing program, based on Kevin Mitnick's 30+ year unique first-hand hacking experience. KnowBe4 is seeking to expand its UK presence through two-tiered channel distribution with Wick Hill.

Ian Kilpatrick, chairman of Wick Hill Group, commented: "A key IT security vulnerability is staff, and many organizations are only as secure as their weakest employee. Traditionally, perimeter security addressed this risk, but now that no longer works on its own. With the continual changes in threats, it's been nearly impossible for most organizations to train and support their entire workforce. We see Knowbe4 as meeting that staff training requirement, by enabling organizations to test employees at their desks and by automating the processes for providing reporting and focussed training for those who are vulnerable."

KnowBe4 addresses the issue of employee vulnerability to malicious emails and provides automated, internet-based security awareness training to combat social engineering, phishing and ransomware. The training is cost-effective, continually updated, easy-to-use, requires a relatively short amount of employee time, and is suited to organizations of all sizes.

Netwrix Brings Complete Visibility to a Whole New Level

Netwrix Corporation recently announced the release of Netwrix Auditor VEGA, a major product upgrade to help change the way organizations find and access audit data for investigating security incidents and passing compliance audits. Netwrix Auditor helps prevent security breaches, pass compliance audits with less expenses on time and money, and just keep tabs on what privileged users are doing in the environment and why.

With new key features, Netwrix Auditor enables complete visibility into both security configuration and data access within the entire IT infrastructure – providing actionable audit data about who did what, when and where, and who has access to what.

An interactive search feature helps to make custom requests and quickly find exactly who changed what, when and where and who has access to what in the IT infrastructure. Delegated access allows key stakeholders to access audit data whenever they need it.

The new Netwrix Auditor client can be installed on any computer to provide full access to actionable intelligence. Out-of-the-box compliance reports, mapped to specific regulatory compliance standards, including PCI DSS 3.0, HIPAA, SOX, FISMA/NIST and ISO help pass compliance audits and minimize compliance costs.

AlgoSec Security Management Suite 6.8

The AlgoSec Security Management Suite delivers a complete, integrated solution for managing complex network security policies – from the business application layer to the network infrastructure. With powerful visibility across virtual, cloud and physical environments, the AlgoSec suite automates and simplifies the entire security change management process to accelerate application delivery while ensuring security and compliance.

The new release, AlgoSec Security Management Suite 6.8, enables users to:

- **Automatically Migrate and Provision Business Application Connectivity to the Public Cloud:** AlgoSec provides easy-to-use workflows that navigate the user through the entire migration process. It identifies which application connectivity flows need to be migrated to support business requirements, provides recommendations on how to modify them, and then automates the entire change management and migration process, thereby simplifying extremely complex and risky processes and saving significant time and effort.
- **Provide Comprehensive Security Policy Management for Amazon Web Services:** With this new version, AlgoSec delivers comprehensive security policy management for AWS Security Groups including change management, network visualization and traffic simulations, policy and risk analysis, auditing and compliance reporting. Through this support, companies can now seamlessly extend their security policy to critical business applications deployed on AWS and ensure that their organizations are fully secure and compliant.

At the Show

Libraesva Continues its International Growth Following Infosecurity Europe 2015

Libraesva, a leading developer and provider of advanced email security solutions, attended Infosecurity Europe for the second time this year and reinforced its intention to extend its network of distributors to the EMEA and APAC markets.

At the show, Libraesva presented its email content gateway solution ESVA – Email Security Virtual Appliance. ESVA has been recognized by the prestigious Virus Bulletin as one of the best and effective systems of protection and analysis of email content, and awarded 'Best Antispam solution of the year' at the 2014 UK Computing Security Awards, thanks to its ability to block spam (99.98%) and to the total absence of false positives.

Paolo Frizzi, CEO & Founder of Libraesva, said: "We are extremely satisfied with our second participation at Infosecurity Europe 2015. We had the pleasure of welcoming 50% more visitors at the stand than last year, all showing a real interest in our solutions. The many connections made with visiting companies allows for the creation of relevant synergies across countries and technologies. Libraesva intends to invest in the UK market and the opportunities that arose at Infosecurity Europe confirmed the validity of our strategy. We will move forward with increasing motivation to extend the reach and consolidate the effectiveness of our security solutions, by investing in R&D and dedicated services for each country we are active in."

At the Show

activereach Announces New Launch at Infosecurity Europe 2015

activereach launched its Secure Access to Cloud Apps solution powered by the FireLayers Secure Cloud Gateway at Infosecurity Europe 2015.

The activereach solution enables the responsible adoption of cloud apps, while ensuring security, compliance and governance of any cloud application, on any device and by any user. Until now, CIOs / CISOs are forced to choose between blocking or allowing cloud apps. With Secure Access to Cloud Apps, users can define and enforce adaptive security policies to prevent data breaches of cloud apps such as ADP, Google Apps, NetSuite, Office365, Salesforce, ServiceNow and WorkDay.

In addition to centralized control and deep visibility, the activereach solution protects against malicious attackers, account hijacking, unintentional risky behavior, unauthorized BYOD and thousands of other risks inherent in using cloud apps.

Prevention capabilities include:

- Control Over Any App: vendor agnostic, granular level control of any resource
- User Centric Prevention: real-time prevention via interactive mitigations
- Policy-Based Architecture: define custom policies, roles and alerts
- Open & Extensible: integrates with any API and 3rd party security or monitoring tool
- Full Stack Security: protects from network, device, OS, IP, app, and content to work flows

More information is available at www.activereach.net

At the Show

Centrify Targets 'Password Rage' at Infosecurity Europe 2015

According to a poll taken at Infosecurity Europe this year, a third of password users admit to suffering from 'password rage' with many driven to crying, screaming and swearing.

The poll carried out by Centrify, a leader in unifying identity management, reveals that users are becoming increasingly frustrated with trying to remember different passwords; with a quarter saying they forget their password at least once a day and 5% admitting they forget all the time.

One in six people admits screaming or shouting in the office if they cannot remember their password, and one in seven admits moaning at colleagues. People also admit to running off and slamming the door and even banging their head on the desk.

"We've all heard of road rage and air rage, but now there's a new one – password rage. As if we don't have enough frustrations in our lives, passwords are an added irritant. The real problems arise though when we start to adopt poor password practices because we can't remember them, like using the same ones again and again, or using easy-to-remember ones like 'password'," explained Barry Scott, CTO EMEA at Centrify.

Locklizard Provides Flexible Document Management Security for Mobile Devices

Locklizard has added flexible mobile extensions to its PDF Digital Rights Management (DRM) services.

In the age of the bring your own device (BYOD) it is increasingly important for corporate bodies to retain control over their document distribution. The Mobile Content Management (MCM) approach is fully implemented in all Locklizard installed Viewers. These allow publishers to control which operating systems are allowed to process Locklizard protected PDF files, and the rights of access down to the user / document level as necessary. These are fixed at the device level, and are enablers – permitting users to 'see' documents that they are entitled to use and preventing them from being able to pass on documents in an unprotected form to third parties.

This approach provides a unique application of PDF control because it can be applied, per document, through to any licensed user, not simply corporate internal staff. It is possible to include BYOD users on an individual basis (or corporately) within the sphere of control. This allows the enabling of protected access with granular controls whilst remaining transparent to the BYOD user so it does not cause artificial constraints on their use of devices.

Visit Locklizard at www.locklizard.com for more information.

GoAnywhere Solves Banking File Transfer Problems

Linoma Software recently announced the availability of a case study describing how its customer, FPS GOLD, solved problems that it had been experiencing for many years, by using the GoAnywhere Managed File Transfer solution.

FPS GOLD, a services company for community banks, was plagued by dropped files and cumbersome procedures for setting up new clients. Among other problems, its old system could not handle the thousands of daily file transfers. It required special scripts and staggered processing to function, and the old system's log made it difficult to detect errors.

Since adopting GoAnywhere, FPS GOLD has solved its file transfer problems. GoAnywhere is capable of handling the volume of transfers FPS GOLD needs. Its clustered architecture is so reliable that FPS GOLD hasn't lost a single file since installing it. Set-up time for new customers has been cut to 15 minutes, and being able to view GoAnywhere's job log has proven to be a "valuable time-saving feature," in the words of the customer. In addition, FPS GOLD estimates a savings of $12,000 per year in licensing fees over its old solution.

Read more about FPS GOLD's file-transfer transformation at http://go.linomasoftware.com/fps-gold.

At the Show

Turnkey Consulting Puts Business-Critical SAP Security on the IT Security Agenda

Today's collaborative business environment requires that third parties have access to a SAP enterprise system, whether that is customers checking the item they want is in stock at a local store, or suppliers requiring inventory information to ensure they will meet production deadlines. The security risk this creates is often not recognized, a situation that is exacerbated by the gap that traditionally exists between SAP and IT security. SAP GRC and security specialist, Turnkey Consulting, attended Infosecurity Europe for the first time this year and put business-critical SAP security on the IT security agenda.

Richard Hunt, managing director at Turnkey Consulting, explains: "Infosecurity Europe 2015 provided the opportunity to engage with the wider IT security world, with a view to enabling discussions between SAP security specialists and their IT security counterparts. The long-term goal is to enable better communication to tackle the current barriers to effective risk management. "

Securing the Smart City

The smart city has long been the realm of science fiction. However, as dark fiber, big data and the internet of things start to converge, the reality is not as distant as it seems. But what are the security implications? **Davey Winder** investigates

Some would argue that our cities are already pretty smart. Glasgow has street lighting that brightens automatically as pedestrians or cyclists approach. Bristol is installing machine-to-machine sensors to supply superfast networks with data about energy use, air quality and traffic flow. Songdo in South Korea even has a waste disposal system that does away with garbage trucks and sucks your rubbish out of the kitchen via an underground tunnel network directly to the waste processing center. So what actually defines a smart city?

According to the British Standards Institution (BSI) the answer is “an effective integration of physical, digital and human systems in the built environment to deliver a sustainable, prosperous and inclusive future for its citizens.”

Unfortunately, explains Dr Gordon Fletcher, co-director of the Centre for Digital Business at Salford Business School, there are an awful lot of alternative definitions out there: “A straightforward summary is that [smart cities] all fall onto a continuum, from a light version which interconnects residences individually with various city systems (typically councils), through to a completely integrated system of residents, visitors and the various private and public organizational systems.”

All the Smart Things

What is on the ground now looks less futuristic than we might imagine. But if we were to let that imagination fly, what might we expect in terms of the positives of a truly smart city?

Helen Viner, chief scientist and research director at the Transport Research Laboratory, sees a number of benefits, from reduced congestion to more efficient energy use and enhanced public safety: “As our cities and the travellers within them become smarter, it’s likely that individual vehicle ownership will become less attractive and multi-modal transport options including car or cycle sharing more appealing.

“I expect that we will soon see a situation where people may choose between alternative cycling routes depending upon the live feeds of air quality information pushed to their smartphones or watches. Similarly, we can expect to see vehicle-to-vehicle communication become a critical element for the effective management of traffic around cities.”

> “Imagine implementing Patch Tuesday on the capital’s traffic light systems
>
> Andrew Rogoyski
> CGI and TechUK

Jacqui Taylor, CEO of FlyingBinary and a member of the Smart Cities Interoperability Committee at the BSI, thinks that each smart city needs a set of objectives which reflect the needs of its own culture and population.

“There is a need to move to more sustainable models of living which will create opportunities and make this an ideal environment to solve existing problems within a smart city framework” she says. “The move to a smart city allows the way we live and the services we consume to be reimagined, essentially creating a connected ecosystem enabled by IoT technologies.”

Indeed, technologists such as Andrew Rogoyski, director at CGI and chair of the TechUK Cyber Security Group, see smart cities essentially as containers for billions of smart things. Rogoyski also sees this creating battles for market share, with technology providers trying to establish dominance as platform, service and device providers.

“Initially this will generate a lot of diversity of proprietary platforms, protocols, hardware and software solutions,” he tells *Infosecurity*, “eventually streamlining to widely adopted technologies, platforms and protocols.”

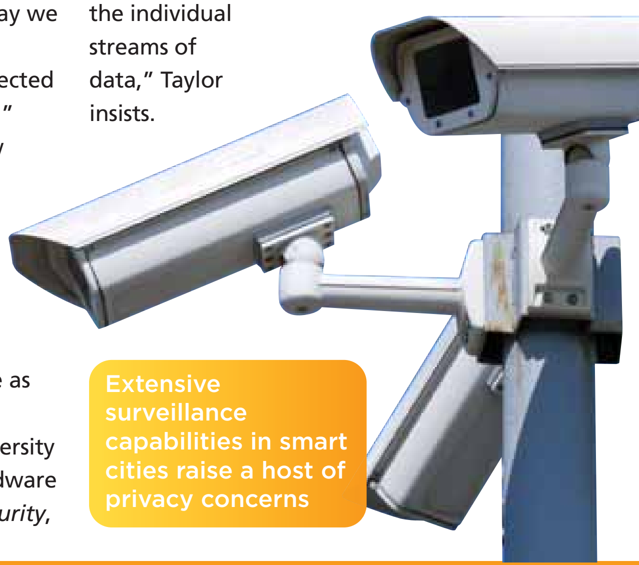
The concern is that smart devices in smart cities will become too small, too numerous and too cheap to have an update strategy. “This means that security vulnerabilities discovered and exploited remain so,” Rogoyski warns. “Imagine implementing Patch Tuesday on the capital’s traffic light systems.”

Building a Smart – and Secure – Future

And so to the smart city negatives, which mainly revolve around security; but is bad security inevitable? Not everyone thinks so. Taylor was part of the team that developed the strategic smart city standards for the UK in 2014 and is currently working as part of BSI to create ISO standards using the UK standards as a base. She sees this as an evolving landscape to be tackled via the collaboration between emerging standards within national boundaries.

“Smart cities are closed systems,” she explains, “they have in-built controls to monitor normal activities and the systems will flag signals in the general noise to determine patterns of change.”

So while each city will need to determine its own strategy for cyber-espionage, the cloud services which curate the data will have controls built in to detect and monitor any activity deemed to be a threat. “It is unlikely that the majority of the sensor technology will need to have additional security around the individual streams of data,” Taylor insists.



Extensive surveillance capabilities in smart cities raise a host of privacy concerns

Fletcher also sees some positives, not least that, in a fully-realized smart city, anomalies within individual systems could be identified early and analyzed and understood precisely in relation to other systems in the smart city. "This could reduce false alarms and enable security analysts to trace a path to the perpetrators" he suggests.

That said, Fletcher also admits that there are already too many examples of poorly secured technology to reassure anyone that all of the components currently in the city are fully secure. What about infrastructure technology obscurity or isolation, would these be enough in terms of IT security from the smart city perspective? Fletcher doesn't think so, seeing them as a trade-off to participation in the smart city.

"In this sense commercially it would be undesirable to take this route towards IT security. It would act as a barrier to the achievement of a genuinely functional smart city" he says. "Both approaches would inevitably necessitate workarounds that would be to the detriment of the smart city's efficiency."

Obfuscation is never a successful long-term strategy at any level for technology and in some ways this approach presents itself as a challenge to hackers. One thing is for sure: as soon as anything becomes connected, a whole new set of security challenges are introduced. Could intelligent traffic management systems be targeted by those seeking to cause accidents by altering the timing of the traffic signals?

Sensors recording traffic flow can reduce congestion in smart cities, and offer a boost to green initiatives

Better Understanding, Better Outcomes

"Currently not enough is known about the security risks to smart cities and a connected infrastructure," Viner admits, "so it's vital that further research is undertaken to identify threats and ways to mitigate risk."

Smart cities bring about a wealth of new opportunities in regards to data analysis and sharing. Rather than being viewed in silos, data in areas such as asset management, safety, air quality, traffic volume and congestion could be analyzed holistically, providing organizations such as road operators, insurers and local councils with a better understanding of movement throughout the city, and impact on the environment.

"At the same time, it could reduce the ability to be anonymous which in turn introduces additional privacy risks," Viner warns. "In such circumstances, we need to have educated and informed debate about the risks and benefits of such approaches."

Although it would seem, at first glance, that any big data and machine-to-machine driven city structure was bound to be bad for citizen privacy, an Orwellian dystopia may not be inevitable. "We cannot expect to move to a connected ecosystem with the same approach to privacy," insists Taylor. "Since the Snowdon revelations there is a general issue from a citizen viewpoint that 'surveillance' will not be accepted."

This is particularly important as we move towards a world where Generation Y has reset the privacy agenda. This generation has two golden rules: if you do something in my name you need to tell me, and don't be creepy.

"Smart cities will need to build their use of data based on trust, particularly where there is use of citizen data," Taylor warns. This allows for new trust and privacy models to be explored and the curation of the city data on behalf of citizens or the city, on either a monetization or direct benefit basis. It's not just the cities that will get smarter; so will our approach to dealing with the security and privacy issues of evolving technology.

NetWars CyberCity

Infosecurity spoke to Ed Skoudis, Fellow at The SANS Institute, regarding a smart city it has built in 1:87 scale miniature. Working on the basis that smart cities are happening now, with most critical systems already controlled by networked computers in a way they were never originally intended to be, SANS built the CyberCity project as a research platform to help better understand the impacts of everything from SQL injection through to buffer overflows and beyond.

"It's a physical city in miniature form (6 by 8 feet in size on top of a table)," Skoudis explains, "but under the table we've included real industrial control equipment that you'd see in life-sized power grids, water treatment facilities, and more."

As well as the research element, this virtual smart city in miniature is also used as a 'cyber range training environment' for military personnel, law enforcement, and utility providers. It's an essential tool in demonstrating to senior leaders and planners the potential impacts of cyber-attacks and cyber-warfare.

Secure the DNS to Secure the Business

Securing DNS is crucial to mitigating APTs. Businesses that don't are neglecting their best defense, says **Chris Marrison**, consulting solutions architect at Infoblox

From banks to healthcare providers, no industry is safe from the effects of malware and advanced persistent threats (APTs). Spreading and mutating while concealed within your IT infrastructure, APTs are long-term attacks, representing a substantial threat to corporate data.

Although malware and APTs will commonly use an organization's domain name system (DNS) as a means of communication, many companies aren't taking the precautions necessary to detect and mitigate these attacks. They're also overlooking their best tool for combatting such threats: the DNS itself.

The Importance of DNS

DNS has evolved over three decades to become arguably the most fundamental part of the internet. Every business needs DNS to function, whether keeping its website online, or for communication via email or VoIP. Given the significant role it plays, it's perhaps little surprise that DNS is an attractive target for cyber-criminals. If it goes down, businesses grind to a halt.

What's more, DNS is relatively easy to exploit. When it was developed 30 years ago, no one would have foreseen its use as an attack vector. Securing DNS is, therefore, of critical importance.

Traditional protection, however, is ineffective, meaning that many businesses are unprepared for DNS-based threats. With firewalls and IPS devices tending to leave port 53 open to allow DNS traffic in, for example, very few incoming queries will be inspected, leaving the door open for APTs and malware.

APTs and DNS

DNS can play a key role in every stage of an APT attack. An attacker will generally use one of three methods for infecting a system, two of which – phishing attacks and watering hole attacks – rely on DNS, highlighting the importance of ensuring its security.

The initial infection primarily exploits zero-day vulnerabilities. The attacker's malicious intent will be carried out by the real APT which, in most cases, will be downloaded by the initially installed malware remotely using DNS.

Once downloaded and installed, the APT will set about disabling antivirus or similar security software on the target computer, a task that is generally worryingly simple. Next the APT will gather preliminary data from its victim and any connected LAN, before using DNS to contact a C&C server for instructions.

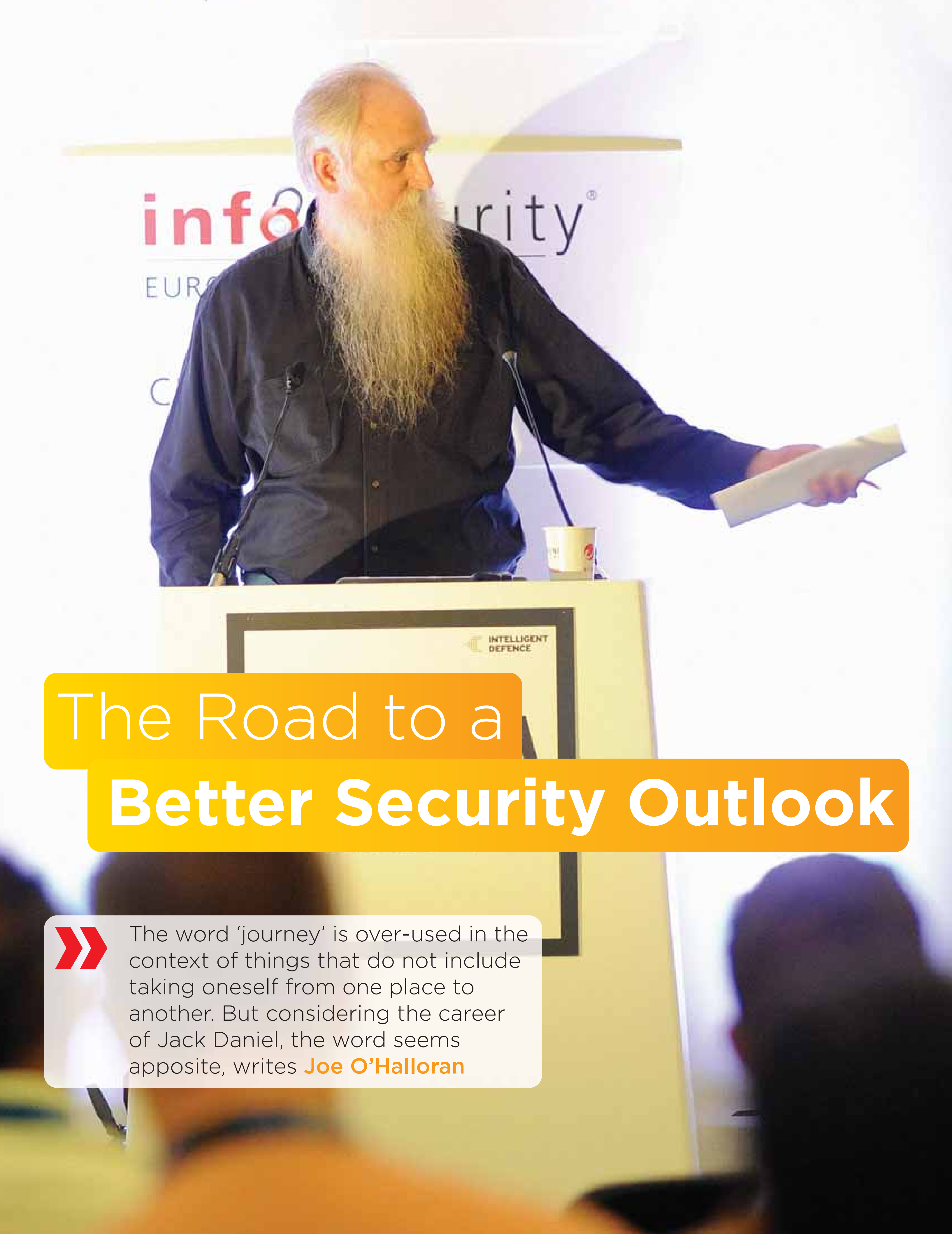
If successful, an APT may identify terabytes of valuable data. This data may simply be exported via the C&C servers, although the bandwidth and storage capacities of some intermediate servers may not be sufficient for transmitting the data in a timely fashion. This increases the likelihood of someone noticing. To avoid this, the APT will often use DNS to directly contact a different server, uploading all of the data at once into a form of dropbox.

Keeping DNS secure

Not only can DNS be easily exploited, but it is often used to enable APT attacks, illustrating the importance of making sure it stays protected – something often overlooked. Deploying a DNS firewall, for example, will enable an organization to use its DNS to block an APT attack at any stage, temporarily or permanently.

Cyber-criminals trust a relatively small number of intermediate servers and networks, which they will tend to re-use, increasing the chances that some, or all, of the server infrastructure used by attackers can be identified and then blocked. This infrastructure-specific insight provides a DNS firewall with the ability to thwart APTs and similar malware in ways that traditional firewalls cannot.

By understanding a threat, a business is already halfway to being secure against attack. Understanding the threat to DNS, however, seems to have passed many businesses by. Until it is taken seriously as an attack vector, an increasing number of APTs will use DNS for malicious purposes.



The Road to a Better Security Outlook

The word 'journey' is over-used in the context of things that do not include taking oneself from one place to another. But considering the career of Jack Daniel, the word seems apposite, writes **Joe O'Halloran**

This journey – from college dropout to car mechanic, co-founder of a worldwide security community, and strategist at a leading security vendor – is a less-travelled one. But it's one taken with great gusto and accomplishment by Jack Daniel. Inducted into the Infosecurity Europe Hall of Fame in June 2015, Daniel now stands alongside luminaries such as Eugene Kaspersky, Phil Zimmerman, Mikko Hypponen, Professor Fred Piper, and Dan Kaminsky.

His journey got into gear, almost literally, when, after dropping out of college, Daniel took on a job in a car dealership as a mechanic: an unorthodox, accidental, but ultimately rather logical first step into security. By starting out as an auto mechanic, Daniel's experience fixing problems with cars set him on a path to diagnosing and solving technological issues that would eventually lead him into computer security.

"I was a mechanic, I was one of the few true Renault experts in the US; it's possible that the masochism of being a Renault expert set me up for a career in security – it certainly set me up to solve problems," he reminisces at Infosecurity Europe before his Hall of Fame induction.

"Like a lot of people I stumbled into security, especially from a network and admin side. [In the dealership] I had systems that I was responsible for running, and bad things happened to them. People attacked some of the systems and I had to fix it. People attacked the systems again and then I had to figure out how to stop them from doing the same thing."

Learning and Unlearning

Proving rather adept at this, his work at the dealership soon led to responsibilities for administering the company's computer systems: "From there it was learning everything I could, because I really liked the challenge of solving the security problem without sacrificing usability."

A career in security consulting followed, before, eight years ago, he moved into the vendor space with German firewall company Astaro, now owned by Sophos. While there, Daniel feels that he learned a lot about the outward-facing side of industry, assisting customers and end-users in trying to secure their environments.

> You have to enjoy learning to continue climbing the security ladder

"There were a lot of things I had to unlearn," he says, comparing his experiences in the new sector with the automotive industry. He cites the latter's poor customer relations as something simply incompatible with the culture of security.

One of the key lessons he most definitely did not unlearn was dealing with finance and the mindset of the security arena: "We can't solve problems without money... [The security mindset] is often about doing the best with resources available. For many, often it is a choice between paying employees and renewing firewall defenses."

The lesson of prioritizing resources is key to anyone seeking to move into a management role within security, he argues. In his experience dealing with more senior officials, he adds: "You can tell the people who have come from the trench position, writing code and doing admin… [there are those] who hang onto the absolutism you have when configuring switches or deploying machines – but if you don't temper that you hit a wall. Those who communicate and compromise tend to move forward and be more effective and satisfied in their job."

The View From The Top Of The Ladder

Daniel can certainly be considered one of the latter. When he looks back at his career, the word 'learn' constantly crops up, and not accidently: "There's a very steep learning curve and you have to enjoy learning to continue to climbing the security ladder."

It's more than fair to say that Daniel is now perched at the top of the ladder, where he is adequately qualified to offer compelling and insightful perspective on all aspects of the market and community. He has had the rare privilege of being a security technology end-user, developer and vendor. Given this, what does he feel is the state of the community right now? The good news, says Daniel, is that the community is in a position of strength – but it has more work to do.

"The community is very strong but I think we could do a better job of being a community across more lines – we have a lot of silos and we don't always break down the walls between military, government, education, etc. We have a very strong community in that the people that are in it are very diverse."

It's only in the past few years, Daniel adds, that people have entered information security as a career: "It's not like automotive engineering or civil architecture or medicine where there are years of doing these things and where you follow a path. Only in the past few years has this path been defined as a collegiate curriculum [for security]."

The vast majority of security pros, Daniel says, come from somewhere else: "I think that gives us diversity. It may be a challenge to maturity, but it certainly gives us perspective. If we work together we can really leverage that broad set of knowledge."

Indeed, another achievement Daniel can be proud of is creating BSides, the community-driven events that act as a forum for sharing knowledge. The idea spawned from the community's complaints about conference papers that had been rejected by Black Hat: "Some of the rejections were valid, but some of the rejected papers were great and simply didn't have a home."

The event was a success, and there was demand for the same model to be replicated across the United States, and eventually worldwide.

Jack Daniel: A Life in Quotes

"In infosecurity, we eat our young."

"We're all over the place as an industry, and the community could definitely be more supportive of new talent."

"The security industry is full of utterly intolerant people."

"We're in a hamster wheel of pain in this industry."

"We're running like mad... sometimes we run in the wrong direction."

"We use temporary bandages and we now have 40 years of bandages built up."

"Share what you learn. Engage in community, and be part of the conversation."

"Success is based on random sequences, mistakes, good luck and the support of friends and family."

Getting The Basics Right

As well as being a font of knowledge, Daniel has been a repository of great quotes from his years in the industry (see above). One classic from a few years ago said the industry tends to forget about its fundamentals and is too focused on creating problems and then building security. How true would this statement be today, and how could it be affecting the industry?

"We get excited about what's newsworthy and we forget the fundamentals," Daniel muses. "It's easy to get excited about Heartbleed, Shellshock, or whatever the latest thing is. But whatever it is, it isn't important if we haven't addressed [what will happen] to all the systems or environments, or if we haven't done risk or an inventory of systems and assessed what really impacts our ability to do the mission of our organization.

"Then [you can] worry about whatever makes the news next week. Rather than worry about the latest news, there are things we should be doing better. Are all the archives protected? Can I back-up and restore reliably, so that every time an event comes up we have a plan to respond?"

Security events will increasingly arise from the growing vectors of point-of-sale and the internet of things (IoT). We need to get used to this, Daniel warns.

"IoT just means that a lot more devices are going to be connected to the network, and that means if there are weakness in those systems they are going to exploited. One specific example is DDoS. We have seen more and more of this. I have seen a lot of reflection attacks using DNS and NTP and those attacks were against systems that were poorly configured on systems run generally by systems administrators.

"One of the [new] attacks is from using a UPnP probe called SSDP – which is in a lot of consumer devices and not managed by professionals. We could fix DNS and NTP but nobody is going to fix SSDP. That sort of protocol is in a lot of these simple devices so that they can communicate and I fear that those are going to be leveraged for this sort of reflection attack."

Setting Out On A New Road – Or Two

But what of the next part of Daniel's journey? Where will the security road lead him? Intriguingly he believes than he will be travelling in two directions at once. He explains: "As my role evolves at Tenable and I spend more time speaking to executives and senior management, it's really helping me grasp even more the challenges of enterprise. Yet coming from small to mid-sized businesses, those guys need a lot of help because they don't have resources."

One thing that has become clear to Daniel over the last several years of working in enterprises is that the challenges we face scale much more effectively than the solutions: "If it's a problem for the coffee shop down the street, the Fortune 500 company is probably struggling with the same problem. It's interesting to be in a role where I can share what I know which hopefully drives security forward.

"In the opposite direction, I started about a year ago looking into the history of information security and assurance, and then sharing that information with a younger generation, because no matter when you come into this industry, just trying to keep up keeps us at a dead run. The idea of looking back really isn't an option for most of us. I have the luxury of stopping and looking back and summarizing that and sharing that knowledge with the younger generations so they know how we got to where we are now."

In studying the journey that Daniel has taken, they are in for some ride.

SAVE THE DATE

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

infosecurity® EUROPE

07-09 JUNE 2016 | OLYMPIA | LONDON | UK

Intelligent Security: Protect. Detect. Respond. Recover.

Collect **CPE/CPD** credits

Why should you attend? See what you missed in 2015:

15,614 international information security professionals attended Olympia, London over three days.

The official event hashtag #infosec15, trended on Twitter.

65% of Infosecurity Europe's 2015 visitors are involved in making vendor decisions.

77 new exhibitor companies (vendors and service suppliers) featured in 2015.

3,761 attendees engaged and networked using the new Infosecurity Europe mobile app.

316 companies from 18 different countries exhibited in 2015; almost a quarter (24.4%) were new exhibitors.

The international speaker line-up of over 260 industry experts included representatives from the UK, USA, Spain, Portugal, Ireland, Germany, Switzerland, Netherlands, Canada, Sweden, Norway, France, Finland, Turkey, Israel, Austria, Romania and Italy.

REGISTER YOUR INTEREST NOW
www.infosecurityeurope.com

Part of infosecurity™ GROUP Organised by Reed Exhibitions®

Health, Safety and Security

Forget the bond of doctor-patient confidentiality, cyber-attacks pose a much bigger threat to your sensitive medical data, finds **Wendy M. Grossman** as she assesses the recent spate of healthcare breaches

In 2014, the UK government announced a plan to improve medical research using patient data generated by NHS England's 55 million registered users. The program, 'care.data', was a PR fiasco. There was near universal support for the stated goal, but near universal condemnation for the finer details, which included selling personal data to commercial companies. The program is being rethought, but the lesson is clear: healthcare data is precious.

Consequently, you might expect maximally secure data practices around healthcare data. Yet reports of data breaches in healthcare organizations are frequent and growing. The statistics from the Ponemon Institute's 2014 *Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data* indicate inadequate safeguards: 91% of healthcare organizations have had at least one data breach in the last two years, and 40% have had more than five. The average cost of a data breach to a healthcare organization is more than $2.1m, which aggregates to $6bn for the industry per year across the US.

"Health data is the most valuable data about you, bar none," says Deborah Peel, the founder of DC-based advocacy group Patient Privacy Rights. "Finance went through this cycle 10 years ago. Healthcare doesn't bother to learn."

Warnings: 0
Messages: 2
Run time: 01:20:49.87
RESET COUNTERS
Watch list
Charts
News
Alerts
Laptop Pro

Cultural Differences

The way healthcare is paid for has a profound impact. The US's myriad tiers of practitioners, healthcare organizations, and business associates such as insurers spawn numerous databases hidden from consumers. By contrast, the UK's state-provided universal healthcare creates many fewer. And these don't need financial or employment information, and are subject to data protection law. The minority of the UK population that buys supplemental private health insurance still relies on the national system for primary and catastrophic care.

This structural difference impacts how much data is held and where. NHS England has huge data assets via the Health and Social Care Information Centre (HSCIC), which is charged with managing them. A US patient's data is generated, copied, and shared in myriad ways patients can't even guess at.

The NHS's data estate offers a huge opportunity to aid research and improve healthcare. The care.data program may have alienated the public, but it sparked a debate highlighting medical information's sensitivity, even without the associated financial and other risks. Healthcare data breaches accounted for nearly 20% of fines given out by Britain's information commissioner in 2014.

Sarah Lawson notes one fear in the UK that doesn't apply in the US: the lack of privacy rules. Lawson's unit is required to ensure that all its data is kept strictly within the EU. "There's an inherent fear that the NSA will be staring at everything."

A case in point: in May 2015, the insurer Columbia Casualty Company filed suit to demand that Cottage Healthcare System repay $4.1m after a breach involving 32,500 customer records, claiming that Cottage had failed at basic information security, including up-to-date patching and regular audits.

Breaches are growing in number and size. In February, a data breach at medical insurer Anthem exposed 78 million records, including names, addresses, medical IDs, birth dates, employment information, and income data. In March, Premera Blue Cross announced a breach had exposed 11 million records. Both of these breaches were due to cyber-attacks, which Ponemon found became the number one cause of such breaches in 2014, surpassing lost unencrypted laptops or USB sticks.

Recently, eight people were indicted after a clerk sold information taken from 12,000 patient records from Montefiore Hospital, which was used to buy luxury goods at retail stores.

Security Failures

Privacy consultant Bob Gellman explains: "The healthcare industry is woefully underinvested in IT, which is why the Obama administration has been pushing electronic medical records." Even with that, problems remain. These include: insurance fraud enabled by copying and pasting between medical records; lack of interoperability to aid customer lock-in; and the prevailing view of security as a bottom-line cost.

> The healthcare industry is woefully underinvested in IT
>
> Bob Gellman
> Privacy Consultant

Peel argues that fundamentally risks are attributable to system weaknesses and the large number of people who can access data. A complicating factor is opacity to patients, who typically don't discover their medical identity has been stolen for two to three years. In the US, at least, such records can't be repaired the way credit records can. By law, nothing can be deleted.

A particular problem in the US, Peel says, is the entanglement of motives and data type; healthcare companies use medical data "not for curing but for figuring out new ways to charge us for things," while stolen medical records can enable large-scale insurance fraud as well as individual attacks.

Not included in Ponemon's cost-of-breach figures quoted above is the price to consumers, though it estimates that the average cost of recovery to each individual is $13,500. Unlike banks, healthcare organizations do not offer protective services, so if a medical record is copied and dispersed, nothing can restore the victim's medical privacy. But that's only one piece of the problem.

Indeed, Pam Dixon, founder of the World Privacy Forum, notes that healthcare breaches are a driver of sophisticated phishing and other attacks. She also sees a trend of attackers digging deeply into systems, lurking and exploring over time. This yields sensitive dataset combinations which can include clinical, bank account, email, and other financial data.

"This kind of data is extraordinarily helpful in creating synthetic identities or in conducting total ID theft, where new bank accounts are opened, new IDs created, and so forth," she says. "It is a very difficult attack to recover from, and these kinds of identity takeovers can be used by criminals to commit crimes."

Law and Compliance

In EU countries, medical data is covered by data protection laws; in the US the relevant law is the Health Insurance Portability and Accountability Act. HIPAA, says Dixon, can be both distracting and unhelpful: distracting because organizations focus on compliance rather than security, unhelpful because it has gaps.

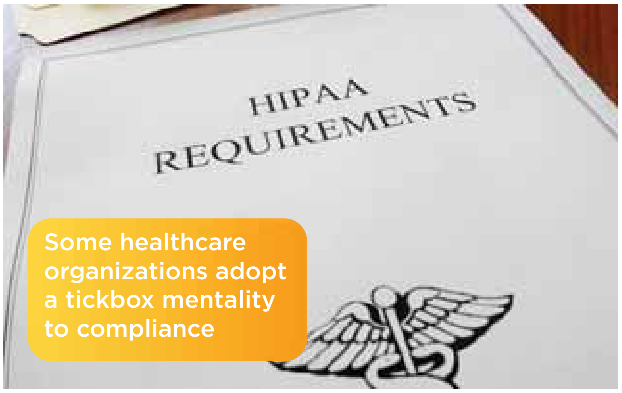
"HIPAA does not specifically require the encryption of a back-end database," she argues. So it's possible that a breach like Anthem's could expose 78 million records without ever violating HIPAA.

Gelman asserts that HIPAA is deliberately written to give some discretion because of the varying nature of healthcare organizations: "You can't impose the same requirements on the Mayo Clinic as you do on a solo practitioner." Some of the rules are requirements; others are merely 'addressable', like encryption, and he argues that in 1996, when HIPAA was drafted, this may have made sense. Even now, he says, "Doing encryption is hard, and it is doubly hard in a healthcare system with millions of user accesses per day. Still, there is no excuse for not encrypting laptops and the like. BYOD makes this all harder."

Dixon has another complaint: the act is widely misinterpreted in ways that add risks for consumers. "One of the most dangerous trends in the last few years has been healthcare providers requiring scans of government identification to prevent identity theft." The goal, of course, is to ensure that patients are who they say they are so no one gains access to medical care they're not entitled to.

But HIPAA has no requirement for identification, Dixon explains, and "the scanning and saving of government ID with a clinical file increases the problems of medical ID theft and increases risk of damage in a data breach. The same goes for palm scans, iris scans, and so on. The healthcare sector does not have adequate security protocols to store this data securely."

Criminals who successfully breach these systems gain much better templates for fake IDs – a vastly increased security risk for patients. Security personnel, she says, should conduct a risk analysis.



Some healthcare organizations adopt a tickbox mentality to compliance

Data Flow

Looking at calls to action, Dixon advocates that healthcare organizations should adopt tiered access practices that ensure clinical data is kept separate from identity and financial information. Peel believes a deeper change is needed: putting patients in control of their own data. "Data shouldn't flow without you knowing," she says. "That alone would limit data breaches."

Phil Booth, the founder of medConfidential, which campaigns for medical privacy, says that it's clear from the breach stories that not enough care is being taken: "Every medical establishment should have someone who is responsible for information governance of the medical records." Booth, like most people, favors the idea of sharing medical data to aid research and improve healthcare, but says that, "because the definition of direct care has become badly blurred, people are becoming risk-averse to sharing when they should, but carp at looking after data when they shouldn't be doing certain things."

Similar problems confront Sarah Lawson, head of IT and information security for the National Perinatal Epidemiology Unit attached to Oxford University. NPEU doesn't typically have patients, just their data. Because of the fallout from care.data, everyone who takes data from the Health and Social Care Information Centre (HSCIC, see box, page 42) is being required to sign a new, overarching contract. Unfortunately, she says, the contract is "basically very ill-thought-out," and although it's stopped the flow until everyone signs, it is "not helping confidentiality."

NPEU's data arrives in several different ways: in addition to the government flow there is data originating from direct contracts with consenting patients. The information provided is often very full and follow-up may continue for decades. A separate government department provides the Information Governance Toolkit, which she describes as "not as strong as HIPAA" but a "relatively sensible piece of process information we use to ensure we're doing the right thing." In the present situation, Lawson may find data blocked that pertains to patients that have given their express consent to its use at NPEU.

> This kind of data is extraordinarily helpful in creating synthetic identities or in conducting total ID theft
>
> Pam Dixon
> World Privacy Forum

Internally, the unit's lack of interaction with actual patients makes it easy for the data to become abstract, Lawson suggests. "Those dealing with the data start to disconnect from that person at the end. People just stop thinking, because they're busy with research and have all this information and no name, and they forget that in one lump, if it's lost, it would beautifully identify everyone walking around them."

There is a final issue that will have an undeniable but imponderable impact: the trend toward health monitoring devices, including those that will become part of the internet of things. Today's Fitbits and wearable glucose meters will soon be joined by cameras, microphones, and sensors. All these devices collect health data, but it's stored by organizations that are not considered healthcare providers and are not subject to HIPAA (though the EU's data protection rules would likely apply). Today's problems are only likely to escalate.

Are Companies Spending Too Much on Security Detection Solutions?

...Point...

Put Your Wallets Away – Detection Tools Alone Won't Stop Data Breaches

Barely a day goes by without news of another organization falling foul of hackers. There is no predicting who might be hit next; every organization big or small, in every industry, is at risk.

Consequently, companies are spending vast amounts of money on security tools, from firewalls and antivirus to IDS and access control management. So, with multiple advanced solutions in place, why are organizations still finding themselves at the mercy of cyber-criminals? The answer is that these tools simply aren't enough to safeguard systems anymore. There is absolutely still a place for these tools, but organizations are placing too much focus and budget on them.

Detection systems generally fall under the category of prevention tools, which aim to detect and stop threats before they can get into your systems. However, today's sophisticated criminals can easily circumnavigate these tools, as we often see with advanced persistent threats. Traditional security tools, even those deployed in a defense-in-depth model, will never offer you the full protection required to stop an APT. They will rarely catch custom, zero-day malware.

Attackers frequently combine malware with well-planned physical theft and clever social engineering to harness a full spectrum of logical, physical and social attack vectors. What's more, even if your detection tools manage to identify such a compromise, it's difficult to immediately determine if the compromise was due to an advanced threat based on a single event or a simple behavior sequence. To top the challenge off, buying individual tools and trying to knit them together can lead to network vulnerabilities where systems are not 100% compatible. Each will provide a continuous stream of data related to their own individual threat events.

With so much information, your security teams could be blinded to those threats that actually matter and if they can't even pinpoint what needs investigating and what does not, they have little hope of responding in a timely way.

> Tools simply aren't enough to safeguard systems anymore

A shift in mindset is therefore required. Rather than relying on preventative tools, you need to look to advanced security intelligence systems, which essentially enable your firm to detect and respond to threats and breaches more effectively. By combining continuous monitoring for anomalies with security intelligence – which collects forensic data, as well as user and machine analytics in order to provide context – your security teams will be in a far better position to identify immediately what poses a real risk and what doesn't, and respond efficiently.

Without the ability to correlate information from a range of sources, views of network activity tend to be disparate and fail to provide a complete picture of the network. Security intelligence ensures any anomalous activity is identified in real-time, and allows your organization to automatically correlate seemingly unrelated incidents with potential danger being flagged as it occurs. In addition, the forensic element enables you to analyze security events, aiding learning and potentially providing evidence for possible prosecutions.

While security intelligence isn't derived from a single technology, but rather a tightly integrated group of technologies, an ecosystem of compatible tools enables a more coordinated and efficient approach to detection and response. If cyber-criminals want to get into a network they will, so you need to stop trying to stop them, and instead focus on preventing them from getting what they are looking for. Clearly, if detection solutions worked, we wouldn't be seeing as many breaches as we do – suggesting your money could, and should, be better spent elsewhere.

AUTHOR PROFILE

Ross Brewer is vice president and managing director for international markets at LogRhythm. He is a circuit speaker at industry events and a recognized industry commentator, regularly quoted in the press.

......Counterpoint...

Companies Can't Afford to Reduce Detection Software Spend

The idea that you may be spending too much on detection software is at odds with today's cybersecurity landscape. The simple truth is that the proliferation of devices, apps and vulnerabilities is necessitating continued smart investments in security solutions to stay ahead of today's threats and this is being supported by IT reported spend forecasts.

The bad guys are usually well ahead of the pack. Cybersecurity has become a board-level topic and security pros worldwide are desperate to improve their industry knowledge, discover new ways to keep threats at bay, and be better equipped to keep their companies safe.

It's not a problem that's likely to go away anytime soon. As we bring more devices onto the network, the average enterprise IT infrastructure is growing at a remarkable rate in terms of size and complexity. As such, there's an even greater demand for investment in technologies that can effectively detect anomalous or dangerous activity and secure endpoints from malware, including viruses, trojans, rootkits, spyware and adware.

The case is often made that data breaches are inevitable and companies should be shifting their focus from detection and prevention technologies and diverting more attention to response. Although there is considerable value in being prepared to execute a decisive response plan, you would be ill-advised to do anything at all that is going to increase the likelihood of having to implement response plans in the first place.

The risk of cyber-attack has increased dramatically, but there's a balance between accepting risk and being negligent. I wonder how much Sony's senior vice president of information security, Jason Spaltro, regrets telling CIO magazine in 2007, "I will not invest $10m to avoid a possible $1m loss." Hindsight is 20/20, but companies that neglect to spend adequately on security today, could well regret their actions in future.

Even companies that specialize in response technologies recognize that perimeter security and detection solutions play an important role, and that's exactly the point. Every security solution should play its role as part of an effective overall defense strategy – no single aspect is the be-all and end-all. Venerable technologies such as antivirus are increasingly taken for granted, but mature technologies can still play an incredibly important role in securing your business.

> "There's a balance between accepting risk and being negligent

They are the goalkeeper of the security industry: Often the least glamorous part of the team; almost always underappreciated, but of vital importance to defending against attack.

It is important to remember that, for the most part, hacking remains a numbers game. At the start of 2015, AV-Test Institute was registering over 390,000 new malicious programs every day, which puts into perspective the volume of threats. The good news is that the vast majority of these cyber-attacks are automated and can be detected and blocked at the perimeter by keeping software up to date, patching employee devices and implementing the right detection software. It's important to consider that cutting investment in these technologies will ultimately increase the attackers' chances of success.

A major challenge for modern enterprises is actually identifying the growing number of endpoint devices that are on the corporate network in the first place – and subsequently managing them. Investing in any solutions that will help give you insight, and automatically detect and prevent threats from executing, can only ever mitigate the overall operational risks posed by cybercrime.

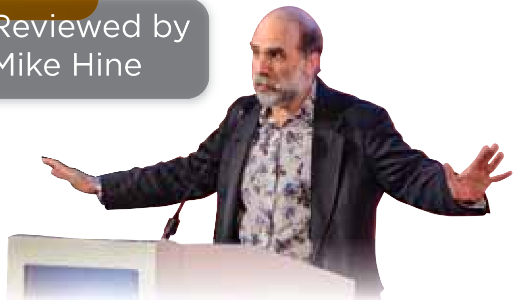
AUTHOR PROFILE

Jonathan Temple is president and CEO of HEAT Software, bringing over 25 years' experience in the software industry. He has held executive leadership positions with Hyperion and Business Objects.

Book Review: Data and Goliath, Bruce Schneier

Title:	*Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*
Author:	Bruce Schneier
Pages:	383
Publisher:	WW Norton & Company
Price:	$27.95/ £18

Reviewed by Mike Hine

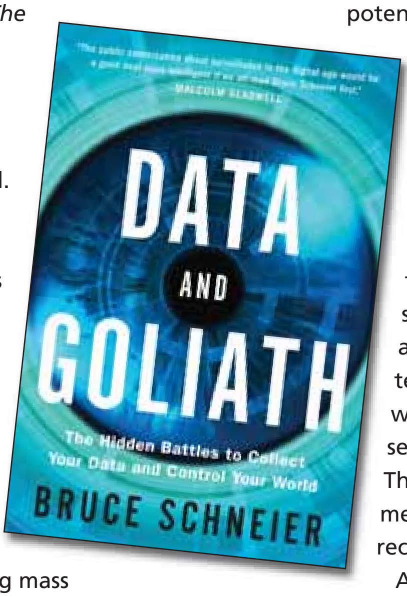


The full magnitude of the Snowden revelations' significance will not be totally comprehensible for many years, when we can look back at the technological, political and philosophical reconfigurations of society that followed the disclosures.

A prescient look at what direction societies could – or should – take post-Snowden is offered by Bruce Schneier, security industry veteran, in his latest book, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*.

Schneier sets out to assess the state of surveillance culture at corporate and government level. After an exhaustive analysis of the creepy ways data is used and abused, the author explains the myriad effects of this. In the final section, he gives a range of potential solutions for governments, corporations and individuals to recalibrate our surveillance culture, before privacy and liberty suffer a mortal blow.

It's not the only book assessing mass surveillance and the formerly clandestine activities of the NSA and its counterparts, but its success is striking a balance between detailed analysis and accessibility to the general reader. This is not just a book for security and privacy experts.


MALCOLM GLADWELL
DATA
AND
GOLIATH
The Hidden Battles to Collect Your Data and Control Your World
BRUCE SCHNEIER

Underlying Schneier's treaty in *Data and Goliath* is the assertion that the large-scale aggregation of data is not harmful all the time. "We all reap enormous benefits from data collection and use," Schneier argues, listing medical uses, real-time traffic data, and virtual communication as beneficial examples.

The crux, Schneier writes, is figuring out how to maximize the good uses of mass data collection while minimizing the potential damage of such practices. That balance, he says, is way out of kilter right now, with governments wielding massive technological power to commit mass surveillance, break anonymity technologies, and weaken the inherent security of the internet. The individual, meanwhile, has little recourse in law.

At corporate level, the balance is also weighted too heavily against consumers, with obscure privacy policies, insecure default settings within applications, and a tendency to overshare with government. "Given current laws, trust is our only option," Schneier writes. The people, he believes, have a right, but also a duty, to demand more transparency and accountability from data brokers.

Perhaps the most significant of Schneier's conclusions is that the data problem cannot be solved domestically, nation by nation.

"Laws might determine what methods of surveillance are legal, but technologies determine which are possible," he writes. Essentially, we can demand of Western governments that they restrict their use of surveillance technologies, but that doesn't stop the technology being implemented by other groups, government or civilian, around the world. And when our data moves constantly throughout a borderless internet, this matters.

The ideal solution, Schneier argues, would reverse the trend of internet Balkanization and open up the floor for an international reevaluation of laws around data collection and processing. It's a bold, long-term vision, but in laying out the arguments so clinically, Schneier's latest book serves as a good starting point.

Though occasionally repetitious, *Data and Goliath* details our precarious position at the dawn of the digital age with striking clarity, accessibility and balance. If only those traits could be applied to the corporations and governments that hoard data, maybe this book wouldn't have to make it into second edition. One suspects that there are many more chapters to come, though.

Slack Space

Facebook Connection Threatens 'Slicing'

Ever consider selling those old Beanie Babies, gaming consoles, CDs, bikes, gardening tools? Beware, because sometimes you may get more than you (literally) bargained for.

Such was the case recently in Wrexham, North Wales, when a man attempted to sell his old PlayStation 2 gaming console. He was using Facebook to do so, thinking that he was being more safety-conscious than if arranging something via, say, Craigslist, because ostensibly the buyer was his 'friend'. But in reality, his 'friend' turned out to be someone who had hijacked a Facebook profile. When he showed up to make the trade, he found a youth with a knife who threatened to "slice" him, then made off with the console.

The seller agreed to meet up at 11pm outside local shops, which wasn't perhaps the wisest time to do it. Police tracked down the youth responsible by tracing his cell phone geographic data. But the lesson is simple: be careful who you choose to meet IRL.

"That moment where we take a relationship, be it a friendship, a romantic liaison or a simple commercial connection, and try to move it from the online world into the real one, can be fraught with inherent dangers," explained researchers at Sophos. "Online, you never really know who the person at the other end of a chat window is and what their agenda might be. Scammers, fraudsters and worse flock to dating and trading sites looking for fresh victims to target."

Meet Chris Gatling, the NBA All-Star Scammer

File under face-palm: Former NBA All-Star Chris Gatling was recently arrested in Scottsdale, AZ, for forgery and theft. And not for the first time.

Gatling was picked up after authorities pinned him as the ringleader in a credit card and identity theft scam in which he amassed a $900,000 'get' in a multi-tiered effort. Apparently, Nike's mantra of Just Do It applies in all kinds of situations.

First, Gatling targeted a business-owner he met on an online dating site, the proprietor of a fitness studio. He then procured a series of stolen credit-card numbers, and asked her to run them for various amounts. After they provisionally went through, she then gave him 90% of the charges in cash, and kept 10% herself. He shoots, he scores!

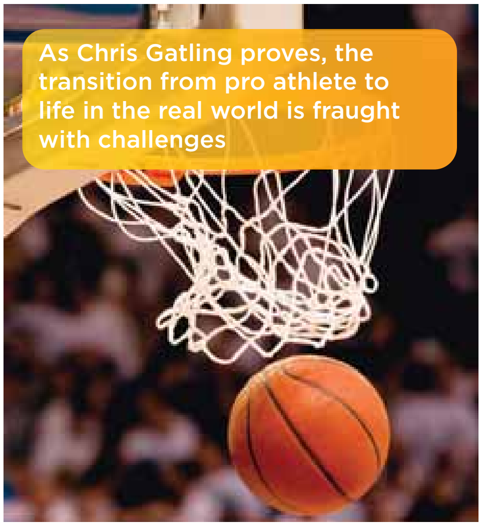
But when those transactions were reported as fraudulent, it left her in the hole to the tune of $90,000 – enough to force her to close up shop.

Is she an accomplice or a victim? We may never know. Authorities seemed content with collaring the basketball star, and charged him with fraud, aggravated identity theft and forgery.

The arrest followed a 2013 conviction on other charges of forgery and theft, after he found an empty house whose owners had left the electricity turned on. In addition to hoopin' it up rent-free for a while, he also tried to rent it out on Craigslist.

Hello Barbie, Let's Go Party… Or Not

Apple has Siri, Microsoft has Cortana, Domino's Pizza has Dom, and Barbie will soon have... a connected version of herself. Mattel recently unveiled Hello Barbie, which has an embedded speech-recognition platform developed by ToyTalk. She can tell jokes, stories and play interactive games, and makes use of cloud-based machine learning so that, over time, she learns and remembers what its child likes to discuss and find out about. Those conversations and digital footprints are kept on a server in the cloud.



As Chris Gatling proves, the transition from pro athlete to life in the real world is fraught with challenges

And some parents just find that creepy. So, Hello Barbie has found herself the object of a petition with thousands of signatures from concerned parents.

She requires a Wi-Fi connection, and is connected to the internet and ToyTalk's secure server via a smartphone app. And in theory, there's an opportunity for a man-in-the-middle attack using a fake app or rogue Wi-Fi connection. But parents are most concerned about privacy, as in, what happens to the recordings of their kids talking to Barbie? They also worry the toy can be used to spy on their kids, or hacked and made to say inappropriate things.

ToyTalk hit back, stating that all internet-connected toys and services fall under the Children's Online Privacy Protection Act, which requires parental consent before any data, including voice data, is collected from products used by under-13s. Hello Barbie must be synced with an iOS or Android app, and parents must read and accept a consent form detailing data collection and use.

Parents also get a weekly email with links to their child's audio sessions, which they can listen to and delete from the company's servers at any time.

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

Mobile payment technology has taken great strides forward in 2015. Earlier this year, at Mobile World Congress, Samsung announced its Samsung Pay service, to be integrated into the new, NFC-toting Galaxy S6 range. Google followed suit, announcing that Android Pay will effectively replace its Wallet system in the next generation of Android phones.

Apple, meanwhile, is ahead of the pack. Its Apple Pay service launched late last year in the US, and in July 2015 will be activated for UK users. As is so often the case, Apple is not the primary innovator in this space, but its adoption of the technology will likely open the floodgates for more popular use.

Security, as ever, is of the essence. To drive consumer trust in new payment methods, especially those that involve NFC, fraudulent use of these technologies must involve as much friction as possible. At the same time, reducing user inconvenience while raising security is vital; no one will adopt technology that is hard to use, especially with something as quotidian as payment.

If there's one area of life we want to be simple, it's how we pay for things. Easy, speedy payment encourages spending. But speed isn't enough; it needs to be secure – ideally, even more secure than using a credit card, or walking the streets with a wallet full of cash. Technologies that somehow strike that balance – achieving ease, and speed, of use, while enabling the user to have peace of mind – are security's Shangri-La.

It's important that mobile hardware and software developers get it right, or they risk delaying the mobile payment project for years as it struggles under the weight of consumer mistrust.

Indeed, research shows that mistrust in mobile payment seems entrenched, even before the technology has really become widespread. A recent YouGov study found 47% of respondents did not want to use their mobile phone for payments with 81% highlighting concerns over security.

Similar wariness followed the introduction of the first contactless debit cards. However, initial 'here-be-witchcraft' skepticism about the safety and security of NFC plastic cards seems to have faded for UK consumers. Visa Europe predicts £1.2bn of contactless mobile payments will be made every week by 2020. The same study found that the UK spent £2.32bn with contactless cards last year.

Worldpay reports it has now processed over £2bn in UK contactless payments since January 2012. It took until October 2014 to reach that first £1bn. That means contactless transactions rose 49% in the last six months. The number of contactless transactions has risen by 964% in two years. Contrast the US, where only 40 million contactless payments were made in the whole of 2014. The UK beat that in December alone.

Clearly there is strong appetite in Blighty for adopting new payment technologies, even if initial distrust is prominent. It's hardly surprising, after all, given that people's finances are at stake, and trust in the banking sector is shot post-2008. If faith in banks is low, it's incumbent on the mobile payment software providers to take risk out their hands.

The ball, for now, is in Apple's court. With Apple Pay, it seems to have created a secure technology that can offer peace of mind to users. No card details are stored or transmitted locally, and instead one-time tokens are transmitted to the payment terminal (when used physically in-store) to verify payment. Payments can only be activated using the biometric fingerprint sensor, TouchID, found on the newest models of Apple hardware.

If it can be successful in the US, where there is typically less friction around making payments and therefore more opportunities for fraud, it can work here. Indeed, much early Apple Pay fraud Stateside fell at the banks' feet, with stolen card-not-present data sold by hackers on the black market being used to set-up Apple Pay accounts. The banks did not make it hard enough to verify that card-holders were legitimate.

In the UK, where multi-factor authentication and Chip and PIN are long-established, fraudsters' chances of success will diminish.

The security commentariat was quick to respond to the Apple Pay UK launch news. Some welcome the moved to a biometrically-authenticated system, others expressed concerns about spoofing of payment entry forms in iOS, and other hypothetical security holes that could be exploited by highly savvy and dedicated criminals.

Of course, the old mantra, there is no such thing as 100% security, always applies. In the world of virtual banking, still a maturing technology, this is truer than ever. Thankfully, Apple, and hopefully its counterparts in Android and Samsung when launched, has started out setting the bar high. Wide adoption is more or less inevitable – so this is a chance for the industry to do something it's not been best at over the years: getting it right first time round.

Mike Hine, Deputy Editor

> Easy, speedy payment encourages spending. But speed isn't enough; it needs to be secure – ideally, even more secure than using a credit card or cash