ELSEVIER

network SECURITY

ISSN 1353-4858 July 2016

www.networksecuritynewsletter.com

Featured in this issue:

No place to hide as DNS comes under attack

Recent analysis demonstrates that the majority of the underlying infrastructure used to launch cyber-attacks lies in some of the world's most developed countries, exploiting weaknesses in DNS technology.

As a vital component of network architecture, DNS should not be overlooked and left unprotected. By employing intelligence on the types of threats facing their DNS infrastructure and taking the steps necessary to impede malicious domains, organisations can take control of their DNS, transforming it into a source of security, says Dr Malcolm Murphy of Infoblox.

Full story on page 5…

The implications of Apple's battle with the FBI

The recent high-profile clash between the FBI and Apple in the US has reopened a debate on privacy that has far-reaching implications.

Alongside calling into question the rights of government in relation to whether there are legal precedents for forcing tech companies to grant access to code and data, the dispute has raised public awareness of digital privacy and civil rights issues. What's at stake is the point at which digital security ends and national security begins, argues Michael Hack of Ipswitch.

Full story on page 8…

How data breaches lead to fraud

Many people will remember 2015 as a year of major data breaches. It wasn't just the sensitivity of the information but the variety of sources from which customer's data was compromised.

These breaches happen because the data stolen is valuable. And in many cases the stolen data is considered valuable because it can be used to defraud businesses. But if organisations get smart and get prepared for fraud, this data won't be as valuable, explains Don Bush of Kount.

Full story on page 11…

Authorities losing the battle against cybercrime, says UK National Crime Agency

The UK's National Crime Agency (NCA) has issued its first report on cybercrime, and admits that it is losing the battle. However, some commentators in the information security industry have criticised the brief report for being too vague and lacking detail.

The report says that, "the accelerating pace of technology and criminal cyber-capability development currently outpaces the UK's collective response to cybercrime. This 'cyber arms race' is likely to be an enduring challenge, and an effective response requires collaborative action from government, law enforcement, industry regulators and, critically, business leaders."

Continued on page 2…

Contents

Editorial Office:
Elsevier Ltd
The Boulevard, Langford Lane, Kidlington,
Oxford, OX5 1GB, United Kingdom
Tel: +44 1865 843239
Web: www.networksecuritynewsletter.com

Publishing Director: Bethan Keall

Editor: Steve Mansfield-Devine
E-mail: smd@contrarisk.com

Senior Editor: Sarah Gordon

Production Support Manager: Lin Lucas
E-mail: l.lucas@elsevier.com

Subscription Information
An annual subscription to Network Security includes 12 issues and online access for up to 5 users.
Prices:
€1424 for all European countries & Iran
US$1594 for all countries except Europe and Japan
¥189 000 for Japan
Subscriptions run for 12 months, from the date payment is received.
More information:
http://store.elsevier.com/product.jsp?isbn=13534858

12987

Pre-press/Printed by
Mayfield Press (Oxford) Limited

…Continued from front page

According to the NCA, the most advanced and serious cybercrime threat to the UK is the direct or indirect result of a few hundred international cyber-criminals who target UK businesses to commit highly profitable, malware-facilitated fraud. Data breaches are the most common cybercrimes committed against businesses and the NCA estimates that cybercrime costs the UK economy billions of pounds per year.

Under-reporting continues to obscure the full impact of cybercrime in the UK. This shortfall in reporting hampers the ability of law enforcement to understand the operating methods of cyber-criminals and effectively respond to the threat. The NCA is urging businesses to view cybercrime not only as a technical issue but as a board-level responsibility, and to make use of the reporting paths available to them, sharing intelligence with law enforcement and each other.

The NCA's National Cybercrime Unit leads the UK's response to cybercrime, working in partnership with police forces, Regional Organised Crime Units and international law enforcement partners, to share intelligence and identify the most significant cyber-criminals worldwide.

"This is the first time the NCA has released a joint assessment with industry on cybercrime," said Jamie Saunders, director of the NCA National Cybercrime Unit. "I hope that senior members of UK business, and not only those involved in the protection of their IT systems, take note of its contents and think seriously about ways that they can improve their defences and help law enforcement in the fight against cybercrime."

However, Steve Durbin, MD of the Information Security Forum (ISF), commented: "For anyone who has been monitoring the cybercrime space, the NCA Cybercrime report doesn't really contain any significant 'aha' moments. The question really is how can law enforcement be seen to be adding a new dimension to protecting and anticipating advanced attacks, not just working to bring perpetrators to justice. Law enforcement is primarily concerned with crime-prevention and bringing perpetrators of crimes to justice. Businesses are concerned with ensuring the integrity of their systems and information in a way which does not lend itself to necessarily supporting law enforcement."

The report is available here: http://bit.ly/29uEVqL.

Police breached thousands of times

In the past five years, there have been "at least 2,315 data breaches" involving UK police forces, according to a report by Big Brother Watch.

Based on the results of requests made under the Freedom of Information Act, the report – 'Safe in Police Hands?' – raises significant questions about the amount of data being gathered and stored by police forces. Big Brother Watch says the results "show officers misusing their access to information for financial gain and passing sensitive information to members of organised crime groups" and that during the period covered more than 800 members of staff at police forces "accessed personal information without a policing purpose" and information was "inappropriately shared with third parties more than 800 times".

Of the breaches disclosed, more than half (55%) did not lead to any formal disciplinary action. In 11% of cases those responsible received either a written or verbal warning; 13% of cases led to individuals resigning or being dismissed; and just 3% of breaches resulted in either a criminal conviction or caution.

The report is available here: http://bit.ly/29AHIBn.

Meanwhile, a database that lists 2.7 million people and organisations thought to present certain kinds of risk – including terrorism and money laundering – has been leaked online. The Thomson Reuters World-Check database is widely used by banks, government and intelligence agencies, employment agencies and law firms. Researcher Chris Vickery found that an old version of the database was accessible by anyone, although he has kept details of where he found it to himself. The most likely explanation is that someone with legitimate access to it made the database available.

In brief

UN calls for online human rights

The United Nations has recognised the role the Internet plays in all our lives by passing a resolution that calls for human rights to be extended online. People should be able to use the Internet for free speech and free assembly without fear of surveillance or hindrance, it says. The resolution also calls "upon all States to bridge the gender digital divide and enhance the use of enabling technology, in particular information and communications technology, to promote the empowerment of all women and girls", and made similar pleas for disabled people. Although the resolution is not legally binding on any nation, 17 countries opposed it, and Russia and China attempted unsuccessfully to impose amendments that would have weakened the text by eliminating its human rights approach. One failed amendment tried to remove references to the UN Declaration of Human Rights (UNDHR). The text of 'The promotion, protection and enjoyment of human rights on the Internet' is available here: http://bit.ly/29tLsXb.

Half of SMEs attacked

Research by the Ponemon Institute shows more than half of small and medium-size enterprises (SMEs) endured one or more cyber-attacks in the past year, and around the same number suffered breaches involving customer and employee data. The report, '2016 State of Cyber Security in Small & Medium-Sized Businesses', concludes that: "No business is too small to evade a cyber-attack or data breach. Unfortunately, smaller organisations may not have the budget and in-house expertise to harden their systems and networks against potential threats." In fact, only 14% of businesses surveyed regarded themselves as "highly effective" at mitigating cyber-security risks. Web-based and phishing attacks were the most prevalent, but the majority of actual breaches were the result of negligence by employees, contractors or third parties. The report is available here: http://bit.ly/29DSnwz. For more on SMEs and cyber-security, see pg 14.

Pokemon Go raises security fears

The new Pokemon Go game has raised a number of security issues and has led to players being robbed of their mobile devices. The game uses 'augmented reality' techniques in which characters are superimposed over real-time camera images on the players' phones or tablets. Players search for the characters and resources in real-world locations. But these locations are known to everyone and it has been reported that criminals have been lying in wait for players in order to rob them of their mobile devices. In addition, many security specialists are concerned that the game app is effectively tracking the players and also requires excessive permissions – for example, wanting full access to the player's Google account. And it seems that trojanised versions of the game app have made their way into a number of Android app stores. These versions contain malware and have been downloaded by a large number of users who were impatient about waiting for the official app to be available in their region.

New anonymising protocol

Researchers at MIT's Computer Science and Artificial Intelligence Laboratory and the École Polytechnique Fédérale de Lausanne have developed a new anonymising protocol that should be more resilient to attack than Tor. Called 'Riffle', it builds on Tor's technique of multiple layers of encryption but also adds two new features. First, it randomises the order in which servers pass on data packets, so that attackers can't use traffic analysis techniques on incoming and outgoing data. And it uses signing techniques to prevent rogue servers from sending forged messages. While both techniques have been available for years, the team, led by MIT grad student Albert Kwon, has used a mix of public-key and symmetric cryptography to overcome technical issues that prevented them being implemented in practical systems. There's more information available here: http://bit.ly/29BDKr7.

Password reuse tool

One of the major threats caused by database leaks is that compromised passwords are often reused on other sites. For example, a database of 33 million Twitter credentials that was recently offered for sale on underground forums was probably created by trying password leaks from other sites. Now there's a tool available that allows 'researchers' – and anyone else – to automate the process of trying leaked credentials against a number of sites. Dubbed 'Shard', the tool has been uploaded to GitHub by Philip O'Keefe of Netsuite. It's currently capable of testing passwords against Reddit, Twitter, Instagram, Facebook and LinkedIn, but O'Keefe says that it's possible to add other sites very easily. There's more information here: https://github.com/philwantsfish/shard.

Defeating ransomware

Researchers at the University of Florida and Villanova University have developed a potential defence against ransomware that relies on spotting what the malware is up to and stopping it in its tracks. They describe the approach as a "save what you can" technique that is capable of recognising when ransomware has started to encrypt a victim's files. It then halts the process and alerts the user – the latter being important because it's possible that the encryption activity is actually genuine, such as when tools like PGP disk encryption or compression utilities are being used. In tests, the researchers say they managed to stop ransomware in its tracks when it had encrypted only 0.2% of the files on a drive. There's more information here: http://bit.ly/29uW2JH.

Privacy Shield comes into force

The Privacy Shield agreement between the EU and the US has been officially adopted by the European Commission. Under the agreement, US-based organisations can move data they have gathered relating to EU citizens outside the continent – for example, to servers in the US – without falling foul of EU data protection regulations. This capability was previously provided under the so-called Safe Harbour provisions, but they were rendered null and void after a legal challenge. According to the EC, the Privacy Shield agreement will provide EU citizens with easier redress in the case of complaints, and imposes stronger obligations on the organisations handling the data. There will also be an annual review.

Spotting encrypted malware traffic

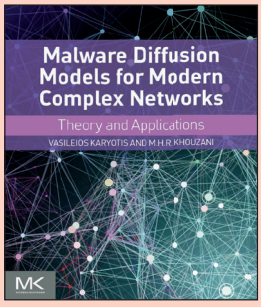
Researchers at Cisco have developed a method for spotting malicious data in encrypted traffic, according to a new paper. Malware now commonly encrypts its own traffic – for example, to command and control servers – using TLS. This usually makes it impossible for firewalls and other defences to detect that the traffic is malicious because it looks like any other TLS-encrypted data, such as email or web traffic. However, TLS encryption actually introduces what the authors call "observable data features" that allow monitoring software to make inferences about both client and server. This means, they add, that, "malware's usage of TLS is distinct from benign usage in an enterprise setting, and that these differences can be effectively used in rules and machine learning classifiers". The paper is available here: http://arxiv.org/pdf/1607.01639v1.pdf.

Hiring hackers

Security firm Radware has found that more than 20% of UK businesses have invited hackers to assess their security systems and a further 37% are open to the idea. Its new report also found that three in five respondents experienced a cyber-attack in the past 12 months. Concerns over the growing threat led four in five respondents to state that security is now a CEO or board-level concern while 33% stated that a change in C-level awareness is critical in order to thwart the latest attacks. Among the leading concerns for executives is the Internet of Things (IoT), with connected devices identified by 29% as 'extremely likely' to be a target for cyber-criminals over the next three to five years. Ransomware is high on the agenda too, with around one in seven respondents experiencing a ransom attack over the last year. In fact, at least three companies said they were under attack at the time of the survey. The report is available here: http://bit.ly/29tO6Mg.

Reviews

BOOK REVIEW



Malware Diffusion Models for Modern Complex Networks

Vasileios Karyotis and MHR Khouzani. Published by Morgan Kaufman. ISBN: 978-0-12-802714-1. Price: 85.95, 324pgs, paperback.

Malware is often regarded as though it were a disease. We even use the term 'virus' for certain forms of malware, and non-specialists tend to use that word for all forms of malicious software. We also understand that malware propagates via 'infection'. Yet even many information security specialists will struggle to describe exactly how this occurs. And almost none can predict the pattern or extent of an outbreak.

The behaviour of malware is often very complex. The creators of the software frequently build in safeguards in an attempt to protect themselves. For example, it's common for malware to remain dormant, or deactivate itself, if it finds the host machine has an IP address known to belong to a security company, such as anti-virus software vendors (which is why those vendors use virtual machines in isolated environments for testing). Or the malware may remain equally inactive if the language of the host device is Russian.

These are just simple examples, but with other built-in behaviours they contribute to the complexity we see in malware diffusion. This is also exacerbated by the inherent complexity of modern IT environments. For example, a single device may attach to a number of networks – wifi, 3G or corporate and home networks – with very different topologies in a single day.

Clearly, malware is a problem for everyone. We can all end up out of pocket and severely inconvenienced, and in some instances an infection can spell disaster. For organisations, though, the problem is even worse, in that dealing with malware creates a heavy burden and a source of considerable cost even if no infection occurs. Equipping networks and endpoints with anti-malware capabilities is expensive in terms of installation, processing power and bandwidth.

Understanding how malware works – and especially how it spreads – is therefore of great importance. According to the authors of this book, however, much of the theory underpinning our knowledge of malware diffusion is incomplete, or is based on a somewhat pragmatic and empirical approach – such as watching malware spread and then attempting to deduce its nature from the data.

The aim here, then, is to provide mathematical models for malware diffusion that describe the behaviour and dynamics of malicious software in modern communications networks. The focus is largely on wireless networks, but much of what's covered here is applicable to wired networks too.

The subtitle of the book is 'Theory and Applications'; however, this is not something that infosecurity practitioners or network managers will find useful in their day-to-day activities of protecting their systems. The emphasis is very much on the theory side, building mathematical frameworks in order to understand malware behaviour. As such, it ranges (in the words of the authors) from "models that are based on systems of ordinary differential equations … to more exotic analytic tools founded on queuing systems theory, Markov Random Fields, optimal control and game theoretic formulations".

If you need any part of that sentence explaining, this book probably isn't for you. So who is it for? While the authors say it should be of interest to final-year graduate students, I suspect it's more likely to appeal to post-doctoral students and highly specialised researchers with a strong grasp of the mathematical techniques used (such as probability and statistical analysis).

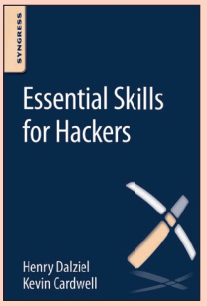
That's not to say that the models discussed here have no practical application. In fact, the third and final main section of the book is all about how the malware modelling frameworks can be applied. This is still, however, at a relatively abstract level, offering theoretical blueprints for applying the frameworks to analytical processes.

With any luck, the understanding of malware behaviour that this kind of mathematical modelling could give us will ultimately result in better security products. There is still something of a gap to be bridged, however, between this theoretical level and products and processes we can actually use to protect ourselves. And, of course, malware evolves all the time, changing its behaviour as it goes. So expect to see a second edition of this book in the not too distant future.

There's more information available here: http://bit.ly/29so0Im.

– SM-D

BOOK REVIEW



Essential Skills for Hackers

Kevin Cardwell, Henry Dalziel. Published by Syngress. ISBN: 978-0-12-804755-2. Price: 28.95, 48pgs, e-book and paperback editions available.

This is yet another in a series of slim volumes looking at different areas of information security and penetration testing. Each book offers a basic overview of its subject, providing an introduction for newcomers.

In this case, the 'essential skills' tackled in the book's 40-odd pages all revolve around network traffic. The three chapters deal with network protocols, packet headers and analysing traffic. A better title for the book, then, might have been 'an introduction to understanding Wireshark captures'.

Wireshark is, indeed, the central tool used here. The contents of this book are pretty much what you'd expect to find as a chapter in a more in-depth volume on network traffic analysis or penetration testing techniques. As a standalone book, it's therefore fairly lightweight. However, if understanding network packets is your weak point, or something you have yet to tackle, it does offer a concise introduction. It's usefully illustrated, too.

As with many of the others in this series, the style of the book is something of an acquired taste. It reads like a transcription of a presentation, with sentences that are often clumsy, rambling and ungrammatical. One feels additional editing wouldn't have been wasted. However, the key information is in there, even if you have to make some additional effort to extract it.

There's more information here: http://bit.ly/29B7WGd.

– SM-D

No place to hide as DNS comes under attack


Malcolm Murphy

Dr Malcolm Murphy, Infoblox

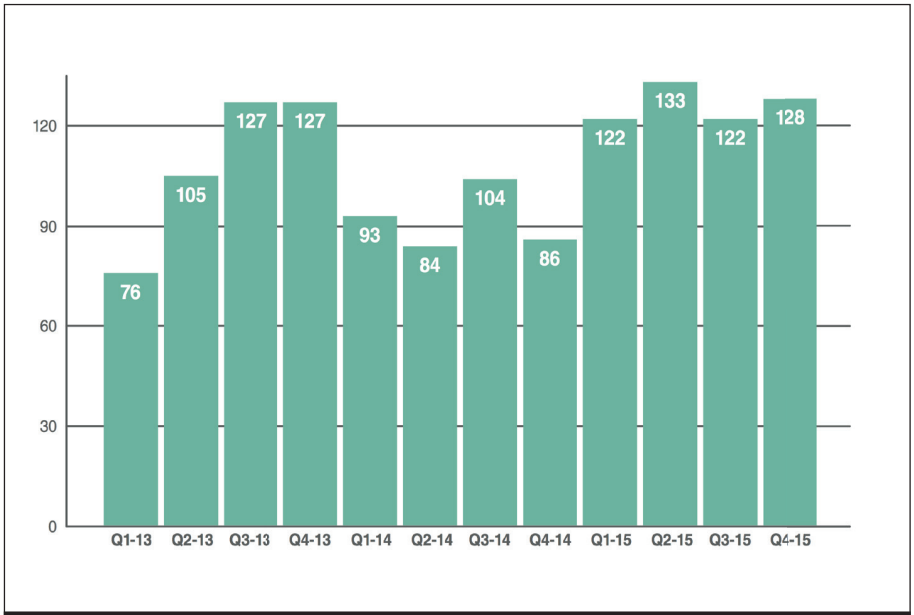
It is commonly assumed that most cyber-attacks originate from hotspots in Eastern Europe, Southeast Asia and Africa, where infrastructure is not especially well policed. However, recent analysis demonstrates that the majority of the underlying infrastructure used to launch these attacks lies safely and comfortably in some of the world's most developed countries.[1] This is according to the latest DNS Threat Index which found that the US and Germany account for more than 90% of malicious infrastructure created from October to December 2015.

The DNS Threat Index

The Infoblox DNS Threat Index is a quarterly indicator of malicious activity across the globe that exploits the Domain Name System (DNS), the address book of the Internet required for almost all Internet connections.[2] Using data from a range of sources including government agencies, Internet service providers, enterprise network operators and open sources, the index tracks the creation of malicious domains tied to 67 separate threat categories. These new domains are created by cyber-criminals as a foundation for unleashing a variety of threats ranging from simple malware to exploit kits, phishing, distributed denial of service (DDoS) attacks and data exfiltration.

To build the index, proprietary methods and capabilities are used to examine data on domains across the world associated with malicious activities. A broad network of partner organisations, Internet infrastructure companies and law enforcement agencies provide indicators of malicious domains to create a representative sampling, rather than a comprehensive list, of bad domains.

Newly observed malicious domains are categorised by the type of threat they represent, with the 67 most active threat types factored into calculations for the index. To reflect the mix of actual threats in use, these categories are continuously adjusted as new threat classifications emerge and become more active, while others become less active or disappear.



The DNS Threat Index over time. The baseline is 100. Source: Infoblox.

It's important to point out, however, that while the report identifies the top countries for hosting infected systems, it does not indicate in any way where the criminals are based. After all, it's possible to develop malware, such as exploit kits, in one country, sell it in another and launch it from a third using systems hosted in a fourth. Indeed, this is one of the reasons it's so difficult to bring an end to cybercrime.

The index can, however, highlight those countries which are subject to lax regulations or policing or, in some cases, both. In doing so, it's then possible to identify the areas that require improvement.

Popular countries for malicious attacks

By far the most popular country for hosting and launching malicious attacks during the final three months of 2015 was the US, which accounted for 72% of malicious domains within an identifiable country of origin. Second to the US and the only other country to register above 2%, was Germany at 19.7%.

There are two conclusions to draw from these findings. The first is that protection is not dependent on location. As we can clearly see, the fact that a domain is hosted in a major industrial nation such as Germany or the US does not necessarily make it safe.

Given its position as the world's top economy, it's perhaps understandable that the US is viewed as such a desirable target for cyber-criminals. However, the index reveals the extent to which it can be seen as a soft target too. Not only are the country's businesses and individuals vulnerable to cyber-attack, but its host-

ing infrastructure appears to be especially easy to penetrate and exploit for malicious purposes.

The second conclusion is that these countries' rich technology and infrastructure are as appealing to cyber-criminals as they are to legitimate businesses. This, however, makes that infrastructure especially difficult to fortify against exploits as this would risk limiting much of the speed and responsiveness that makes it so attractive to businesses in the first place.

"The US is home to hosting providers of all sizes who can be very slow to respond, allowing exploits to propagate for longer than they should"

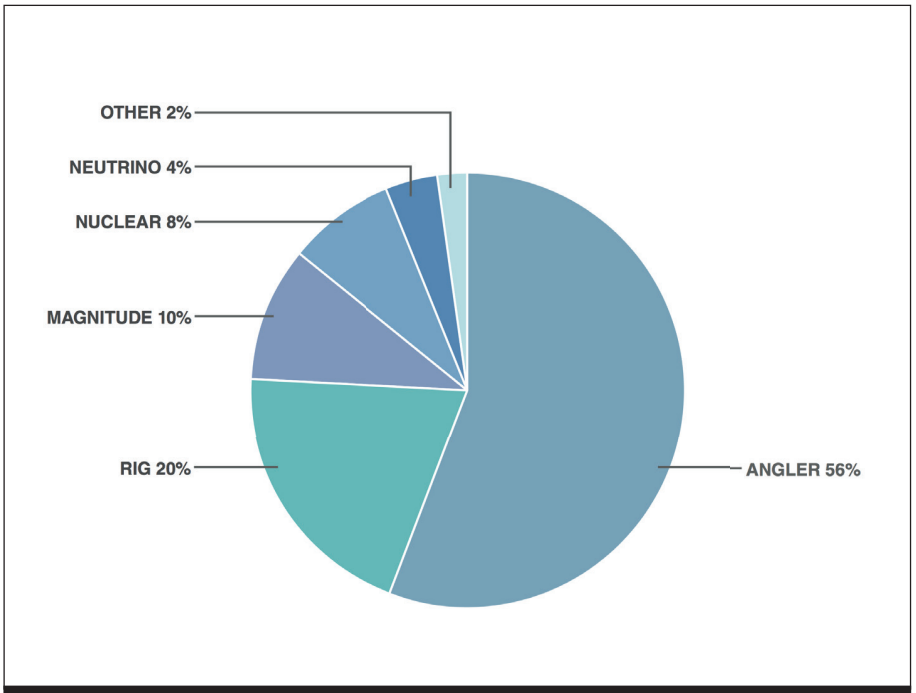
One would expect that, without facing the kind of language barriers, cross-border jurisdiction issues and policy differences that confront an international policing and take-down effort, hosting providers in the US would be quick in taking down a malicious domain once it has been identified, thereby limiting any potential damage. Unfortunately, though, this doesn't currently appear to be the case. Indeed, as well as defining the average global response time, the US is also home to hosting providers of all sizes who can be very slow to respond, allowing exploits to propagate for longer than they should.

A break in the cycle

In addition to highlighting just where they were being hosted, the threat index also identified what appears to be a break in the traditional pattern of how these malicious infrastructure domains are being created.

The cycle of planting and harvesting, which contains periods of increased activity and subsequent lulls in the creation of malicious domains, has historically provided an indication of future trends.

The planting phase sees the rapid creation of DNS infrastructure by cyber-criminals and domains being set up to be used as bases for launching attacks. The resulting significant increase in the number of malicious domains associated with exploits kits and malware is reflected by a rise in the threat index.



Newly observed exploit kit activity in Q4 2015. Source: Infoblox.

Towards the end of this phase, attackers will begin harvesting the infrastructure they've created to launch attacks, steal data and generally cause damage to their victims' networks. The threat index, tracking the appearance of new threats and locations, will then fall correspondingly, even if overall malicious activity hasn't subsided.

However, while the index dipped from Q2 to Q3 2015, suggesting the beginning of a harvesting cycle, it immediately rebounded in Q4 to an all-time high. Although it may be too soon to say for sure, this apparent break in the plant/harvest cycle may indicate a new trend of cyber-criminals continuing to create malicious infrastructure while, at the same time, harvesting stolen data.

Exploit kits

Much of this malicious infrastructure is being used in the creation of exploit kits, a particularly alarming category of malware that represents the automation of cybercrime. Toolkits-for-hire that deliver malware via drive-by download, exploit kits require no knowledge on the attacker's part of how to create or deliver an exploit in order to infect a system, effectively lowering the technical bar for spreading malware. Worryingly, many of these kits feature a user-friendly interface from which attackers are able to manage and monitor the malware campaign.

Targeting potential victims via spam emails or malicious ads on compromised websites, exploit kits will typically take advantage of security holes or vulnerabilities in operating systems, browsers and even some popular software such as Java or Adobe Flash to deliver payloads. In the past, these have included banking malware, advertising click-fraud malware and ransomware.

"With users typically taking fewer security precautions than with computers, mobile devices tend to be easier to compromise. It's not unlikely then, that attackers will gradually move to delivering mobile malware"

While the vulnerabilities used to infect visitors and the tricks used to defeat anti-virus defences will differ from kit to kit, the kits themselves are typically made up of three common components. The back end contains a control panel and payloads, while the middle layer contains the exploits and creates the tunnel to the back-end server, and the proxy layer serves the exploit directly to the victim.

Primarily targeting computers, exploit kits can also be used to compromise mobile devices. Indeed, due to the vast number of people using them for tasks such as email, browsing, banking and social media, smartphones and tablets are becoming an increasingly popular target. Furthermore, with users typically taking fewer security precautions than with computers, mobile devices tend to be easier to compromise. It's not unlikely then that attackers will gradually move to delivering mobile malware through mobile browser web pages, much in the same way that infections are delivered on conventional computers.

"As exploit kits are updated, past threats may begin to reappear under new guises and, with Angler leading the charge, it's never been more important for organisations to protect their DNS infrastructure"

Regardless of an exploit kit's target, whether it be mobile or computer, a successfully delivered payload will be behind the firewalls of the victim's company or service provider. From here, the malware can be spread to other devices and can use the Internet to communicate with its command and control (C&C) server from which it is able to download further malicious software or exfiltrate data. In most cases, the communication between device and C&C requires the use of DNS.

Angler and RIG

Angler, one of the most sophisticated exploit kits currently being used by cybercriminals, was identified by the threat index as the most popular DNS exploit activity in the last quarter of 2015.

This particular form of exploit kit is infamous for the pioneering 'domain shadowing' technique it uses to defeat reputation-based blocking strategies and for infiltrating malicious URLs into legitimate ad networks, leading users who click links in the infected ads to websites which then insert malware.

Often quickly updated with the latest zero-day vulnerabilities in popular software, Angler exploit kits use sophisticated obfuscation techniques that make it difficult for them to be detected by traditional anti-virus technologies. Their constant and ongoing evolution means organisations must invest in protection technologies that not only address one aspect of the exploit but are able to detect and disrupt activity across the whole kill-chain.

The quarter's second most popular exploit was RIG, an older kit that over recent quarters had seen far less common usage. First identified in 2013, RIG, along with other exploit kits at the time, increased in popularity following the arrest of the creator of the Blackhole exploit kit, which subsequently lost its position as the year's most prevalent web threat. It's believed that the leak of RIG 2.0's source code in 2015 led to its developer creating RIG 3.0, a version which, according to SpiderLabs, was infecting an average of 27,000 machines a day in mid-2015, with 90% of the traffic resulting from malvertising.

As it grew in popularity, analysis of RIG activity in 2015 shows it beginning to use shadowing techniques such as those pioneered by Angler in order to defeat reputation-based blocking strategies. The increasingly sophisticated use of RIG suggests that as exploit kits are updated, past threats may begin to reappear under new guises and, with Angler leading the charge, it's never been more important for organisations to protect their DNS infrastructure.

Internal DNS security

Effective internal DNS security solutions can be deployed to help protect against malware exploiting an organisation's DNS to further infect its network, as well as prevent it being used as a vector for data exfiltration, all without the need to change its existing network architecture.

DNS response policy zones (RPZs) on internal DNS, running in conjunction with a threat intelligence feed of known malicious destinations, will enable a DNS appliance to intercept DNS queries associated with known malware, effectively blocking the threat by interrupting its communication with external C&C servers. Cutting connection with a C&C server prevents the exfiltration of data using standard network protocols while simultaneously reducing the risk of infection and preventing malware from breeding within the network. Additionally, internal DNS security can detect and prevent data exfiltration via DNS tunnelling by establishing query thresholds that will enable any unusually large queries or responses to be detected and flagged.

A vital component of network architecture, DNS should not be overlooked and left unprotected, particularly with exploit kits and other attack vectors taking advantage of its vulnerabilities for criminal gain.

By employing intelligence on the types of threats facing their DNS infrastructure and taking the steps necessary to both identify and impede malicious domains and their inbound and outbound communications, organisations can take control of their DNS, transforming it from a network vulnerability into a considerable source of security.

About the author

Dr Malcolm Murphy is systems engineering manager at Infoblox. His experience with DNS dates back to the mid-90s, and as a Unix sysadmin he worked out a method of using DNS to hide messages in plain sight, with no audit trail. He also claims there was a valid reason for doing so at the time, although he can't remember what it was. He has spent most of his career helping organisations deploy networking and security infrastructure and currently leads a team of technical consultants at Infoblox, specialising in scalable, secure, cloud-ready DNS solutions.

Resources

1. More Than 90% of Newly Observed Malicious Domains Worldwide Hosted in the U.S. and Germany, According to the Infoblox DNS Threat Index'. Infoblox, 23 Mar 2016. Accessed Jun 2016. www.infoblox.com/company/news-events/press-releases/2016/more-90-percent-newly-observed-malicious-domains-worldwide-hosted-us-and-germany-according-infoblox-dns-threat-index.
2. 'Infoblox DNS Threat Index'. Home page. Infoblox. Accessed Jun 2016. www.infoblox.com/dns-threat-index.

The implications of Apple's battle with the FBI

Michael Hack

Michael Hack, Ipswitch

The recent high-profile clash between the FBI and Apple in the US has reopened a debate on privacy that has far-reaching implications that extend far beyond the semantic boundaries of the security and privacy models pursued by the technology sector.

Alongside putting the rights of government into the frame, in relation to whether there are legal precedents for forcing tech companies to grant access to code and data when national security is at risk, the dispute has raised public awareness of digital privacy and civil rights issues. What's at stake is the point at which digital security ends and national security begins. And it's forcing governments, citizens and tech companies to examine the 'ins and outs' of data encryption – what makes the technology effective, and how much control individuals should have over a broad range of personal data held on devices such as phones.

In the process, the Apple/FBI showdown has also raised the question of whether tech companies should be required to subvert their own privacy systems, building 'back doors' into their security systems that enable the hacking of customer devices and data.

It's an issue that has far-reaching connotations. As consumers connect more and more of their devices to the Internet, the wider ramifications of the Apple/FBI battle extend to who, in the future, potentially has access and control over the growing number of Internet of Things (IoT)-connected devices that are capable of tracking where we are, what we are doing, how we drive, who we socialise with – and more.

The encryption conundrum

In February this year, the FBI called on Apple to help them hack an iPhone belonging to Islamic State-inspired terrorist Syed Rizwan Farook, who had opened fire on a local government office building in San Bernardino in December 2015, killing 14 people.

Despite Apple providing the FBI with data obtained from the weekly back-ups Farook had made using Apple's iCloud service, FBI investigators believed the iPhone itself contained important additional data about Farook's motives along with his contacts list. The phone's contents, however, were encrypted and FBI agents weren't willing to risk the phone's automatic data wipe facility kicking in should more than 10 incorrect passcode entries be made.

Apple refused to comply, so the FBI pursued a US court order that would compel the company to subvert its own encryption systems and provide a back door entry to the iOS operating system. In response, Apple argued this would force it to create a weak link in its encryption which, while speeding up the investigation of crimes such as this, would also put the privacy of millions of law-abiding iPhone users at risk.

"Once you have holes in encryption, the rule is not a question of if, but when those holes will be exploited and everything you thought protected will be revealed"

Apple's stated contention was that any such back door represented a potential security vulnerability that would quickly become a target for hackers and cyber-criminals, resulting in the personal data stored on iPhones – including banking details, health records and details of frequently visited locations – potentially becoming accessible to any cyber-geek

An Apple iPhone 5C, similar to that owned by Syed Farook, which became the centre of the dispute between Apple and the FBI.

Tim Cook, Apple CEO: "There's no such thing as a back door for the good guys only."

determined enough to crack the code.

As California Congresswoman Zoe Lofgren, commented: "Once you have holes in encryption, the rule is not a question of if, but when those holes will be exploited and everything you thought protected will be revealed."

The stance of Tim Cook, Apple's CEO, is clear. He has publicly stated: "There's no such thing as a back door for the good guys only," and has urged the Obama administration to make a public statement in support of strong encryption.

Cook's position has gained widespread support from other big-name tech companies. Google, Facebook and Amazon, among others, have all rallied behind Apple, expressing concerns about the ramifications of this dispute in relation to the privacy and safety of their customers. Indeed, Microsoft's general counsel, Brad Smith, has called for everyone to "stand up with Apple in this important case," saying that "the path to hell starts with the back door".

National security vs data privacy

The current heated debate around encryption, data privacy and national security isn't a new one. Back in the (Bill) Clinton era, there was much controversy around the Clipper chip – a microcircuit capable of encrypting data while providing government access to the keys required to unlock it again. Fears of a potential public backlash, however, meant the chip was never adopted – and an important precedent for encrypted communications in the US was set.

Since then, a co-operative arms-length relationship had blossomed between US authorities and tech companies. Prior to this recent dispute, FBI investigators would have been given access to an iPhone sent to Apple along with a search warrant. But following the Edward Snowden revelations about NSA surveillance activities, in September 2014 Apple took the decision to introduce new encryption into its iPhone OS that made it 'impossible' for the company to unlock its own devices. It was a step that set up the conditions for the showdown with US authorities.

And it's not just authorities in the US that are trying to navigate the data privacy issue. The UK Government, for example, recently unveiled its Investigatory Powers Bill. Nicknamed 'The Snooper's Charter', the proposed legislation aims to give government agencies the freedom to undertake 'equipment interference' to investigate or prevent "serious crime" and "death or injury, or damage to a person's physical or mental health".

Widespread apprehensions about the new bill, due to be enshrined at the end of 2016, have been voiced by activist groups and human rights organisations. Concerns have been raised that the UK Government's exercise of these powers will not be subject to a meaningful judicial authorisation process and that its exercise of powers to compel technology companies to hack their own products or services will be wielded in secret, thanks to strict non-disclosure and gagging provisions.

The tech community has also expressed anxiety around these issues and others, including the lack of clarity around encryption, network integrity and cybersecurity requirements.

The narrative continues

Returning to the Apple/FBI saga for a moment where, following a New York judge's pronouncement that the US Government could not use the All Writs Act (1789) to force Apple to create a back door, the FBI suddenly announced it no longer needed Apple's help. With the help of a third party, it had managed to unlock the iPhone.

Despite Apple's request that the FBI share details of any vulnerability it found, the FBI is refusing to disclose the process or tool utilised to hack this particular iPhone model. For Apple, this represents a potential breach of its technology security that, in theory, could now be exploited by individuals operating outside the security services.

"Should citizens trust government with their information and accept government's ability to acquire this information, including accessing their private devices, in certain circumstances?"

The FBI's actions place organisations like Apple in uncertain territory. How much control over the integrity of their own security systems do they really have? And what are their rights to information

on any security flaw identified by government agencies which, if left unaddressed, potentially puts customers at risk?

Pundits have also raised the need for discussion around the broader issues the Apple/FBI dispute raises: namely, should citizens trust government with their information and accept government's ability to acquire this information, including accessing their private devices, in certain circumstances?

As the Apple/FBI dispute rumbles on, the lines between government organisations and high-tech companies appear to be hardening. WhatsApp, the instant messaging company, has recently announced it is implementing end-to-end encryption to protect all users' communications – a move that's likely to further infuriate the US Department of Justice, which has expressed strong reservations over unreachable information contained in devices.

State-sponsored hacking

Tech companies appear to be at an impasse with state authorities. Law enforcement agencies, in seeking to protect the public, have a vital job to do and have long had the right to violate people's personal space, with a court's approval – whether that's entering someone's home, or gaining access to financial or phone records.

But what's at stake now is whether high-tech companies can be forced to rework their products or circumvent their own security and grant government access to digital devices and networks. It's a landmark tech policy question that draws a line under the previous social contract between technology companies and government authorities.

The US and UK Governments aren't claiming they want to implement a surveillance state and are instead seeking to initiate a more balanced approach in which consumers generally maintain digital privacy – but in times of duress, criminal suspects might lose theirs. It's an important issue that requires some cold and rational debate.

Delegates at the recent RSA security conference held in San Francisco, however, universally agreed that inventing a back door was not the answer – and that weakening encryption was a misguided solution to resolving the wider state security issue.

Looking to the future

The very public squabble between Apple and the FBI will further fuel concerns around the world about just how secure corporate data is when processed and stored – both at home or overseas – by US companies, or held on devices developed by US companies.

It's also certain to make the work of the EU Working Groups currently finalising the Privacy Shield protocol that much harder in relation to how much protection will actually be afforded to EU citizens' data being transferred in and out of the US.

The issue of digital data protection, data privacy and the right of companies to build end-to-end encryption into their products, however, now poses a significant challenge for security agencies and the police, who believe that widespread encryption could hamper intelligence collection and provide a safe haven for criminals.

For tech companies, however, protecting the data of customers is a primary commercial driver. And there are wider concerns that deliberately compromising digital security could well undermine human rights around the globe, paving the way for countries like China to demand that a back door be built into all new technology innovations going forward.

"Should commercial tech organisations be forced to incorporate a back door, then this will represent a vulnerability that's open to exploitation"

Snowden's revelations spurred many US tech companies, like Apple, to review their encryption strategies, but the fear now is that knee-jerk reactions on both sides of the privacy/national security debate will now ensue.

Anti-encryption bill

Reports have already emerged that the FBI plans to brief US senators on drafting an anti-encryption bill – a move that could, warns US defence secretary Ashton Carter, prove detrimental for all. An advocate of commercial encryption, who doesn't believe in back doors or a single technical approach, Carter has recently exhorted technology companies to look for ways to compromise and address the needs of law enforcement agencies.

"Criminals will be able to enjoy the benefits of encryption mechanisms that keep their communications and activities safely hidden"

The chilling consequence of this very public dispute is that criminals potentially stand to gain, whichever way the decisions go. Should commercial tech organisations be forced to incorporate a back door, then this will represent a vulnerability that's open to exploitation. Should this not be the case, however, criminals will be able to enjoy the benefits of encryption mechanisms that keep their communications and activities safely hidden from law authorities. And law enforcement agencies may well be forced to illicitly hack commercial devices in secret – with no transparency and without recourse to requesting court orders to do so.

What happens next remains to be seen. But navigating a middle ground is going to prove difficult given the increasingly entrenched positions taken by governments both sides of the pond, and the tech industry itself.

About the author

Michael Hack oversees Ipswitch's entire EMEA business and is responsible for its operations and partner structure. He has many years of experience in IT firms in different software segments and markets. Prior to taking his role at Ipswitch, he was president at Sitecore, a global leader in customer experience management software. Hack has also acted as senior vice-president sales EMEA & International for the Enterprise Search Group at Microsoft.

How data breaches lead to fraud

Don Bush

Don Bush, Kount

The past few years have been particularly eventful and 2015 will be remembered for many momentous milestones. Those of us involved in security and fighting fraud online will remember it as a big year for major data breaches. A report carried out by PwC examining UK data breaches showed that not only had there been a rise in 2015 but that the scale and cost of these breaches had doubled.[1] The report concluded that data breaches, for large business, are "a near certainty".

According to Financial Fraud Action UK (FFA UK): "The rise across all fraud loss types during 2015 owes much to the growth of impersonation and deception scams, as well as sophisticated online attacks such as malware and data breaches."[2]

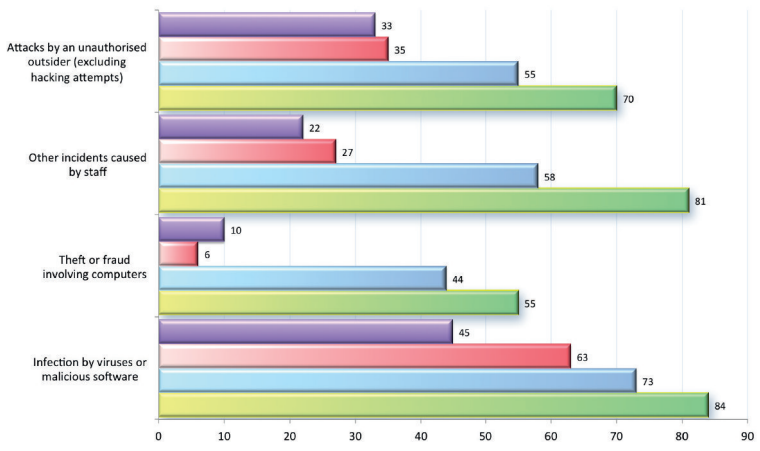
It wasn't just the sensitivity of personal information released into the public realm for fraudsters to find that made the year particularly memorable, but the extensive variety of sources from which customer's data was compromised. With that in mind, it's clear to see why financial institutions and consumers are so concerned about the increased number of records now on the open market because of security breaches.

In the UK, personal identifiable information has been leaked from numerous sources such as:

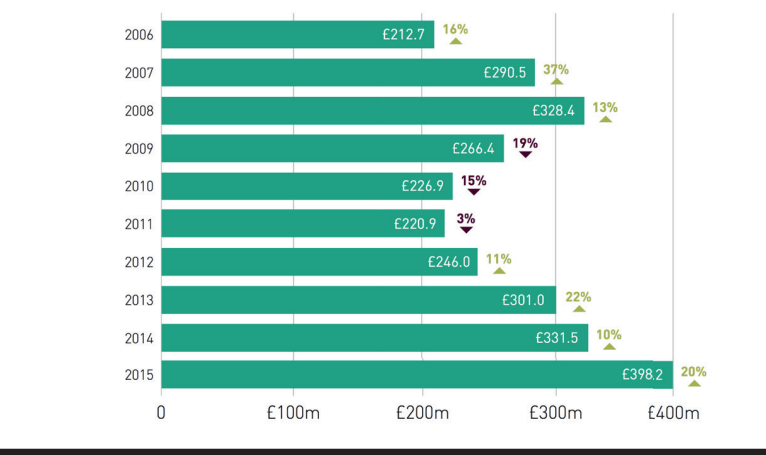
- **Local authorities:** it was revealed in 2015 that UK local authorities had suffered 4,000 data breaches between 2011 and 2014, compromising the details of millions of UK residents.[3]
- **Retailers:** JD Wetherspoon saw its database containing the names, email addresses, birth dates and card details of up to 656,732 customers violated by data hackers.[4] Up to 2.4 million Carphone Warehouse customers may have had their personal details accessed by hackers, including up to 90,000 credit and debit card details.
- **Banks:** in 2015, it emerged that every single major UK bank and lender (that's Barclays, HSBC, Lloyds Banking Group, NatWest, Nationwide and Santander) had contacted the UK Information Commissioner's Office about data breaches. The extent of these breaches remains unknown.[5]

These are just a few examples among many and data breaches continue to make the headlines with sobering regularity.

In the short term, these attacks mean less consumer confidence and less business for the businesses that were breached. CEOs fall on their swords to put new protocols in place and employ crisis PR



Types of breaches suffered by large organisations and small businesses in 2014 and 2015. Source: PwC.



Remote purchase (card not present) fraud losses on UK-issued cards, 2006-2015. Source: Financial Fraud Action UK.

trying to save face. There is also the legal requirement to notify the Information Commissioner's Office (ICO) and the possibility of being in breach of Privacy and Electronic Communications Regulations (PECR) leading to fines and other possible sanctions.

"What is happening with the 600,000-plus personal and financial details that JD Wetherspoons lost? Who is using the bank details from the UK's leading banks? And what are they using them for?"

In the longer term there is the genuine concern that data breaches will harm consumer and business confidence in online commerce and the digital economy. So the debates and arguments continue. Stakeholders wonder what to do, vendors produce new solutions that hackers then view as a challenge to be overcome.

Yet there is one issue that doesn't often get the coverage that it deserves: what is happening to all this leaked data? What, for example, is happening with the 600,000 plus personal and financial details that JD Wetherspoons lost? Who is using the bank details from the UK's leading banks? And what are they using them for? That's an aspect that doesn't hit the headlines, and yet it's the most important part of the story.

Causing fraud to rise

FFA UK is the UK's financial industry anti-fraud group and works alongside a dedicated police force to monitor and combat financial fraud in the UK. In March this year, it published its 2015 year-end report, announcing, as stated above, that "financial fraud losses across payment cards, remote banking and cheques totalled £755m in 2015, an increase of 26% compared to 2014."6

When looking for key drivers behind this huge increase, the experts at FFA UK are in no doubt: "The rise across all fraud loss types during 2015 owes much to the growth of impersonation and deception scams, as well as sophisticated online attacks such as malware and data breaches."

The message is crystal clear – data breaches in the UK are a significant cause of the increase in financial fraud in 2015.

It might seem obvious, but this is the first time that these two trends have been linked and causality demonstrated. The continued rise of CNP fraud in the UK is being driven by, among other things, the data illegally obtained via data breaches.

Of course, it's not just the financial data that is valuable, personal data is valuable too. According to Action Fraud UK, the UK's national fraud and cybercrime reporting centre, fraudsters need only know a customer's name, date of birth and address to open bank accounts and access credit in their name, which they can then utilise to take over their existing accounts and cards.7 When this information is taken from data breaches, fraudsters are able to get to work straightaway.

Data is out there, it is being used by criminals and it is driving fraud. The key question, then, is how can merchants brace against it?

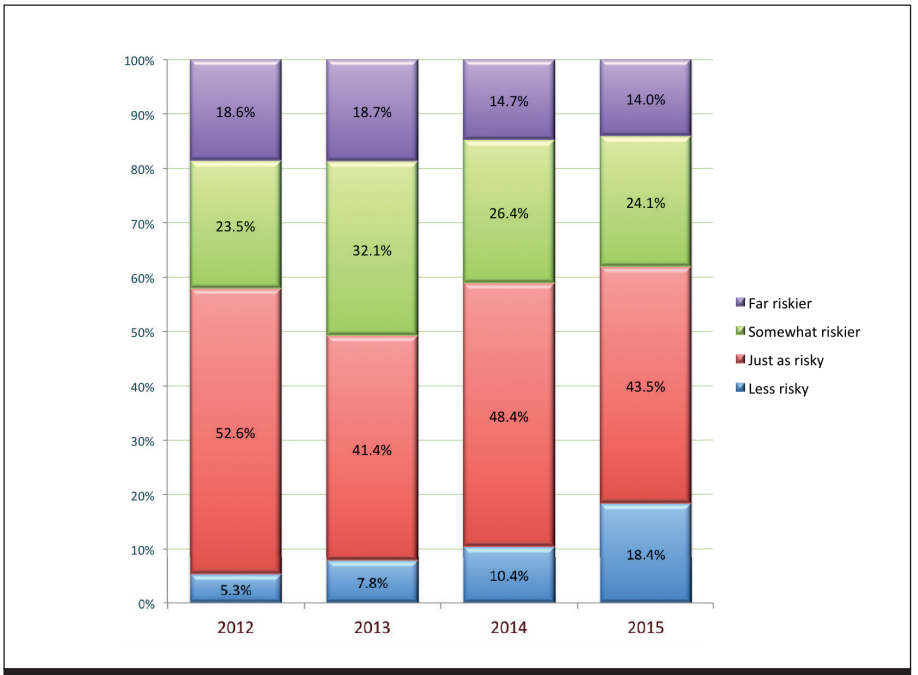
Bracing against breach-related fraud

Fraud costs merchants money in a number of different ways. Lost goods and lost revenue through chargebacks both hit merchants in the pocket. There is also the possibility that merchants will become too risk averse and tighten up their rules to the extent that legitimate transactions are declined because merchants do not have the protocols, expertise and systems in place to differentiate between fake and genuine consumers. Fraud is a real and present threat but our research has shown that merchants are still not receiving the critical intelligence they need to fight it.

In April 2016, we published our annual report and discovered that, despite these breaches and rising fraud, merchants were still not facing up to the threat of mobile fraud. Looking at the responses to three critical areas, we saw that although merchants seemed to be slightly more aware of the amount of fraud taking place, in some cases they seemed to be becoming less fraud-aware than they had been previously (see Table 1).[8]

Transactions taking place on mobile devices are the most vulnerable to intrusion and only around four in ten merchants believe it is important to detect mobile transactions. Detecting a mobile transaction is critical. This vital piece of intelligence should be a central part of evaluating the risk factors of any transaction. Without this knowledge, merchants are not making a fully informed decision about the level of risk presented by the transaction.

Equally, the tools that can track e-com-



Perception of mobile risk relative to e-commerce. Source: Kount.

	2015	2016	Change
Merchants aware of share of total fraud coming from mobile channel	40%	43%	+ 7.5%
Merchants who consider it very important to detect mobile transactions	46%	42%	- 8.5%
Merchants who believe that existing e-commerce fraud prevention tools are suitable for m-commerce	28.5%	36%	+25%

Table 1: Awareness among merchants of fraud.

merce fraud are not always up to the task of tracking m-commerce fraud. Different platforms require different security systems.

Thinking beyond the breach is critical for merchants. There is a demonstrable correlation between data breaches and fraud; figures from the US and UK bear this out. In the past year, there were 442,000 thefts of mobile devices in the UK.9 A significant proportion of these would have had payment and financial information stored on them. Multiply this by the increasing number of data breaches and merchants have to start getting mobile security savvy. Sadly, the research shows that merchants are still not prepared.

Conclusion

While these breaches are linked to a rise in fraud and the subsequent related issues such as chargeback and reputation damage, those who fear the rise of fraud can rest assured that precautions can be taken. Merchants can and should work to reduce their losses from fraud, and the following can help to arm against it:

- **Don't be complacent.** With mobile technology changing constantly, new opportunities are opened up for fraudulent activity. Make sure your business reviews and updates its security and anti-fraud measures to stay astride of technology and thieves alike.
- **Be aware of your business's limitations.** Many online merchants aren't experts in detecting or preventing fraud. It's important to put the right protections in place through a fraud prevention platform that will safeguard against fraudulent transactions without blocking legitimate sales.
- **Consider all payment channels in your calculations**. Fraud levels often vary between device platforms – Apple vs. Android vs. Windows. Knowing the type of device gives crucial intelligence into the risk level of the transaction.

Merchants need to start looking at data breaches as a four-minute warning of fraud. When a big data breach happens, it's not a question of if fraud will rise or even how much it will rise by. It's a question of when.

These breaches happen because the data stolen is valuable. And the data stolen is valuable because it can be used to defraud businesses. If businesses get smart and get prepared for fraud, this data won't be as valuable. And perhaps data breaches won't happen with such regularity.

About the author

Donald Bush is the VP of marketing at Kount. He joined the company as director of marketing in October 2010. He attended Brigham Young University studying Business Administration and Marketing. Prior to joining Kount, Bush was the director of marketing at CradlePoint, a manufacturer of wireless routing solutions in the mobile broadband industry. He has worked in several management roles within the technology segment for over 20 years with both hardware/software manufacturers and as a partner in two technology marketing agencies. He has led product launches and marketing programmes for dozens of companies around the world such as Citi, HP, IBM, Kodak, Motorola and Weyerhaeuser and co-authored the seminar series, 'Common Launch Disasters and How to Avoid Them'.

References

1. '2015 Information Security Breaches Survey'. PwC/HM Government. Accessed Jun 2016. www.pwc.co.uk/services/audit-assurance/insights/2015-information-security-breaches-survey.html.
2. 'Fraud the Facts 2016'. Financial Fraud Action UK. Accessed Jun 2016. https://fraudfacts16.financialfraudaction.org.uk.
3. Garthwaite, Emily. 'Local authorities suffer over 4,000 data breaches in three years'. ITProPortal, 13 Aug 2015. Accessed Jun 2016. www.itproportal.com/2015/08/13/local-authorities-suffer-over-4000-data-breaches-three-years/.
4. Reynolds, Emily. 'Wetherspoon hack is four times bigger than TalkTalk'. Wired, 4 Dec 2015. Accessed Jun 2016. www.wired.co.uk/article/wetherspoons-cyber-attack.
5. Shah, Sooraj. 'All of UK's major banks and lenders have reported data breaches in the past two years'. Computing, 5 Jun 2016. Accessed Jun 2016. www.computing.co.uk/ctg/news/2411812/all-of-uk-s-major-banks-and-lenders-have-reported-data-breaches-in-the-last-two-years.
6. 'Year-end 2015 fraud update: Payment cards, remote banking and cheque'. Financial Fraud Action UK, Mar 2016. Accessed Jun 2016. www.financialfraudaction.org.uk/cms/assets/1/2015%20year%20end%20fraud%20update%20report.pdf.
7. 'Identity fraud and identity theft'. ActionFraud. Accessed Jun 2016. www.actionfraud.police.uk/fraud_protection/identity_fraud.
8. 'Mobile Payments and Fraud: 2016 Report'. Kount. Accessed Jun 2016. http://info.kount.com/mobile-payments-report-2016.
9. '2015 UK Phone Theft Statistics'. MissingPhones.org. Accessed Jun 2016. www.missingphones.org/content/2015-uk-phone-theft-statistics.

Securing small and medium-size businesses

Steve Mansfield-Devine

Steve Mansfield-Devine, editor, *Network Security*

It seems that barely a week goes by without the revelation that yet another large, high-profile organisation has been breached, with millions of records being stolen. It would be easy to imagine that hackers are attracted only by big-name firms with huge databases just begging to be ransacked. But as Colin Tankard, MD of Digital Pathways, points out in this interview, organisations of all sizes are at risk.

Information security can be a complex task, involving expensive solutions that require advanced skills to configure and administer. At least, that's the impression you can so easily form from even a casual encounter with the subject. Combined with the headline-grabbing stories, does this engender a belief among many small and medium-size enterprises (SMEs) that information security is something that only big firms need to worry about?

"I definitely have heard that question from some of the medium-size companies that we deal with frequently," says Tankard. "They think it is only big companies that need to have it. That it's only big companies that may face fines or prosecutions from the Data Commissioner or agencies like that."

This is surprising, he suggests, not just because of all the press coverage given to breaches these days, but also because the government agencies responsible for employment, growth and wealth have engaged extensively with this issue in recent years. "They all talk about the threats to organisations about loss of data, downtime and non-trading due to their systems being down," he says. "But it is definitely a fact that a high percentage of those companies we speak to don't think they're susceptible."

Colin Tankard, Digital Pathways: "A high percentage of those companies we speak to don't think they're susceptible."

Fear of fines

It's interesting that fines and prosecutions feature so prominently in this attitude. You would imagine that most companies would be concerned primarily about their intellectual property (IP) and ability to function. But it seems that many are more worried about the regulatory and legal repercussions.

This attitude may be due in some part to the arrival, finally, of the EU's General Data Protection Regulation (GDPR), says Tankard. Regardless of whether the UK goes through with its threatened exit from the EU, most firms – including small ones – will find themselves having to comply with the GDPR and the publicity given to this new regulation has been focusing minds on the ramifications of non-compliance. Yet even in the area of compliance, just a minority of SMEs seem to think it applies to them.

"Even if it's a smallish organisation that has some interesting development work or IP, they don't think anyone else would want that, they're too small for anyone else to worry about"

"To be honest, the large corporates that we deal with, they're very concerned about loss of reputation and that type of thing," says Tankard, "whereas the

smaller companies don't seem to even worry about that. It is a definite different mindset that we see outside of the large corporates."

It almost sounds as though SMEs have evolved from not worrying about being hacked to not worrying about being fined. So why is that?

"I think that a lot of it stems from organisations thinking that they have nothing of value, or nothing that somebody wants to have," says Tankard. "Even if it's a smallish organisation that has some interesting development work or IP, they don't think anyone else would want that, that they're too small for anyone else to worry about and I think that's where the complacency starts."

This is the same flawed thinking that leads individuals to think 'hackers wouldn't be interested in little me'. And there's a very important reason why SMEs are wrong to adopt this attitude, explains Tankard – and it's that hackers often target small firms as a way of getting to the bigger ones. A high percentage of SMEs have much bigger organisations as their customers. If attackers can break into the small company, they can then masquerade as the SME as a way of breaching the big firm. Or the SME may have direct connections, via interlinked networks such as ordering and billing systems, with the large organisation. The SME effectively becomes a springboard and is attractive to the attackers specifically because its security is weak.

"They don't think about the wider ramifications of their system being compromised in order to attack somebody else," says Tankard. He also explains that the 'springboard effect' can itself be complex. The breached SME might not have major firms as customers, so the attackers use its systems to breach the next SME with weak security. And so it goes on, with the hackers moving from one small firm to the next until they find a way into a big company. "Ultimately the target might be 10 or 20 hops down the line," he says. Exploiting SMEs as proxies in this way helps to hide the source of the attack on the large organisation.

This is not to minimise the importance of direct attacks on SMEs. Too many of them underestimate the value to attackers of the information they possess, reckons Tankard. And while some SMEs do find that their bank accounts have been raided or their systems vandalised, "generally it is the information that that company has, or the contacts that it has, that attackers are going for and that's really hard to get across to some of these organisations."

Untargeted attacks

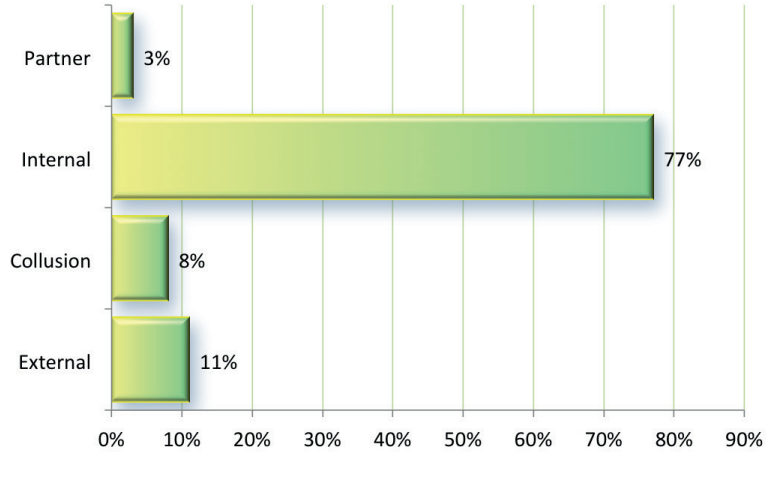
Of course, not all attacks are targeted, nor do all threats originate from outside the organisation. Random, mass attacks such as phishing and ransomware can easily lead to downtime, disruption and serious costs stemming from lost business and remediation. And even where hacking is involved, it may be that the hacker has found your organisation by chance, rather than by design. You get hacked purely because your security is weak and because the attackers don't care what information or resources you have – they may, for example, just need a place to set up a botnet command and control server. Often, they find you with a simple Google search, using so-called 'Google dorks'.[1]

And then there are your own staff. "We've seen a lot of that recently," says Tankard, "where the insider threat is really the biggest thing, because the smaller organisations tend to not have so many controls. We often hear a director or an owner of the company say 'I trust my staff'."

"They seem to expect that their employees understand those risks and they expect them to know not to click on things, whereas in the larger organisations they're very conscious of education"

The evidence suggests they shouldn't. Tankard points to the Verizon 'Data Breach Investigations Report' which shows that 77% of breaches were due to an insider and a further 8% were a result of collusion between insiders and outsiders.[2]

A majority of these insider-sourced breaches were, explains Tankard, "just employees making silly mistakes, clicking on a link they shouldn't have clicked on, doing something that, in hindsight, is wrong." But, he adds: "Small organisations don't tend to put the controls in place to pick those up and they also seem to fall behind on the education. They seem to expect that their employees understand those risks and they expect them to know not to click on things, whereas in the larger organisations they're very conscious of education and they're very conscious of training their staff and putting systems in place that educate or stop the accidental clicking of a link or the accidental sending out of information that shouldn't go out. But the smaller companies, they don't think that there's the risk and they think all of their staff are trustworthy and will never make any mistakes."



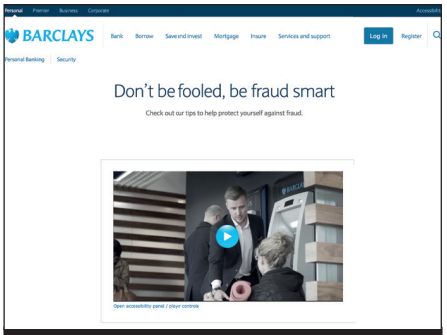
Actors involved in data breaches. Source: Verizon.

The cost factor

Underlying many of these attitudes is a reluctance to embrace security because of the perceived costs. Typically, security is seen as a pure cost – effectively, money down the drain if nothing bad happens. And it's also assumed that installing security will be expensive – in terms of kit and the skills needed to use it. Even with those SMEs that think about security, these perceptions often lead to inadequate work-arounds.

"If they are thinking about security they'll go to Mr Google and they will find products on Google that are free," says Tankard. "And so quite often we will come across organisations that are using something that they think is good, but we know that there are vulnerabilities, or the encryption level is very, very low because the person who downloaded it was just looking for encryption and didn't know anything about levels of encryption or the complexities of that.

"The other area tends to be that it's scary," he adds. "They don't understand what they're looking at. If they have a mainstream security product which, on the face of it, is a good thing, they don't really know how to set it up or run it. Quite often we will find that everything is set as default, which maybe isn't the best way. Or, frequently, we find that the system has been installed by a friend, or someone they know, or a third-party vendor which maybe has nothing to do with data security – maybe they look after their phone system."

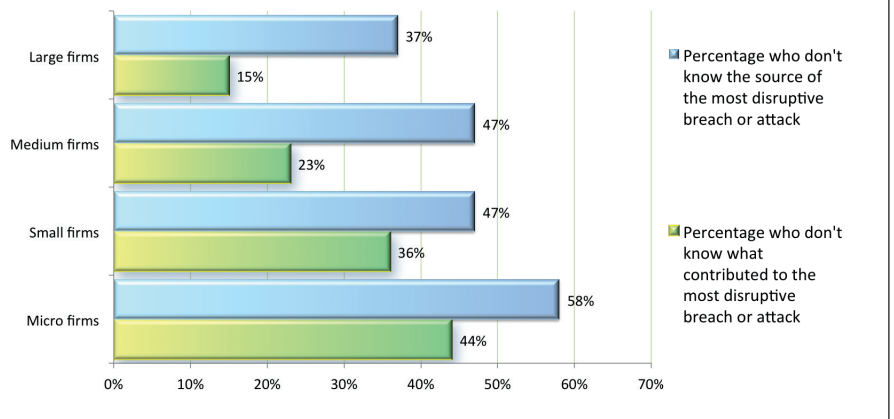


Online security advisories, such as this one from Barclays Bank, could be used for educating staff.

"The cost to recover from the breach is going to be more than putting in, right at the beginning, a good piece of equipment or some good monitoring tools, or even just investing in some education of their users"

When organisations get hit with a breach and reach out for some professional help, quite often they'll say: 'We've run a scan and we didn't find any viruses or rogue software'. It has to be pointed out to them that the software they thought was protecting them clearly isn't going to pick up malware in a post-exploit scan when it had failed to intercept it during normal use.

"It's little things like that," says Tankard. "You start to realise that the education level in organisations is quite low. That compounds the problem. It's costing them a lot more money. Probably the cost to recover from the breach is going to be more than putting in, right at the beginning, a good piece of equipment or some good monitoring tools, or even just investing in some education for their users. There's a lot of free education out there. Barclays Bank, for example, has some very good online videos talking about phishing emails – you could just give all your employees that link and say, go look at that and use it as a tool to educate."



Businesses' understanding of the factors and sources behind their most disruptive breaches of the past year. Source: 'Cyber Security Breaches Survey 2016', HM Government.

Perceived costs

So is there an incorrect perception about the cost of implementing security properly?

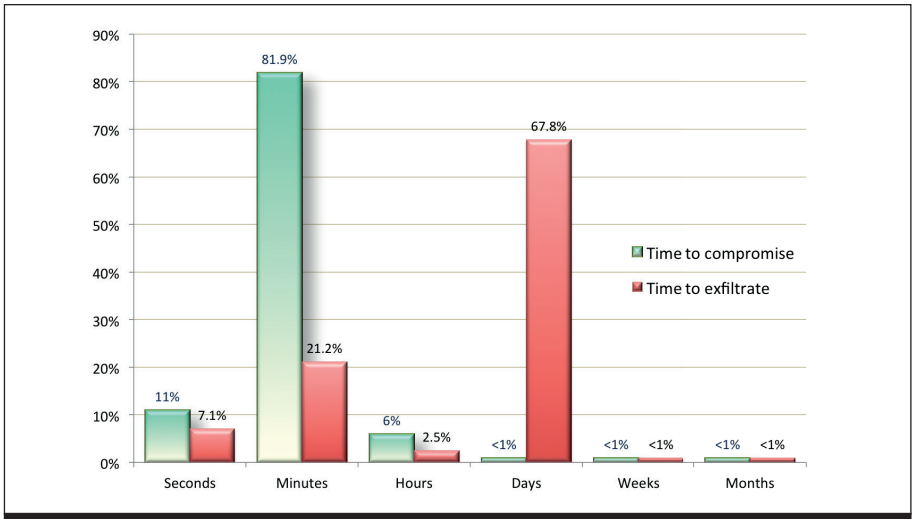
"Yes, I definitely think so," says Tankard. "We've just recently been working with some organisations that have suffered ransomware attacks. Their original thought process was, 'well if we had a bad attack, it's bad, obviously, but we would shut down all our systems, we would wipe everything and we would then restore from the previous night's back-up. So a worse case is, we've lost, say, 24 hours of data'. But they clearly forget that the ransomware was already in there at least 24 hours ago."

Firms are often shocked to learn how little time it takes to hack into a system and how long the attackers can loiter before they are discovered.

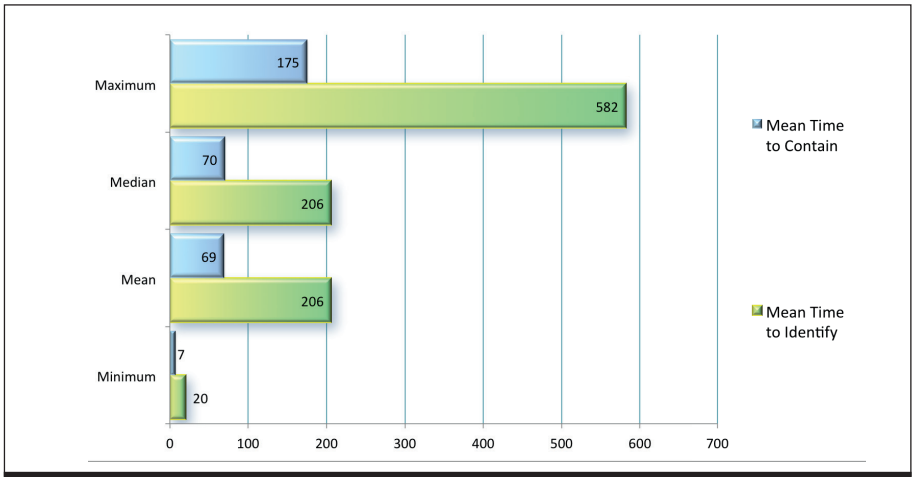
"It takes us generally three to four minutes to hack a system," explains Tankard, "but it's normally about eight months to detect". From the hacker's perspective, he adds: "In those eight months, I've been rummaging around your system, I've been inviting my friends into your system, we've been having a great party in your system. So taking your statement, that you'll just roll back 24 hours, I could have been in your system a month, two months or eight months. Have you got an eight month old back-up that you possibly could put in?"

The vast majority of medium-size firms would not be able to cope with this situation. And even if they did have an eight month-old back-up, losing that amount of invoices, billing data and other crucial business information would kill the company.

"It's only when you start talking in those terms that many of these companies start to think about it," says



Time required to compromise systems and exfiltrate data. Source: '2016 Data Breach Investigations Report 2016', Verizon.



Mean time to identify and contain data breach incidents, in days. Source: '2015 Cost of a Data Breach', IBM/Ponemon Institute.

Tankard, "and then the cost of putting in some systems, the cost of managing and monitoring your systems a little bit more effectively, is quite low compared to that complete loss of a business."

Skills shortage

It's not difficult, then, to make the case for implementing security measures. But many SMEs are still going to be concerned about the issue of skills. People with information security skills are in short supply and difficult to hold onto. Tankard admits that even specialist security firms like his struggle to find security engineers. And developing these skills in-house is going to be impossible for SMEs – they simply don't have the funds and resources to do it. But maybe they don't need to. A reasonable baseline of security is achievable through automation, Tankard argues.

"What you find is that the users educate themselves – it doesn't really take much management because once it's set up it's there and it's running"

"For many of the small to medium companies, that are stretched with technical resources, they can use tools that make that easier," he explains. "Things like log management, just a system that manages the logs for you and once a week puts them into a report that is understandable for virtually any manager – if it's all green it's good, if it's red we've got a problem."

With a little initial effort, you can also install monitoring software that will monitor what the users are doing and spot any unusual behaviour. "If somebody's clicking to move something to Dropbox and that's not in the company profile, the system will pop a little window up to the user and just say to them, are you aware that that is in breach of the company policy and you shouldn't do that? And what you find is that the users educate themselves – it doesn't really take much management because once it's set up, it's there and it's running."

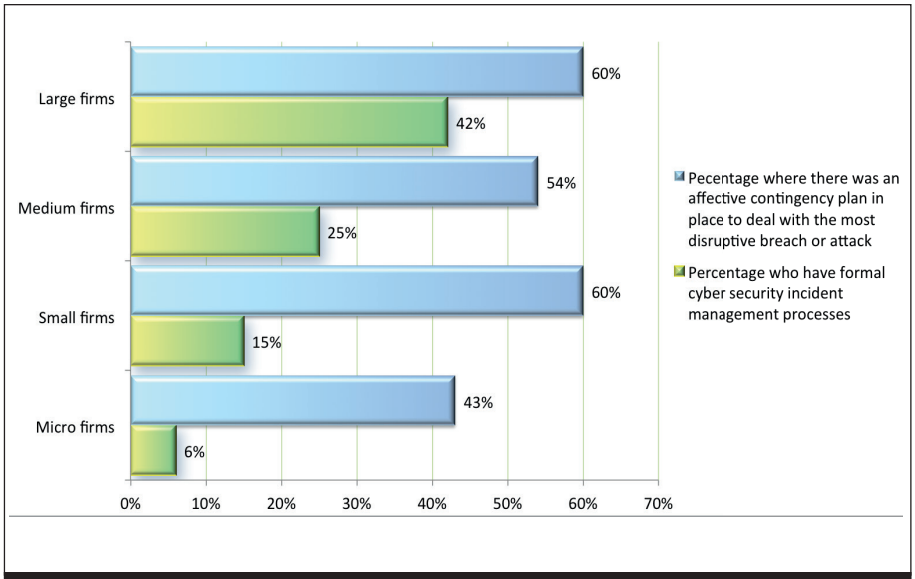
Tankard likens the challenge of finding dangerous activity – such as someone clicking on a link or copying a file that they shouldn't – to finding the needle in a haystack. In any organisation, even a small one, there is constant activity and 'noise'. Automated systems can filter out innocuous activity, effectively reducing the size of the haystack. And the use of things like automated messages warning staff that the action they're about to perform is contrary to company policies helps to raise the awareness level – educating users 'on the job', as it were.

"Return on investment with security is always a tough one. It's an easy one if you have been hit because you know the costs and the ramifications: but if you haven't been hit, you don't really think about it"

"They probably won't do it again," says Tankard. "They learn and so the haystack gets lower and lower, the noise level goes down. It makes the management of the real incidents, the real problems, that much easier, because they're easily identifiable."

The management comes in for some education too. The reporting tools in such monitoring systems can offer some real insights into what's going on in your systems.

"It will show you your top five dangerous resources – as in employees – and you can then target those particular people," says Tankard. "It just makes the whole thing easier and not such a big task and I think that's where we need to get to, to get that education over to those organisations that there are tools and it's not a huge problem. It just takes a little bit of setting up – you need some time



Whether businesses have incident management processes and contingency plans. Source: 'Cyber Security Breaches Survey 2016', HM Government.

to define your policies and craft how you want to handle certain events, but once you've done it, it's done."

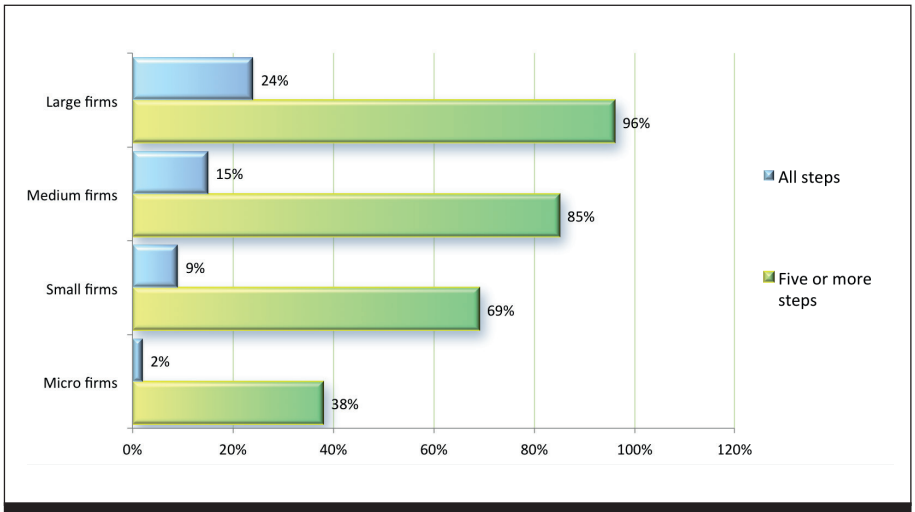
"If you have been hit you know the costs and the ramifications; but if you haven't been hit, you don't really think about it"

A modest up-front spend could save your business, or at least save it considerable clean-up costs and lost business. That would seem a simple business case for security, but it's not an easy one to get across.

"Return on investment with security is always a tough one," says Tankard. "It's an easy one if you have been hit because you know the costs and the ramifications; but if you haven't been hit, you don't really think about it."

There are plenty of reports that spell out the cost of a data breach – not least the Ponemon Institute's annual report.[4] However, these tend to focus on big companies and measure the cost of breaches in millions of dollars. SMEs find it difficult to relate to such reports and this may reinforce the idea that it's only large enterprises that are afflicted with such problems.

"I think if there were more stories in the press about businesses going down because of their systems being compromised, or because they couldn't bill because of no access to the Internet, that would probably register much more with SMEs," says Tankard. "And that's something we've been talking about with the Federation of Small Businesses, just to try and use that as another way of educating."



The percentage of UK companies that have undertaken the Government's 10 Steps programme. Source: 'Cyber Security Breaches Survey 2016', HM Government.

Compliance and security

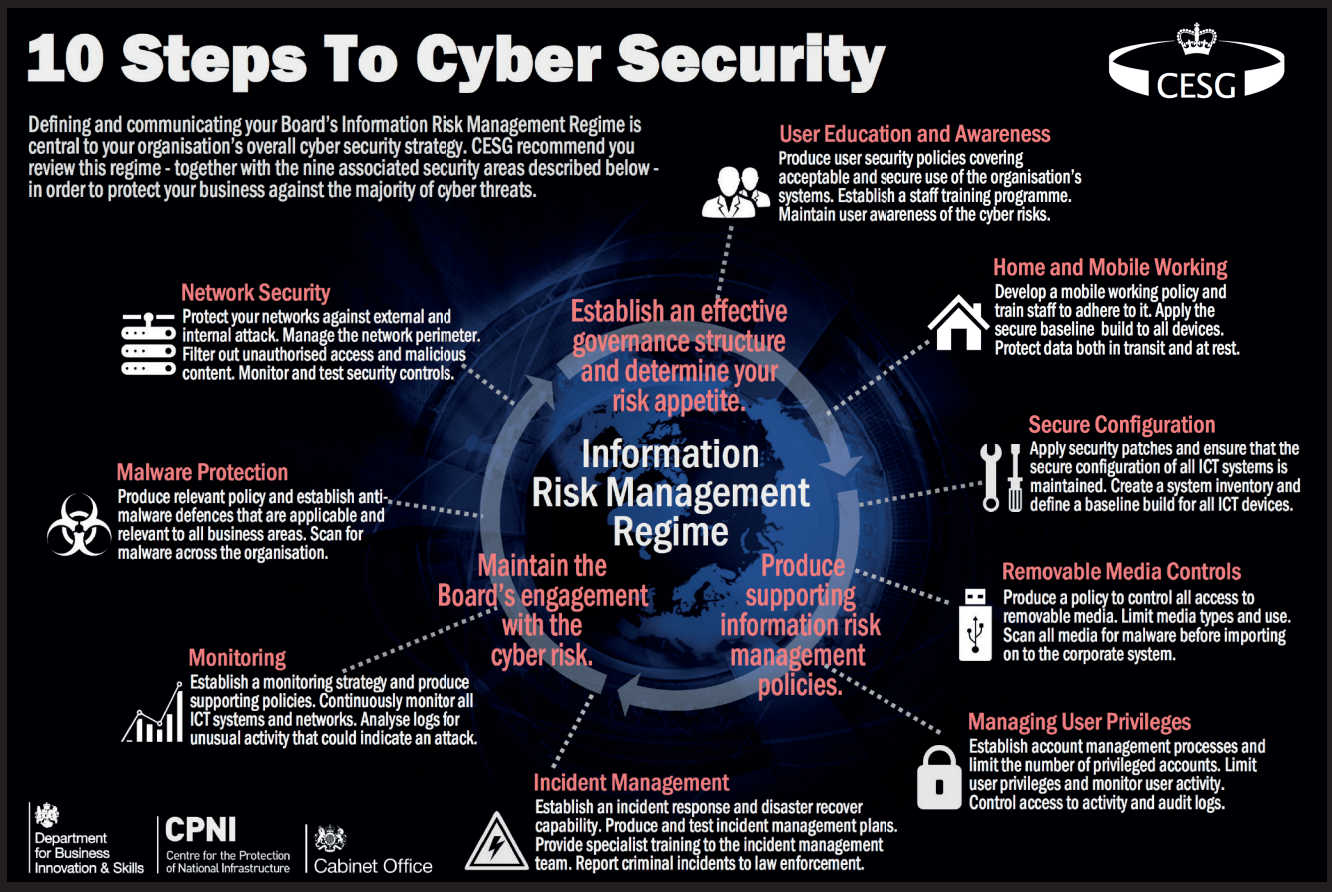
We've already touched on the GDPR. Just like their larger counterparts, SMEs are becoming increasingly subject to regulation. And while regulatory compliance and security are not the same thing, there's often a significant degree of overlap. So is there a way that smaller firms can roll up their compliance obligations and their security needs into one big bundle and attack both issues at the same time – with the help of third parties – and reap some business benefits into the bargain?

"Organisations would look at your financial statements and your financial records and look at how competent you are – accreditations and suchlike – and cyber is coming in there as well"

"Oh definitely," says Tankard. "What we see happening a lot now is, if you're tendering to public sector organisations, or some larger organisations, they look for your security compliance position. So do you have Cyber Essentials, for example? Do you have cyber insurance to protect you? And those are things that will enable you to go and get more business. But it will also help you to protect your own business, because if you follow Cyber Essentials recommendations, you're going to be in a much stronger position to protect yourself."

In fact, being seen to be compliant and to have at least a basic level of security isn't just a selling point, he says. SMEs are going to come under increasing pressure from their customers, as well as the regulators, to get their act together when it comes to security.

"We've seen it a few times ourselves now, where we've been tendering for different pieces of business," says Tankard. "Organisations would look at your financial statements and your financial records and look at how competent you are –



The UK Government's '10 Steps to Cyber Security'.

accreditations and suchlike – and cyber is coming in there as well. And particularly if you are an organisation that works on a company site – or perhaps you have some of their information on your site, because you're doing some analytical work on their data – that's all becoming quite mandatory. And the cyber insurance area is something we're starting to see coming up much more. The issue there is that although you can take out cyber insurance, you then have to prove that you've got the measures and processes in place to meet the criteria for having the insurance, otherwise it wouldn't pay out. That's an interesting point that people need to look at, because we're finding that, certainly in the public sector now, most of the tenders are stipulating that you have cyber insurance – and it's not just normal company insurance, it is all about your infrastructure and how you protect third-party information that you might be storing."

Government assistance

It's not just third-party specialists that can help. In 2012, partly in reaction to a number of high-profile breaches, the UK Government issued its '10 Steps to Cyber Security' guidance.[5] The aim was to raise awareness, particularly among SMEs, that cyber-security is something everyone needs to be concerned about. The scheme lays out the key capabilities that organisations need to have, such as anti-malware, system monitoring and so on. The guidelines act like a basic 'to do' list of security requirements.

The '10 Steps' were seen as a reasonable start. But it was still up to individual organisations to take the advice on board and there was no way of telling, from the outside, if they had done anything effective with regard to the requirements laid out in the scheme. In fact, the overall opinion is that, a couple of years after the

'10 Steps' were launched, nothing much had changed.

So the Government then went a step further and introduced the Cyber Essentials scheme, already mentioned by Tankard.[6] With the assistance of a number of approved and accredited security organisations and managed by CESG, the data assurance arm of the government signals intelligence agency GCHQ, Cyber Essentials not only helps organisations become secure, but also provides two levels of (optional) certification that they can use in tendering for business.

Cyber Essentials focuses on five mitigation strategies based around:

- Boundary firewalls and Internet gateways.
- Secure configuration.
- Access control.
- Malware protection.
- Patch management

The basic Cyber Essentials certification is achieved through self-assessment. And the Cyber Essentials+ level is gained after tests carried out by an external, CREST-certified organisation – typically a penetration testing company. So what does Tankard feel about the scheme?

"I think it's a good stepping stone," he says. "It's a great starting point for companies and it's not an onerous task to apply for it."

"As you know, security is such a huge topic, but not everyone needs to cover every single aspect of it. There are some key points and that's how Cyber Essentials helps you. It gives you that focus"

Although certification under the scheme is becoming mandatory in a few instances – for example, some local authorities demand it in the case of companies providing certain IT-related services – not enough firms have applied, in Tankard's view.

"It is still quite a rare thing but it's gathering a lot more momentum," he says. "On the continent, we see organisations jumping straight to [ISO security certification] 27001 and maybe not doing some of these intermediary steps. But if you haven't got anything in the way of certification, I think it's a great starting point and I encourage every company we deal with to go do it. Start off having just a gap analysis to understand the Cyber Essentials criteria."

If SMEs take the trouble to analyse their systems and processes and map these against the Cyber Essentials criteria, they'll probably find they're already half-way towards certification, Tankard reckons – "most of it is good practice," he says. Firms can then focus on some of the more technical areas where they have weaknesses.

"It gives them a starting point and a framework to work to, rather than just sitting there and saying, 'well what do I need to do?'," he says. "As you know, security is such a huge topic, but not everyone needs to cover every single aspect of it. There are some key points and that's how Cyber Essentials helps you. It gives you that focus."

About the author

Steve Mansfield-Devine is a freelance journalist specialising in information security. He is the editor of Network Security and its sister publication Computer Fraud & Security. He also blogs and podcasts on infosecurity issues at Contrarisk.com.

References

1. 'Google Hacking Database (GHDB)'. Exploit Database. Accessed Jun 2016. www.exploit-db.com/google-hacking-database/.
2. '2016 Data Breach Investigations Report'. Verizon. Accessed Jun 2016. www.verizonenterprise.com/verizon-insights-lab/dbir/2016/.
3. 'Security'. Barclays Bank. Accessed Jun 2016. www.barclays.co.uk/Helpsupport/Security/P1242557966927.
4. 'Cost of a Data Breach Study. Ponemon Institute/IBM, 2016. Accessed Jun 2016. http://www-03.ibm.com/security/data-breach/.
5. '10 Steps to Cyber Security'. CESG/HM Government. Accessed Jun 2016. www.cesg.gov.uk/10-steps-cyber-security.
6. 'Cyber Essentials'. CREST. Accessed Jun 2016. www.cyberessentials.org/index.html.

EVENTS

30 July–4 August 2016
Black Hat USA
Las Vegas, US
www.blackhat.com

4–7 August 2016
DefCon
Las Vegas, US
www.defcon.org

10–12 August 2016
25th USENIX Security Symposium
Austin, TX, US
www.usenix.org/conference/usenixsecurity16

31 August–2 September 2016
ARES–International Conference on Availability, Reliability and Security
Salzburg, Austria
www.ares-conference.eu/conference/

6–7 September 2016
CyberTech Singapore
Singapore
http://cybertechsingapore.com/

7–9 September 2016
International Cyber Security & Intelligence Conference
Ontario, Canada
https://icsic.ocmtontario.ca/

14–16 September 2016
44Con
London, UK
www.44con.com

19–20 September 2016
Information Security Network
Reading, UK
https://thenetwork-group.com/information-security-network/

21 September 2016
New York Cyber Security Summit
New York, USA
http://cybersummitusa.com/new-york-2016/