INDEPENDENT PUBLICATION BY

RACONTEUR

raconteur.net | #0418 | 27 / 11 / 2016

CYBER SECURITY

Organised cyber criminals are digital mafia

In the wake of the Tesco Bank hack, which saw 9,000 customer accounts targeted, cyber security experts are warning of organised online crime gangs operating like a digital mafia

OVERVIEW
STEPHEN ARMSTRONG

Mr Robot is possibly Hollywood's ultimate hacker show – the chaotically unfolding story of Elliot Alderson, a cyber security engineer with emotional problems, who is recruited by a fiendishly cunning group of hacktivists in their attempt to bring down the fictitious financial giant E Corp.

Elliot wears a hoodie and hacks from his bedroom, just like all good movie or TV hackers do. For Mikko Hypponen, chief research officer at the cyber security firm F-Secure, this image is quaint and entirely false. Mr Hypponen looks at 350,000 samples of new malware attacks almost every single day. Some 95 per cent of them are from organised online crime syndicates. Only the tiniest proportion of hacks is committed by hacktivists.

"The earliest viruses were written by bored teenagers looking for a challenge, but today's hackers are much more malicious," he explains. "What makes them different from old-school hackers is they have a motive."

> "This new breed of cyber criminals see themselves as digital mafiosos

This new breed of cyber criminals see themselves as digital mafiosos. The Moldovan hackers behind the Dridex malware attack stole millions of dollars in co-ordinated hits on 300 banks around the world. Evgeniy Mikhailovich Bogachev, the Russian thought to be the author of the Zeus trojan, has a $3-million bounty on his head from the FBI, and is wanted by Interpol and Europol.

That's not to say naughty teenagers aren't a threat, says Troy Hunt of data breach aggregation service Have I Been Pwned? "There are teenagers getting hold of vast amounts of personal data, using freely available software, as in the recent TalkTalk hack," he points out. "Scotland Yard told the press it was a Russia-based Islamic jihadist group, but it turned out to be two teenagers."

Either way you lose, says Adrian Nish, who leads the Threat Intelligence team in BAE System's cyber-defence division. Real-life hackers are as good as or even better than movies suggest. A few months ago, Mr Nish explains, hackers targeted the Central Bank of Bangladesh and tried to steal $951 million, six times the amount in George Clooney's *Ocean's Eleven*.

"They set up bank accounts in Manila in the Philippines and in Sri Lanka then broke into the Bangladesh bank network, probably sometime in 2015, and waited until February 4," he explains. "This was a Thursday, the end of the week in Bangladesh and just before the Chinese New Year, so overall they had this four-day window to get away with the heist. They flipped just eight bits of code, secured root access and covered up the transactions to make it look like the money hadn't left the bank's accounts at all."

Of 35 attempted transactions, only four got through – meaning the hackers stole $81 million rather than $951 million – but it's still one of the biggest bank robberies in history. "Banks don't do enough testing," Mr Nish warns. "We're dealing with people who've been trained to make network intrusions, so the people we have defending our system also need training, also need to know how to spot these types of attacks and how to set up the system security in order to defend against it."

In TV drama, people are a big weak point that hackers take advantage of. In *Sherlock*, for instance, Moriarty pretends to hack the Bank of England, the Tower of London and Pentonville Prison before – spoiler alert – revealing it was the human factor all along – disgruntled employees, with no super technology needed. And the human factor is definitely key in online security.

"The most sophisticated attacks of recent years had people on the inside," says Sadie Creese, professor of cyber security at the University of Oxford. "That's people who work for us, people that are members of our family, our small groups, employees on the books, our business partners, anyone with valid access to some part of our system.

"We all carry sophisticated technology like smartphones around with us and we all work or use the cloud. So now hackers no longer have to hack 20 or 50 organisations. They hack one cloud and they get every single person who is using that cloud."

Working the people factor is commonplace. "You've got to work on five or six different attack factors at any one given time," says white hat hacker Jamie Woodruff from Metrix Cloud. "My favourite is the viewing webcams on Google. You can locate a specific area, find open cameras and build up a profile about who walks into that infrastructure and who walks out. People follow routine. You see them repeat, you build up a pattern then use tools like Montego, where you can type in key identifiable information then find your eBay account, your e-mail account, your address, your telephone number... then you're in."

Among the tricks Mr Woodruff has pulled there's setting up fake .eu versions of company sites and asking employees to log in, tailgating into an office with a group of smokers then walking around dropping tainted USBs and sticking up official looking QR codes at business conferences which infect smartphones with malware.

And movies rarely show one of the fastest-growing forms of cyber attack – ransomware, where a hacker locks down all the files on anything from a laptop to an entire company or steals extensive information and demands money to release or return everything.

Moty Cristal, professional negotiator and chief executive of NEST Negotiation Strategies, recalls one banking client receiving an e-mail stuffed with very confidential customer information. Two minutes later, he received a WhatsApp message demanding $120,000.

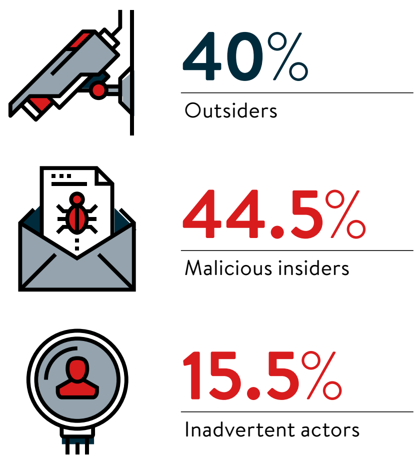
Mr Cristal adds: "When you're facing this crisis, it is the human factor that needs to be managed. Making connections and negotiating are essential."

Although, to be fair, *The Negotiator* is a whole different movie. Looks like hackers can get into almost everything.

Share this article online via **raconteur.net**

WHO ARE THE CYBER ATTACKERS?

Based on data IBM collected in 2015 from more than 8,000 client devices in 100 countries

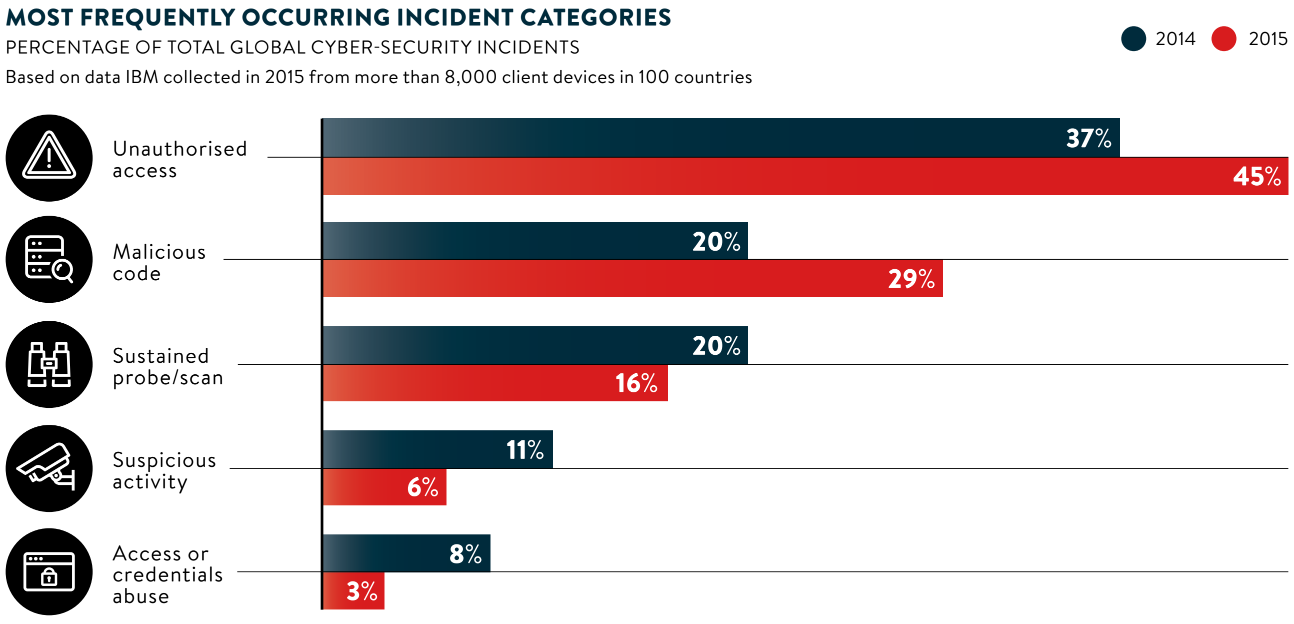


Source: IBM Security Services 2016

MOST FREQUENTLY OCCURRING INCIDENT CATEGORIES

PERCENTAGE OF TOTAL GLOBAL CYBER-SECURITY INCIDENTS

Based on data IBM collected in 2015 from more than 8,000 client devices in 100 countries



Source: IBM Security Services 2016

DISTRIBUTED IN THE SUNDAY TIMES

RACONTEUR

PUBLISHING MANAGER
John Okell

PRODUCTION EDITOR
Benjamin Chiou

MANAGING EDITOR
Peter Archer

HEAD OF PRODUCTION
Natalia Rosek

DIGITAL CONTENT MANAGER
Jessica McGreal

DESIGN
Samuele Motta
Grant Chapman
Kellie Jerrard

CONTRIBUTORS

STEPHEN ARMSTRONG
Contributor to *The Sunday Times, Monocle, Wallpaper** and *GQ*, he is also an occasional broadcaster on BBC Radio.

JOHN LEYDEN
Former crime reporter in Manchester, he is now a writer for the technology news and opinion website *The Register*.

DAN MATTHEWS
Journalist and author of *The New Rules of Business*, he writes for newspapers, magazines and websites on a range of issues.

EDWIN SMITH
Writer and editor, he contributes to publications including *The Guardian* and *The Sunday Telegraph*.

FINBARR TOESLAND
Freelance journalist, he specialises in technology, business and economic issues, and contributes to a wide range of publications.

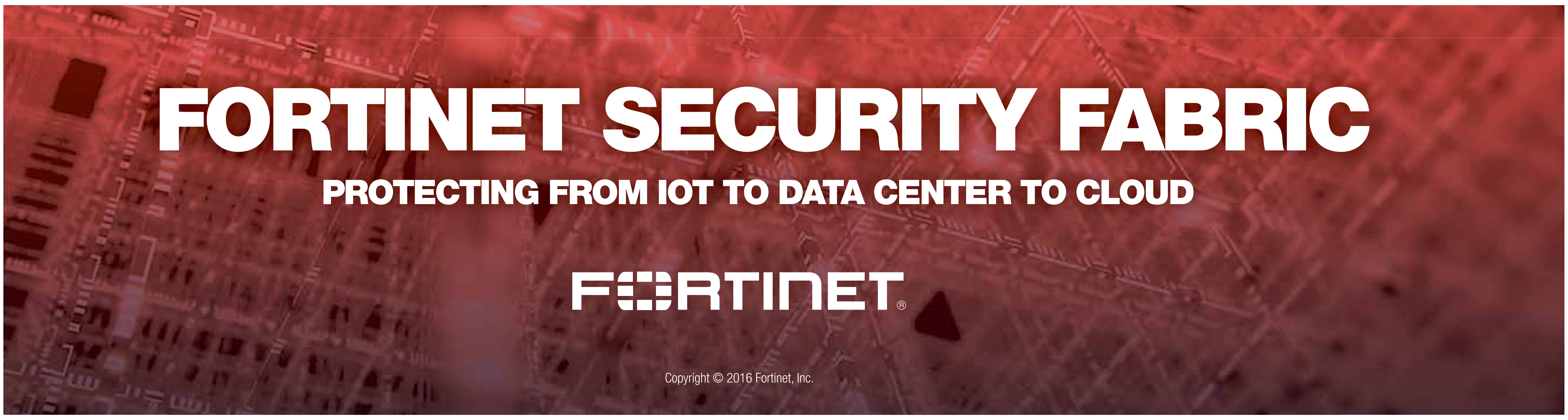
DAVEY WINDER
Award-winning journalist and author, he specialises in information security, contributing to *Infosecurity* magazine.

EMMA WOOLLACOTT
Specialist technology writer, she covers legal and regulatory issues, contributing to *Forbes* and the *New Statesman*.

Although this publication is funded through advertising and sponsorship, all editorial is without bias and sponsored features are clearly labelled. For an upcoming schedule, partnership inquiries or feedback, please call +44 (0)20 8616 7400 or e-mail info@raconteur.net

Raconteur is a leading publisher of special-interest content and research. Its publications and articles cover a wide range of topics, including business, finance, sustainability, healthcare, lifestyle and technology. Raconteur special reports are published exclusively in *The Times* and *The Sunday Times* as well as online at raconteur.net

The information contained in this publication has been obtained from sources the Proprietors believe to be correct. However, no legal liability can be accepted for any errors. No part of this publication may be reproduced without the prior consent of the Publisher. © Raconteur Media


FORTINET SECURITY FABRIC
PROTECTING FROM IOT TO DATA CENTER TO CLOUD
FORTINET
Copyright © 2016 Fortinet, Inc.

COMMERCIAL FEATURE

jamesteohart/istockphoto

SECURITY RISK OF THINGS

The internet of things is connecting devices to networks on an ever-increasing scale. Everything from industrial controls to smart cars and even baby monitors are now connected to the internet, raising major security concerns

FORTINET®

The internet of things (IoT) has opened up new markets and business opportunities worldwide, but it has also brought with it an array of new and significant security threats.

"With the increasing deployment of IoT devices, by both the consumer and enterprise, the cyber criminal now has a much broader attack surface to take advantage of. This growing attack surface means that these networks are now more vulnerable than ever before," says Derek Manky, global security strategist at Fortinet.

> These solutions must work together to form a cohesive fabric, spanning the entire network, linking different security sensors and tools together to collect, co-ordinate and respond to any potential threat

Derek Manky, global security strategist, Fortinet

PERFECT STORM

According to the latest forecasts, there will soon be tens of billions of connected devices in use worldwide, many of which are owned by businesses. The significance of this trend needs to be taken more seriously than is currently the case, says Mr Manky, who explains that most businesses are simply not properly protected against the threat of IoT security risks.

He is convinced that enterprises are generally less well protected against IoT-based threats than they believe they are, with Fortinet's FortiGuard Labs estimating that some 500,000 hacking attempts are now being made every minute around the world.

"We speak to many vulnerable enterprises that are unaware of compromised or infected devices attached to their systems increasing the risk of a successful cyber attack and data breach," he says.

Mr Manky makes clear that the number of new vulnerabilities being spotted continues to increase, as does the number of attacks being initiated on a global basis and the scope of settings in which hackers can have an impact.

"I've been with Fortinet for more than 12 years. In 2004, we recorded half a million viruses for the entire year. Today, we can record over two million new viruses in a single day and we monitor more than 50 billion potential threat events worldwide daily," he says.

But without the means to assess the risks associated with having so many connected devices or the expertise to understand the exact nature of the threats being faced, what can businesses do to protect their networks?

Mr Manky points out that not every business can have a security analyst looking out for potential IoT vulnerabilities or problems in real time. From Fortinet's perspective, the answer jointly lies with developments in artificial intelligence, and the need for integration between the network and its security infrastructure.

CO-OPERATIVE SECURITY

"We are also moving towards the creation of systems that defend against cyber attacks through an approach based on a combination of artificial intelligence and human input," Mr Manky says.

"We're already able to quarantine devices and view networks like a grid to spot potential problems automatically through 'co-operative security' and digital asset mapping.

"But without bringing in artificial intelligence processes there isn't enough scope for these systems to scale in order to meet the needs of both small and medium-sized enterprises (SMEs) and larger businesses that don't have an IoT security analyst on site."

However, the first step in the process must be to ensure the underlying network has the fundamental security technologies in place to support IoT. Randomly or haphazardly implemented security will only complicate the task of securing the network when IoT is implemented.

"Fortinet's technology vision, the Fortinet Security Fabric, lays out the blueprint for integrating the necessary technologies needed to meet these and other security challenges of today and in the future. Simply deploying security end-to-end is not enough," says Mr Manky.

"These solutions must work together to form a cohesive fabric, spanning the entire network, linking different security sensors and tools together to collect, co-ordinate and respond to any potential threat."

REAL-WORLD ISSUES

Mr Manky also explains that the lines between the cyber and physical realms are blurring because of the growth of IoT.

One market segment where the consequences of improperly implemented IoT are particularly relevant is healthcare, when the potential consequences of a successful hack can quickly become life threatening. Much the same can also be said in the context of connected vehicles and all manner of public services.

Mr Manky's view is that enterprises ought to be focused on developing more robust strategies for protecting against threats associated with IoT and connected devices, and work with companies that can provide security services to assist them.

> We can record over two million new viruses in a single day and we monitor more than 50 billion potential threat events worldwide daily

SKILLS GAPS

He also identifies the looming skills gaps as a significant challenge for enterprise security, with the growth of IoT only likely to bring the issue of a diminishing pool of qualified professionals into sharper focus in the coming years.

"Part of the challenge is the type of IT security jobs that are being created worldwide continues to change significantly as a result of developments like IoT and big data," he says.

The growth of IoT is a scenario in which security vulnerabilities and risks to enterprise IT systems continue to proliferate. Indeed, what's going on already is having a massive impact as far as the growth of new vulnerabilities and the relative lack of readiness to defend against them is concerned, he says.

As the threat landscape intensifies, only larger organisations will be able to establish relevant experts and security analysts in-house. For the rest of the market, and in particular SMEs, they simply won't be able to afford it.

However, they can turn to the products and solutions that security experts such as Fortinet provide, as well as managed security services based on these solutions, to equip themselves properly in the fast-changing cyber-security battleground.

For more information please visit www.fortinetsecurityfabric.com

NUMBERS FROM FORTINET'S FORTIGUARD

310k botnet C&C attempts thwarted per minute	545k network intrusion attempts resisted per minute
100 intrusion prevention rules per week	416k hours of threat research globally per year
140k malware programs neutralised per minute	312 zero-day threats discovered
170k malicious website accesses blocked per minute	290tb of threat samples

Source: Fortinet

Ethan Miller/Getty Images

The fallout of Yahoo!'s data breach is a major concern for chief executive Marissa Mayer, who is currently working to finalise a $4.8-billion deal to sell Yahoo!'s core internet business to Verizon

Be ready to limit damage after a data breach...

Cyber attacks are on the rise and may even be inevitable, so organisations must create a culture of cyber awareness and be prepared to protect their reputation

CYBER-AWARE CULTURE
EMMA WOOLLACOTT

The costs of a data breach can be high, with *Forbes* calculating that cyber attacks are costing businesses around the world up to $500 billion a year.

And the hacks are likely to become even more expensive when new legislation comes into force in 2018. Under the European Commission's General Data Protection Regulation (GDPR), companies that are hacked because of inadequate security measures will be liable to fines of an eye-popping €20 million or 4 per cent of annual worldwide turnover, whichever is greater.

However, the costs of a data breach don't end there. Research has shown that an incident can seriously damage a company's reputation and in cases such as Yahoo!'s high-profile hack, for example, this can have serious implications of its own.

A report from security firm FireEye reveals that around a third of people feel less loyal to a company that's experienced a breach and six in ten say they would leave an organisation if their details were used by criminals.

Similarly, a poll by the Information Commissioner's Office has found that a fifth of people would definitely stop using a company's services after hearing news of a data breach. The stakes, in other words, are high.

However, a surprising number of organisations fail to have a plan in place when it comes to communicating a cyber breach to the public and some get it badly wrong.

There's particular mistrust, for example, when companies take too long to reveal a breach, particularly when, as so often, news of the breach is leaked.

"If you cover up, there's a danger that the breach will be detected by other means, for example a pattern of bank fraud," says Piers Wilson, head of product management at Huntsman Security. "And, like Yahoo!, where you've had a breach and not disclosed it, when it's revealed there's more embarrassment and loss of face."

Under the planned GDPR legislation, organisations will be required to notify the authorities within 72 hours of an event. But while this means that really long delays will effectively become impossible, companies won't necessarily be forced to alert customers immediately. And it's often not a good idea to go public too soon, as this can jeopardise the clean-up operation.

"A lot of companies think they need to let employees know first. They think they're being transparent, but if one of the employees leaks the information, that could hurt remediation," says Vitor Souza, vice president of global communications for FireEye.

"One company needed to do a password reset over the weekend. Two days prior, the company e-mailed all employees to tell them. One person was not happy at work and remediation failed because the attackers were tipped off. They got out of the network, so the team couldn't complete remediation."

Disclosing too soon can also make a problem seem much more significant than it ultimately turns out to be. When one large company in Japan was breached, for example, cultural reasons meant it was eager to go public with the news.

"The issue was that they didn't have any plan, so it was the communications team taking the lead," says Mr Souza. "The board goes on TV to apologise and says potentially nine million records were stolen. But it turned out that what actually took place was an intrusion not a breach, so in fact no data was taken."

As all these examples show, cyber security is an issue that needs to be at the heart of decision-making so the C-suite isn't caught on the hop. Too often chief security officers complain the board lacks awareness of cyber security, with FireEye's survey indicating nearly eight in ten want to see changes to boardroom structure that would give it more prominence.

RESCIND

1/3 of people feel less loyal to a company that has experienced a breach

6/10 would leave an organisation if their details were used by criminals

Source: FireEye

Research from PwC revealed that only 28 per cent of UK boards are involved in setting security strategy, despite the fact that nearly eight in ten organisations experienced downtime caused by security incidents last year, costing an average of £2.6 million.

"Cyber security is far more than just building security controls – it's about changing your organisation to be securable," says PwC UK cyber security partner Richard Horne. "That requires all aspects of a business to be engaged, to make tough decisions at board level and embed consideration of cyber-security risk in all decision-making processes."

Most cyber breaches are caused by phishing attacks, with current and former employees representing the top insider risk and source of incidents. Increasingly, though, current service providers, consultants or contractors are causing threats, so these companies are having to up their game.

"Any small company that has customers' financial records is going to be potentially at risk," says Mr Wilson. "Organisations that are small in themselves, but form part of the supply chain are vulnerable – it's potentially easier to find a target."

The Centre for the Protection of National Infrastructure provides security advice to businesses and organisations across the UK and has a 20-point checklist of best practice.

It starts with an audit of authorised and non-authorised hardware and software, and works through the various assets that may need to be protected, from application software to wireless LANs (local area networks).

It covers creating administrative controls to manage access and continuous monitoring to detect breaches when they occur, as they inevitably will.

"Today, it's clear that your speed of remediation is what's really important. Everyone is breached, whether they know it or not," says Kevin Bocek, chief security strategist at Venafi. "It's about actively taking proactive measures to mop up the store every night. Good cyber-security programmes are constantly sweeping out – that's really the measure now of cyber-security effectiveness."

Mr Souza says it's vital to put together a team from the start charged with handling a breach, including legal, technical and communications staff. And, he says, they should work together on a regular basis as too often the team only comes together when a breach actually happens.

"The best organisations are those that at least twice a year have a table-top exercise," he says. "It not only prepares you for the problems you might face, it also builds trust."

Ultimately, embedding cyber security in organisational culture means expressing the threat in terms that are easy for the various stakeholders to grasp.

"If you're a chief security officer, then obviously your view of the cyber risk is going to be how much data you lose and the cost of fines. The chief executive is often more concerned about the reputation of the company and the market view of that, which is the share price," says Mr Wilson.

"One of the difficulties a few years ago was getting the board's attention. Now we've got the board's attention, chief executives are losing their jobs and the security team has suddenly got the opportunity to talk to the board."

Share this article online via **raconteur.net**

BREACH BATTERS YAHOO!'S REPUTATION

Realstock/Shutterstock

In September, Yahoo! admitted that it had been hacked, with half a billion accounts affected. The theft, the company said at the time, could have included names, e-mail addresses, telephone numbers, dates of birth, and even encrypted or unencrypted security questions and answers.

So far, so bad. But, say experts, the company made things even worse for itself by handling the breach as it did. Indeed, the news has thrown a massive spanner in the works of its pending acquisition by Verizon.

"How many times has Verizon now hinted that it needs to go back and look at the value of Yahoo! because there is clear damage to the brand?" asks Kevin Bocek, chief security strategist at Venafi, which analysed the breach. "It's taken at least $1 billion off the value of Yahoo!"

So what did Yahoo! do wrong? Firstly, and perhaps most shockingly, the company took two years to alert users to the fact that their data had been stolen.

"In this time, a great deal of additional harm will have occurred to the comprised accounts, ranging from account hijacking through to identity theft and fraud," says Jamie Graves, co-founder and chief executive of security firm ZoneFox.com.

Yahoo! has also been criticised for saying just a week or two before the disclosure that it wasn't aware of any security breaches.

In fact, the company seems to have been remarkably blasé about the effects of its revelations. When Venafi investigated it found that in the three months running up to the announcement, only 2.5 per cent of security certificates had been replaced.

"They were just going ahead with everyday business, but it seems a bit surprising for an organisation that was just about to announce the biggest ever data breach," says Mr Bocek.

And, after the event, the company failed to do everything for users that it could, choosing not to offer free credit report monitoring, for example.

All in all, the incident has been a textbook example of how not to handle a breach and has been catastrophic for Yahoo!'s reputation. Not only has its acquisition by Verizon been threatened, users are up in arms and there are several lawsuits pending.

Beware the home appliances that can attack

The internet of things, connecting devices and collecting data, holds great promise for business, but presents a serious cyber-security risk

VULNERABILITY
JOHN LEYDEN

The rise of machines is upon us, fronted not by killer robots from the future, but by hopelessly insecure webcams. Last month millions were left unable to access many of the most frequented websites after insecure internet of things (IoT) devices were commandeered to assault a key online pressure point.

Hackers hijacked an estimated 100,000 internet-connected devices by taking advantage of default, factory-set passwords before using these devices as a platform to flood Dyn, a US-based supplier of managed DNS (domain name system) services, with junk traffic.

By rendering Dyn inoperable, hackers effectively obscured the “road signs” that allow surfers to navigate the web. Many high-profile sites, including Amazon, Twitter, Reddit, Netflix and more, become inaccessible during a wave of attacks on October 21.

These attacks against a key internet technology were run using a botnet – a zombie network of compromised devices – made up of compromised routers, digital video recorders, webcams and security cameras. Hackers used a strain of malware or malicious code called *mirai* (Japanese for “the future”) to infect and control these IoT devices.

A group called New World Hackers, earlier linked to an attack that knocked out the BBC’s iPlayer last New Year’s Eve, claimed responsibility for the assault.

The *mirai* malware had also been linked to separate, less high-profile distributed denial of service (DDoS) attacks against cyber-crime blogger Brian Krebs and French hosting provider OVH in mid-September. Source code for the malware leaked online in early-October, giving copycat hackers a blueprint to create botnets of their own.

Although *mirai* seems solely focused around DDoS, it would be possible to use compromised routers to redirect users to phishing sites or to allow the attacker to steal data from internal network shares.

The scale of the attack has caught the attention of politicians. Chancellor Philip Hammond referred to “worrying expansion in the scale of DDoS attacks” during a speech announcing a revamp of the UK’s *National Cyber Security Strategy* at the start of November.

Mr Hammond referred to attacks that take advantage of “insecure coding, weak access controls, poorly implemented cryptography and unprotected databases”.

Security experts have long warned that security mistakes made and resolved in the field of computer and mobile devices years ago are being repeated in the development of internet-connected devices, which often rely on embedded processors running the Linux open source operating system.

Although most familiar in the home, IoT devices ranging from connected light bulbs to building management systems are attractive to business because they offer cost-savings.

Ken Munro, a director at UK security consultancy Pen Test Partners, says the list of vulnerable IoT equipment in small business is long and growing. These include CCTV security cameras, creating a back door into the network, building alarms that can be hacked and switched off over radio frequencies, as well vulnerable smart coffee machines, thermostats, building management systems and more.

Many devices are not designed to be updated. Even if updates exist, notification is rare, so even conscientious users will be left in the dark, assuming they’d take the trouble to patch their systems.

“The most dangerous IoT devices out there are the ones that don’t have a decent patch pipeline or upgrade path,” says Tod Beardsley, senior research manager at Rapid7, the firm behind the popular Metasploit penetration testing tool. “That’s the crux of everything here. Not so much which devices, but it’s any device that can talk on the internet and can’t or won’t be patched.”

Daniel Miessler, director of advisory services at IOActive, says the IoT risk to business centres on rolling out products, connected to other business and operational technology systems.

Protecting IoT systems involves understanding what they are, how they connect and what their capabilities are, Mr Miessler explains.

“Many IoT systems have a local web server, a mobile application, listening network ports, and cloud connectivity,” he says. “Using them normally often involves dozens of connections to third parties, so it’s important to know what are those dozens of connections? What data is being sent? Are there ways to control the device remotely? What credentials and access methods are used to protect each part of this ecosystem?”

The business landscape is yet to adjust to IoT vulnerabilities. “Businesses are just starting to realise both the promise and the risk of IoT,” says Mr Miessler. “Some companies are being cautious and careful, but many are embracing the functionality enthusiastically and placing themselves in danger in the process.

“Right now businesses, like the industry as a whole, are largely in a wait-and-see mode where they’re not sure how and when to deploy IoT, when so many of the risks seem both unknown and substantial.”

Some defences against abuse and attack are already possible. For both businesses and security-conscious consumers, a number of straightforward defences can be applied. Changing from the default password on any purchased equipment is a must. In addition, users should turn off port-forwarding and UPnP (universal plug and play, a home networking protocol) on their routers. Finally businesses should segment their network so that a compromised device on any segment can’t be used to access more sensitive resources such as e-mail and company file servers.

US cryptographer Bruce Schneier recently warned that the market won’t be able to resolve the IoT security problem because neither the buyer nor the seller cares about the problems caused by insecure IoT technology. Chinese manufacturing company Hangzhou Xiongmai recalled several models of webcams that were hijacked by *mirai* malware. But the recall falls short of evidence that vendors can be forced to act through market pressure, according to Mr Schneier.

“Vendors can choose to act, but they can’t be forced to act,” he says. “That’s one electronics firm out of many that are vulnerable. Recalls aren’t a long-term solution to a continually recurring problem. Imagine if Apple had to recall its iPhones every time it issued a security update.”

Sean Sullivan, a security adviser at anti-malware firm F-Secure, says retailers ought to be concerned about a repeat attack on their sites during late-November and early-December, traditionally the busiest shopping periods of the year.

> “Retailers ought to be concerned about a repeat attack on their sites during late-November and early-December, traditionally the busiest shopping periods of the year

“If any DDoS attacks do disrupt retail or other notable attacks occur, there will be calls to regulate IoT devices, demanding better security and passwords by default, while largely ignoring that a great deal of network operator infrastructure could be improved to reduce its vulnerabilities to reflection attacks,” Mr Sullivan says. “IoT devices would not be as dangerous if many networks were configured properly.”

Cees Links, a general manager of Qorvo, provider of low-power, low-cost radio-frequency communication technology for the IoT, is optimistic that security challenges can be overcome.

“History shows that security is a learning process,” he says. “Every day, we are learning what the risks are, but this will take time and, unfortunately, it will take some victims as well. There is a sense of urgency, and I know there is a lot of work done making the IoT a safe and secure place.”

Asked whether a market-based solution to this IoT insecurity problem was possible or whether government regulation was needed, Mr Links, who led the team at US networking firm Lucent that invented and popularised wi-fi technology, conceded that government may have a role to play. “Government needs to make laws and enforce them,” he says.

Government involvement in setting standards for IoT security is so far preliminary. A one-day meeting convened by the US Department of Commerce in mid-October, for example, proposed a new labelling system for smart home devices. This may take years to come to fruition.

Consumers and small businesses buying electronic equipment can look for the CE mark for reassurance that the device satisfies the requirement of applicable European directives, such as electrical safety, but there’s no information security equivalent. In the meantime, IoT device manufacturers are continuing to supply equipment marketed solely on price and functionality. The market has not yet matured to the point buyers will pay more for a more secure device, and there’s no clear yardstick to judge between secure and less-secure products anyway.

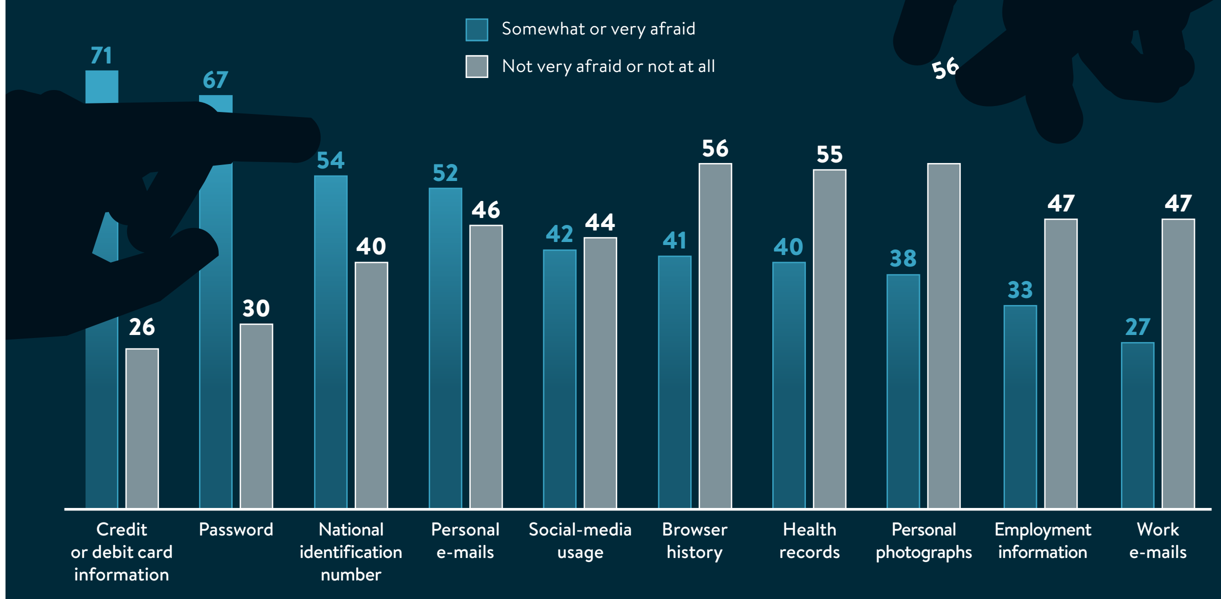
IOActive’s Mr Miessler struck a downbeat note typical of other security experts. “IoT security is going to get a whole lot worse before it gets better,” he concludes.

Share this article online via **raconteur.net**

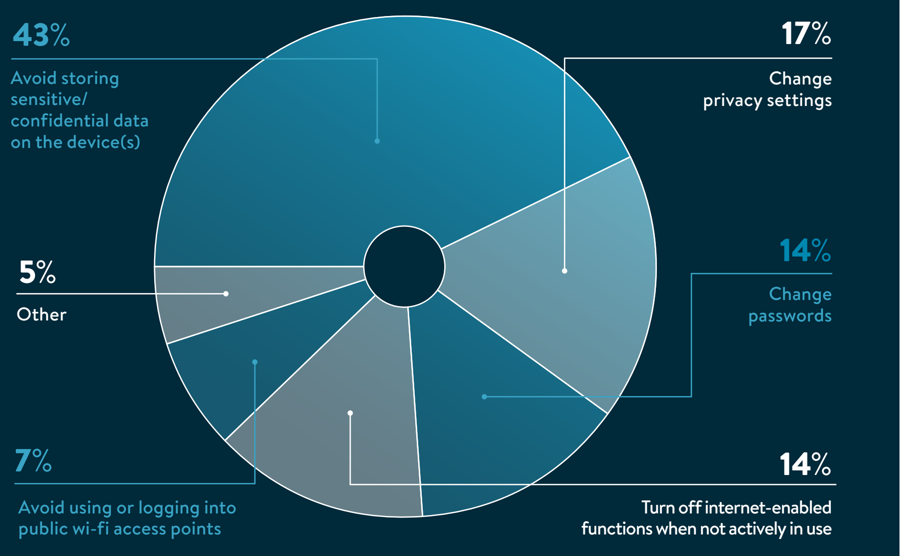
IoT CYBER SECURITY

CONCERNS ABOUT PERSONAL DATA*

HOW AFRAID ARE YOU ABOUT THE FOLLOWING PERSONAL DATA BEING COLLECTED VIA IoT AND MISUSED BY A CYBER CRIMINAL? (%)



WHICH OF THE FOLLOWING IS THE MOST IMPORTANT FOR USERS TO KEEP INFORMATION SECURE ON IoT DEVICES?



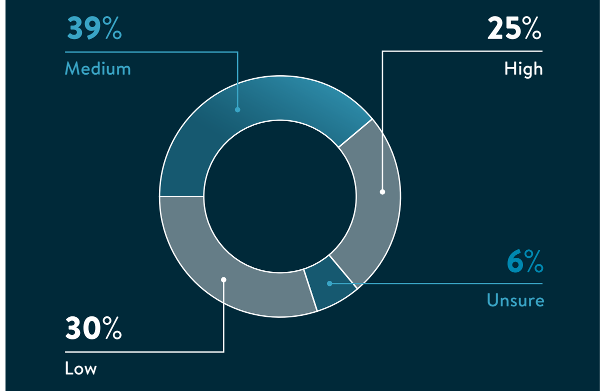
*UK survey of IT professionals

Source: Information Systems Audit and Control Association 2015

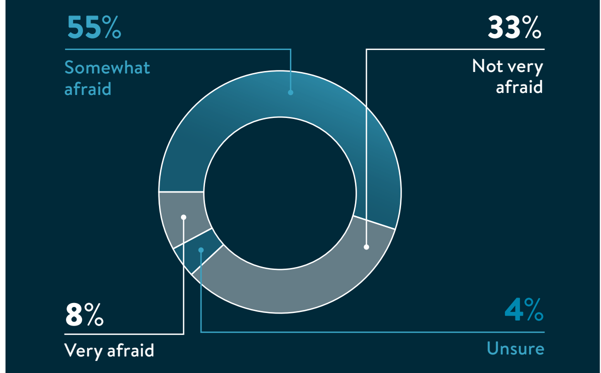
HACKING IoT DEVICES

HOW LIKELY IS IT FOR A COMPANY TO BE HACKED THROUGH AN IoT DEVICE?

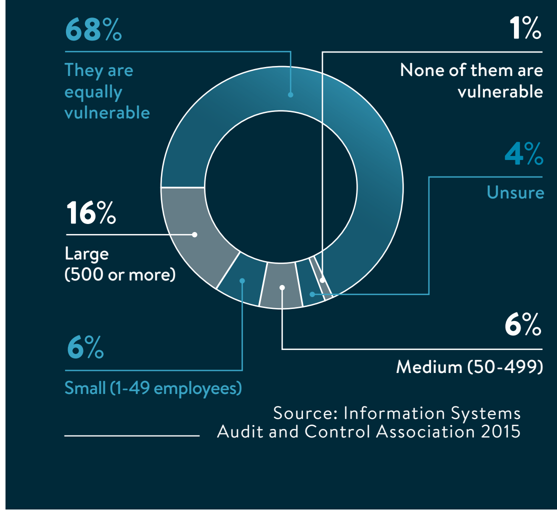
*UK survey of IT professionals



HOW AFRAID ARE YOU THAT YOUR IoT DEVICE MAY BE HACKED?



WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?



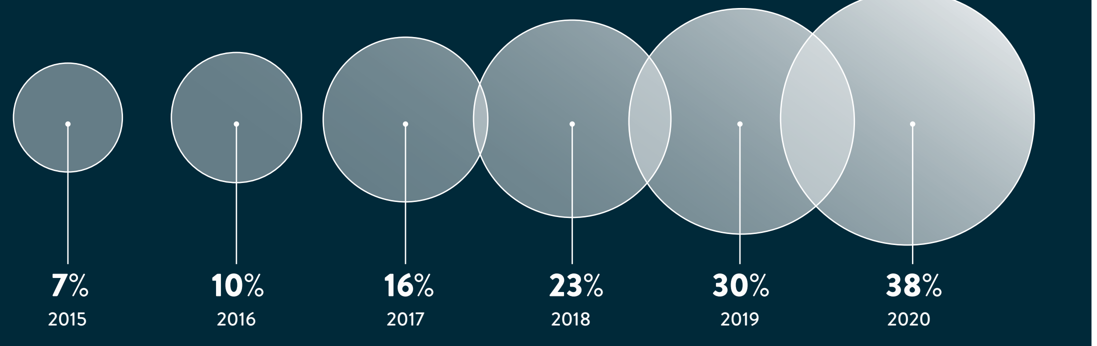
Source: Information Systems Audit and Control Association 2015

25% of identified enterprise attacks will involve the internet of things by 2020

however...

only **10%** of IT security budgets will be spent on protecting against these types of attacks

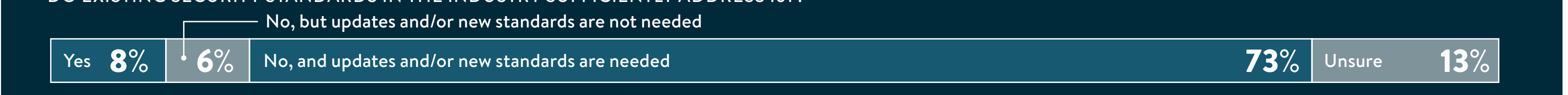
IoT’s SHARE OF THE GLOBAL CYBER-SECURITY MARKET



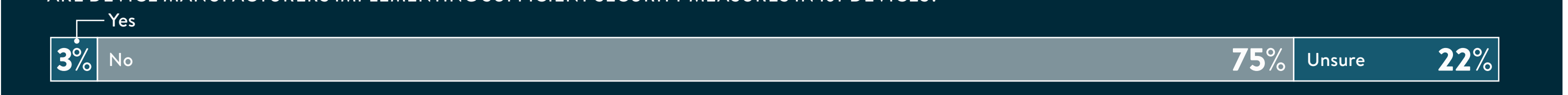
Source: Gartner 2015

IoT SECURITY*

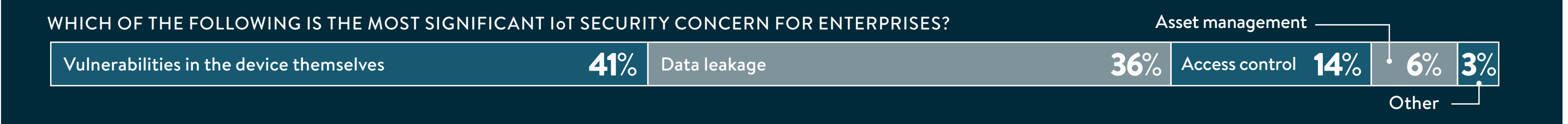
DO EXISTING SECURITY STANDARDS IN THE INDUSTRY SUFFICIENTLY ADDRESS IoT?



ARE DEVICE MANUFACTURERS IMPLEMENTING SUFFICIENT SECURITY MEASURES IN IoT DEVICES?



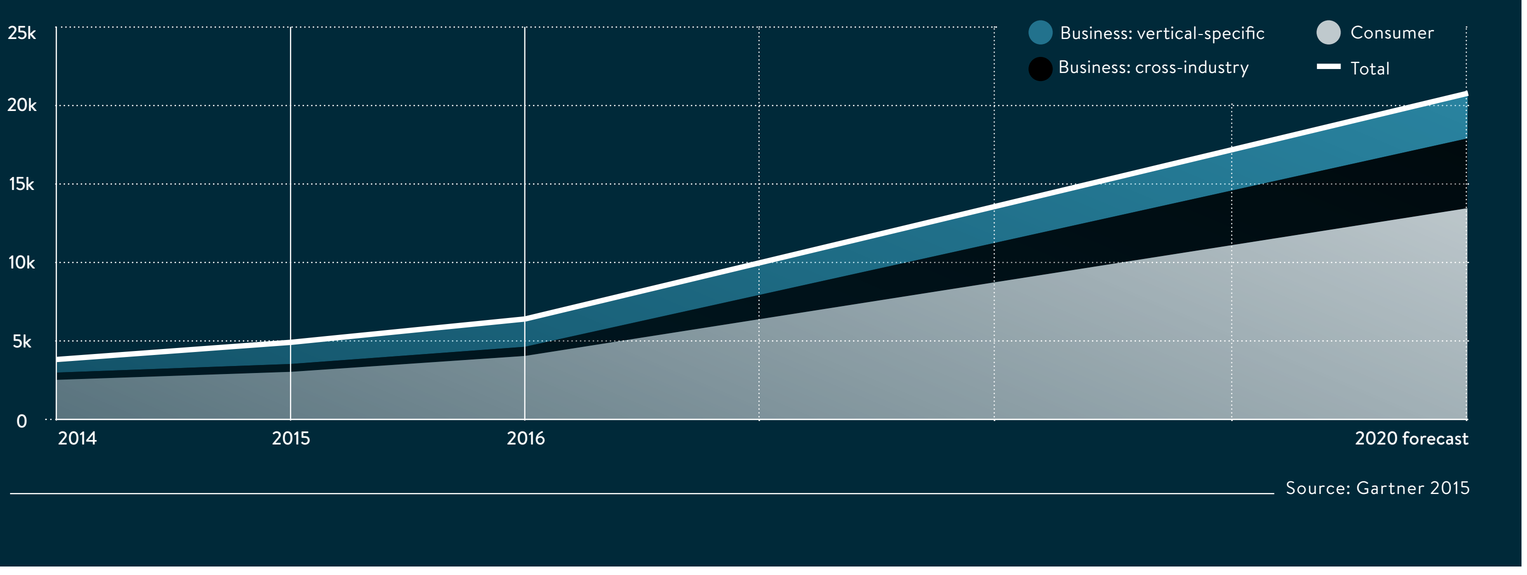
WHICH OF THE FOLLOWING IS THE MOST SIGNIFICANT IoT SECURITY CONCERN FOR ENTERPRISES?



*UK survey of IT professionals

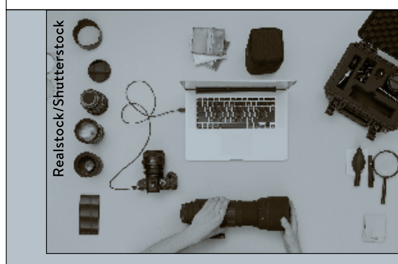
Source: Information Systems Audit and Control Association 2015

IoT INSTALLED BASE, BY CATEGORY



Source: Gartner 2015

WATCH OUT FOR THE HACKERS



Realstock/Shutterstock

Digital video recorders and cameras are widely used by small businesses. Many of these devices are put directly on the open internet with port-forwarding, bypassing NAT (network address translation) and firewall protections. Once hackers hack into an IoT device, they can begin attempting to hack systems on an associated network.

The Holy Grail for hackers is to identify a remote code execution flaw that allows them to plant their own malicious code on vulnerable devices. Hackers exchange details on such vulnerability and the devices they affect. Resolving problems often involves a firmware upgrade that end-users seldom apply.

Shodan, the search engine for the internet of things, locates vulnerable devices passively, but real attackers would use active port-scanning.

The approach taken by the *mirai* malware of automating the process of hacking into devices still running default factory-set login credentials could be used to compromise the network of a business.

Sometimes the login interface is exposed directly to the internet, in which case administrative credentials can be guessed directly via SSH (secure shell) or telnet. This will generally give a login shell at which point the attacker is able to execute commands.

Alternatively, CSRF (cross-site request forgery) attacks are possible, a type of attack that involves tricking a user into viewing a webpage from a computer on a targeted network using a particular wi-fi extender with default credentials.

A proof-of-concept exploit, developed by UK security consultancy Pen Test Partners against a vulnerable wi-fi extender, downloads a copy of Netcat computer networking utility before setting up a simple reverse shell to a server on the internet.

Hackers might be able to use this CSRF to load new firmware on to a targeted device.

If it was possible to gain shell access or upload new firmware to a CCTV camera on the internal network, then the hacker is past the firewall and able to attack computers and servers on an internal network.

COMMERCIAL FEATURE

BEST OF BOTH WORLDS: SWIFT AND SECURE FINANCIAL TRANSACTIONS

As sophisticated cyber criminals become increasingly aggressive and collaborate with offline criminals, banks face a greater threat than ever before. However, one simple innovation can enormously improve their security

KASPERSKY lab

There was a time when a fraudster who had acquired your cashpoint card and discovered your PIN number could steal a few hundred pounds from your bank account through a cash machine. Today the threat is much more serious. Cyber criminals can steal a customer's bank details and not only help themselves to that person's entire funds and assets, but they can gain access to almost every aspect of their lives. These criminals are increasingly more enterprising, more ambitious and better resourced.

Around two years ago, researchers at Kaspersky Lab made a disturbing prediction. They foresaw financially motivated cyber fraudsters adopting the sophisticated techniques previously identified with groups of hackers responsible for what is known as an advanced persistent threat (APT), in other words the continuous, long-term hacking of an organisation, often for political reasons.

The prediction came true just a few months later when Kaspersky Lab announced that it had identified a cyber-crime gang called Carbanak that was using custom malware and APT techniques to steal what could be as much as $1 billion from up to 100 financial institutions in at least 30 countries.

Since then the company has seen an increase in these covert, APT-style attacks that combine the use of reconnaissance, social engineering, specialised malware and long-term persistence to steal money from financial institutions, particularly cashpoints and money-transfer systems.

Alongside this trend is another worrying development, according to Kirill Slavin, UK and Ireland general manager at Kaspersky Lab. "We're also seeing cyber criminals increasingly working in collaboration with traditional fraudsters in a blend of online and offline fraud," he says. "These old-school crooks collaborate with internet criminals to hack online systems, and hijack video cameras and keyboards, so they can see exactly what bank employees are doing. They then share their detailed knowledge of how banks work.

"In some cases, for instance, they will invent a company with fake employees who are receiving fake salaries, but this is still real money that's being paid out. They have knowledge of the online world and they use this to help them to do things that criminals have been doing for years."

Traditional and cyber-crime gangs are merging and, along with the perpetrators of APTs, they're finding more weak points in financial institutions. For banks and building societies, the risks are both financial and reputational as they're forced to compensate customers and apologise to them, as well as often dealing with adverse media coverage.

"The banks face a dilemma," says Mr Slavin. "They want to make customers' lives easy and to ensure that all transactions are smooth, swift and seamless, but they also need to ensure that they're secure. Making things easy for customers, so that they're more likely to remain loyal was why, for instance, banks in the US were reluctant to introduce the chip-and-PIN system. They're now having to bring it in though."

> The good news is that financial institutions don't have to choose between ease of use and security – they can have the best of both worlds

However, card readers and other, similar technology not only slow the transaction process, but often lead to a false sense of security as they're not always as effective against fraud as many people assume.

As attacks become more frequent and sophisticated, some banks are increasingly taking the view that they'd prefer to quietly and discreetly compensate customers for any loss than introduce more cumbersome security. "The problem is that this approach is a bit like paying kidnappers," says Mr Slavin. "The more you do it, the more you encourage fraudsters to attack you as they realise that you're willing to tolerate higher levels of fraud."

The good news, he reveals, is that financial institutions don't have to choose between ease of use and security – they can have the best of both worlds.

"Until recently there has always been a big divide between business-to-business or corporate security on the one hand and customer security on the other," explains Mr Slavin. "In effect, the banks have their security and customers have their own. But a few years ago, Barclays started to buy consumer security products from us in bulk and give them away to their customers.

"At the moment this is only entry level, but we've suggested they also look at something a little bit more substantial. Customers would have to pay for this, but they'd receive a big discount, typically around half the normal price of the product."

But it's the second phase of this initiative, which began around a year ago, that is particularly exciting and offers great benefits for the financial services sector as a whole. Working with another bank that cannot yet be named, Kaspersky Lab's technology can now report back to the bank when a customer's device is subject to an attack. This means the bank will be able to identify how much risk that customer is subject to.

"Meanwhile, we also provide the bank with threat intelligence feeds. These present a real-time picture of the world – which attacks are happening where and when as they happen, as well as which are successful and which are not," says Mr Slavin.

"The bank can then compare this information with the data that it's receiving from individual customer's devices. This allows it to understand not only which consumers are affected, but also what kind of attack they're being subjected to. The banks can then act to reduce the risk they face from cyber criminals and the traditional fraudsters they work alongside. Banks have hitherto not thought of putting these two elements together."

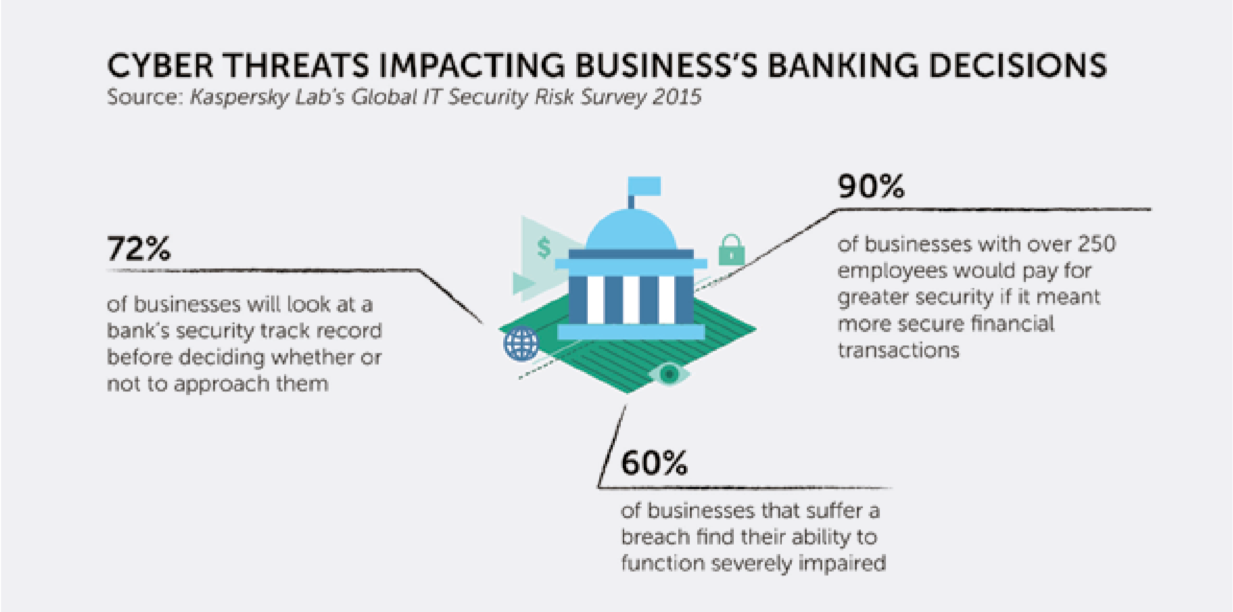
Over the next few years, more and more banks will introduce high-tech security features such as biometrics, including voice, face and iris recognition. First Direct, for instance, recently launched a voice-recognition system for its customers. However, in a traditionally conservative sector where no one institution wants to be seen as pushing the boundaries too far too quickly, caution is the watchword.

"These new technologies will arrive at some point down the line," predicts Mr Slavin. "But in the meanwhile, banks can connect their customer and corporate security to each other to allow information about attacks and threats to be sent from devices to the bank's corporate security centre. This merely requires adding a few words to the customer's terms and conditions. Banks don't even have to reorganise their security departments. Taking this approach represents a paradigm shift in the way they handle security."

For more information please visit www.kaspersky.co.uk

CYBER THREATS IMPACTING BUSINESS'S BANKING DECISIONS

Source: *Kaspersky Lab's Global IT Security Risk Survey 2015*



'Silent' cyber arms race is making a noise

Suspected state-sponsored attacks have triggered an international cyber arms race aimed at repelling and even retaliating if secrets are stolen or online infrastructure targeted, threatening to paralyse critical systems

01

CYBER ARMS RACE
DAVEY WINDER

The United States and Russia are enemies of old, and that this hostility has continued into the cyber age should surprise nobody. That Russia should be quite so blatant in its attempts to influence the 2016 presidential election, with the hacking of Democratic National Committee (DNC) e-mails and their consequent publication on the WikiLeaks website, perhaps more so.

But the surprises don't stop there. The US government has taken the unusual step of formally accusing the Russians of hacking the Democratic Party servers and Moscow of attempting to interfere with the election process. The White House press secretary even went as far as promising there would be a proportional response in retaliation.

"The president has talked before about the significant capabilities that the US government has to both defend our systems in the United States, but also carry out offensive operations in other countries," Josh Earnest told reporters on Air Force One in October. The future of conflict increasingly looks like it sits squarely in cyberspace, and the increasingly open hostility between Russia and the United States has exposed the fact that a cyber arms race has begun.

Carl Herberger, vice president of security solutions at Radware, began his career working at the Pentagon evaluating computer security events affecting daily air force operations. "The cyber arms race is often incredibly clandestine and inherently silent," says Mr Herberger.

Compare the cyber arms race to the nuclear arms race which preceded it. That was all about the power of deterrent and ownership; this is all about strike and denial. Nuclear weapons were tested in the public eye; cyber weapons are tested in secret. The value of a so-called zero-day attack that exploits a vulnerability known only to the attacker and so very difficult, if not actually impossible, to defend against can easily run into six or seven figures in the dark markets where such things are brokered.

Yet while ownership of nuclear weapons was loudly exclaimed, even by those who often didn't have them, ownership of cyber weapons is far more likely to be denied. This unpredictability makes it hard to say with any certainty which countries are capable of what strikes. Or, for that matter, to attribute attacks already carried out.

That said, while there can be little doubt some nation states are far more advanced than others, it doesn't take a cyber stockpile to wreak havoc. We don't know who was behind the recent Dyn DDoS (distributed denial of service) attack that brought many US East Coast-based internet services to their knees on October 21. We do know that pretty much any nation would have had the wherewithal to launch such an attack. It could also be a game-changer.

Even before the attack struck, world-renowned security expert Bruce Schneier had warned that someone was using DDoS attacks to learn how to take down the internet. It seems he might have been right. It certainly demonstrated the internet is far from bulletproof and that paying lip-service to the internet of things (IoT) has created a genie that cannot be put back in the bottle.

The DDoS attack was launched using a network of digital CCTV cameras, video recorders and the like all under the control of the *mirai* botnet. This control system has been released into the public domain, so any cyber criminal can make use of it. However, researchers digging deep into the code it's made with have found traces of Russian language strings. This suggests it was created by Russian coders or someone wants us to think so. Which brings us full circle to the denial of ownership problem, courtesy of potential false flags.

> The increasingly open hostility between Russia and the United States has exposed the fact that a cyber arms race has begun

2016 DYN CYBER ATTACK

The Dyn cyber attack which took place on October 21 involved multiple distributed denial-of-service attacks. Using so-called *mirai* malware, hackers hijacked an estimated 100,000 internet-connected devices by taking advantage of default, factory-set passwords before using these devices as a platform to flood Dyn, a US-based supplier of managed domain name system services. The attack took down major internet platforms and services such as Amazon and Twitter.

False-flag operations enable cyber warfare to take place under the cloak of a third-party adversary and could be very commonplace indeed. The so-called Cyber Caliphate, claiming to be the Islamic State hacking division, successfully disrupted the US Central Command's social media feeds and hacked a US military database after which it posted exfiltrated data on 1,400 personnel online.

The US Cyber Command response was to launch attacks against cyber communication channels and drone-strikes against human targets in Syria thought to be linked with the group. It's now known that the Cyber Caliphate was a false-flag operation run by APT 28, a Russian state-sponsored hacking group.

"Once an organisation's techniques and fingerprint are known, it's relatively trivial for other organisations to emulate it," says David Venable, former US National Security Agency intelligence officer and now vice president of cyber security at Masergy. It's a huge danger, Mr Venable insists as "the use of this information to impact the foreign policies of other states is extremely likely, especially with regards to states with sophisticated cyber operations".

Decoys and distraction are common enough parts of the military strategy puzzle and so it's no surprise they are evident in the cyber sphere as well. Cases of attributing an attack to China might be based upon little more than political will and some handily placed Mandarin dialect in the source code, for example.

It's easy to attribute attacks to groups, less so to attribute nationality with any degree of certainty. So how sure can we be that Russian state actors were behind the US presidential election e-mail hacks?

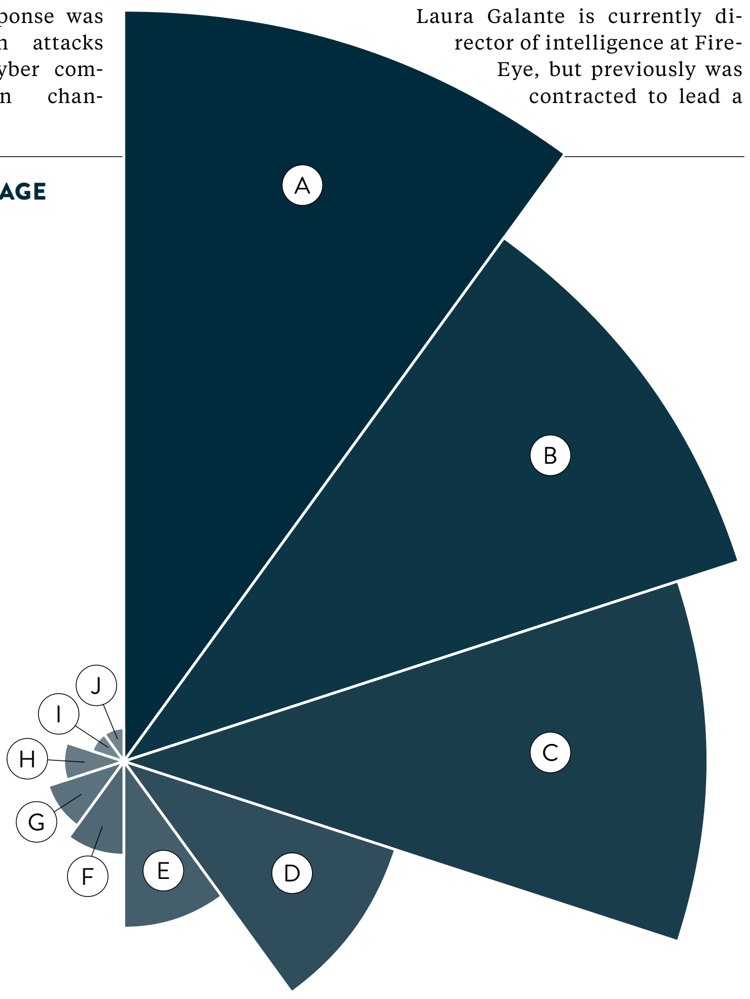
Laura Galante is currently director of intelligence at FireEye, but previously was contracted to lead a

TOP THREAT ACTIONS WITHIN CYBER ESPIONAGE

RESEARCH BY VERIZON FOUND THAT CYBER ESPIONAGE ACTORS ARE PREDOMINANTLY STATE-AFFILIATED GROUPS

Study of 154 accounts of cyber espionage

A	57.14%	HACKING – USE OF BACKDOOR OR C&C*
B	49.35%	MALWARE – C&C*
C	44.16%	SOCIAL – PHISHING
D	21.43%	MALWARE – BACKDOOR
E	12.34%	HACKING – USE OF STOLEN CREDENTIALS
F	6.49%	MALWARE – EXPORT DATA
G	5.84%	HACKING – FOOTPRINTING
H	4.55%	SOCIAL – PRETEXTING
I	1.95%	MISCELLANEOUS – PRIVILEGE ABUSE
J	1.95%	SOCIAL – BRIBERY



*Command-and-control servers

TOP VICTIMS OF CYBER ESPIONAGE

BY INDUSTRY

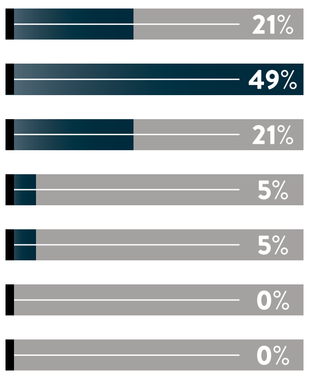
Study of 86 accounts of cyber espionage

36.05%	PUBLIC
19.77%	MANUFACTURING
11.63%	PROFESSIONAL
6.97%	INFORMATION
4.65%	UTILITIES
4.65%	TRANSPORTATION
3.49%	MINING
3.49%	HEALTHCARE
2.33%	FINANCE
2.33%	EDUCATIONAL

DISCOVERY TIMELINE WITH CYBER ESPIONAGE

TIMEFRAME OF CYBER ESPIONAGE INCIDENTS DISCOVERED AFTER THE OCCURRENCE

Study of 358 accounts of cyber espionage

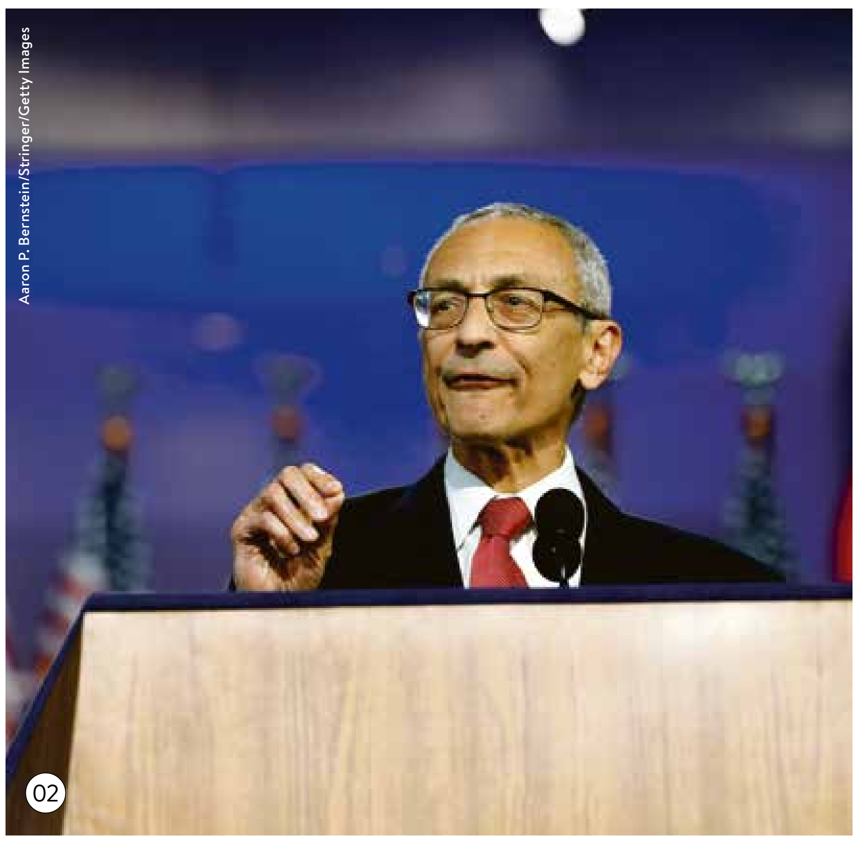


YEARS	21%
MONTHS	49%
WEEKS	21%
DAYS	5%
HOURS	5%
MINUTES	0%
SECONDS	0%

*Percentages do not equal 100 per cent due to rounding

Source: Verizon 2016

PETRAS MALUKAS / Stringer / Getty Images



Aaron P. Bernstein/Stringer/Getty Images

Alexei Druzhinin/Getty Images

01
The United States accused Russia of hacking US Democratic Party servers and attempting to interfere with the presidential election process

02
WikiLeaks published thousands of hacked e-mails from the account of John Podesta, Hillary Clinton's campaign chairman

03
Vladimir Putin has denied any Russian involvement in the hack, saying: "Does it even matter who hacked this data? The important thing is the content that was given to the public."

cyber-security portfolio covering Russian threats at the US Department of Defense. FireEye has worked on many of the high-profile breaches in the current US election cycle, including tracking the two state-sponsored groups behind the DNC e-mail attack, APT 28 and APT 29.

"We've seen a variety of different forensic artefacts that indicate Russia-sponsored groups are behind the DNC hack and a variety of other leaks that occurred this summer," says Ms Galante. "We've been following these groups for years, tracking their activities and profiling their infrastructure."

Unlike Chinese-based threat actors, these groups focus purely on military and political targets, and do not appear to conduct widespread intellectual property theft for economic gain. As far as APT 28, also known as Fancy Bear, is concerned, for example, the group compile malware samples with Russian language settings during working hours consistent with the time zone of Russia's major cities.

"It collects intelligence on defence and geopolitical issues, intelligence that would only be useful to a government," says Ms Galante.

So what about Guccifer 2.0, the so-called Romanian hackers who have claimed responsibility for the DNC e-mail hacks and the consequent uploading of them to WikiLeaks? "The Guccifer 2.0 persona is likely a Russian denial and deception effort to undermine the narrative of Russian responsibility for the leaks," says Toni Gidwani, director of research operations at ThreatConnect.

"They are a shiny object designed not to fight these accusations, but to distract the public by leaking sensitive information. That they've been this successful is a real cause for concern."

Using so-called "faketivists" such as this to intimidate, discredit and gather intelligence on its opponents affords the Kremlin a layer of anonymity with which to advance its interests and distract from its activities.

So what investments are being made in developing, buying or just stealing cyber arms? When it comes to financing this cyber arms race, statistical data is unsurprisingly hard to find. In the UK, chancellor Philip Hammond has spoken about a £1.9-billion investment in cyber, but the strategic breakdown is vague to say the least. There's money for educating the next generation of security researchers, for helping businesses to protect themselves against the ongoing cyber-crime wave and money to protect critical national infrastructure from cyber attack.

> The United States has more capacity than anybody, both offensively and defensively, when it comes to cyber weaponry

What there isn't, nor would you expect there to be, is an itemised budget for cyber weaponry as part of the "defend, deter and develop" strategy.

"We know of the GCHQ budget for cyber due to the openness of former chancellor George Osborne," says Peter Barbour, head of response with Context Information Security. "Similar figures can possibly be found for US military and intelligence spend on cyber, and potentially even China and Russia."

What that means in terms of development of specific cyber arms is anyone's guess and anyway the ability to inflict the most damage is not as simple as who invests the most money. "A small team that is highly motivated and equipped with the right set of tools and access can achieve huge amounts without the multi-million-dollar investment figures that are suggested," says Mr Barbour. "Equally a heavily funded, well-organised effort can achieve phenomenal success too." So maybe the question should be who's spending the most on national cyber defence efforts? It's not, after all, just about attacking with "arms" in this domain.

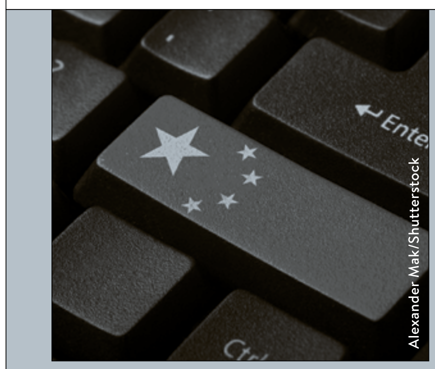
After the G20 conference in China earlier this year, President Obama told reporters the United States has more capacity than anybody, both offensively and defensively, when it comes to cyber weaponry.

So how much emphasis is being put on the defensive capability of cyber weapons by nation states? "Traditionally, almost all the focus has been on defensive capability, by all factions within the cyber warfare arena," says Jonathan Couch, senior vice president of strategy at ThreatQuotient. "But it was defence in the blind." In other words, everyone focused on generic defence-in-depth, layered security without understanding the threat.

Over the past few decades, Western governments and the military have been trying to learn from their offensive capabilities. That is, says Mr Couch "leveraging what we know about breaking in to others to defend ourselves better". Additionally, there is cyber-threat intelligence gained on the offensive side that has traditionally been very close held information, which we are now finding ways to share with the defensive mission to do it better.

Share this article online via **raconteur.net**

CHINESE WHISPERS IN CYBERSPACE



Alexander Mak/Shutterstock

"China is one of the most prolific actors in the economic espionage space, having invested in cyber espionage in a way that is unprecedented in other countries," says Eric O'Neill, Carbon Black's national security strategist and a former FBI operative best known for his role in the capture of Soviet spy Robert Hanssen.

Beyond the typical theft of military and government secrets, China has engaged in theft of trade secrets and IP from businesses across the United States. "This provides them the economic advantage of refining technology that has already moved through the R&D gauntlet into direct production and then copying using a cheaper industrial base," says Mr O'Neill.

That said, according to FireEye's Laura Galante, China has slowed its espionage activity more recently. "Since mid-2014 we have observed an overall decrease in successful network compromises by China-based groups against organisations in the US and 25 other countries," she says. "These shifts have coincided with ongoing political and military reforms in China, widespread exposure of Chinese cyber activity, and unprecedented action by the US government."

The late-2015 US-China agreement, stating that neither government would support or conduct cyber-enabled theft of intellectual property against the other, might be more successful than many thought it could be. However, any speculation that China has scaled back or even disbanded its cyber-attack capabilities is misplaced, according to Ed Wallace. The director of incident response at MWR Infosecurity reckons the reality is that "due to a substantial shake-up in its military structure, a large proportion of its US-focused cyber-attack activities were paused for a short amount of time".

That time is now up and with the reorganisation bedding down the attacks have started to pick up pace again. They are, Mr Wallace insists, likely to be "both harder to detect and harder to defend against".

That reorganisation of China's military strategy has resulted in a new Central Military Commission, under which sits its new command unit, the People's Liberation Army Strategic Support Force (PLASSF). Headed by the hugely experienced Lieutenant-General Gao Jin, the PLASSF will consist of around 250,000 to 300,000 staff and contain the bulk of the country's cyber operations. It will also now run 24 hours a day, as opposed to Chinese business hours as was the case previously.

"The creation of the PLASSF, dedicated human intelligence units and SpecOps teams are all bad news for China's targets," Mr Wallace concludes. "Far from being left behind, China has significantly upped its game, throwing down the gauntlet for other threat actors."

COMMERCIAL FEATURE

AUTHENTICATION: NEXT SECURITY FRONTIER

Powerful new ways of verifying a tech user's identity can achieve the right balance between security and access

Access to information, whether on a tablet in Tallinn, a laptop in Luanda or a smartphone in Shanghai, is now a fact of modern life. Executives need to work on data, on the go and on all devices if they're to embrace an increasingly connected world.

Yet companies are struggling to offer employees secure access to the systems they need. Stronger authentication models such as multi-factor authentication have been around for some time, but their use is still lagging. This is especially concerning since we are in era when cloud computing, mobile devices and social networks have radically transformed the way businesses operate.

A myriad of top cyber-security reports released earlier this year from the likes of IBM, Verizon, Dell, Symantec and Cisco all paint a grim picture: an escalation in targeted hacking, cyber attacks and security breaches. Juniper Research estimates this type of crime will costs businesses globally more than $2 trillion by 2019.

"It doesn't help that the bad guys are getting way more sophisticated in their engineering of attacks," says Kent Purdy, solutions marketing manager at Micro Focus, a multinational software and information technology company. "So it's interesting to see where identity management is going to go. It needs to change."

As we enter what many are calling the fourth industrial revolution, characterised by the digital economy with the intensive digitisation of consumption and production of goods and services, industries globally are seeing a proliferation of risk and the potential for wrongdoing, especially with people's precious data.

"What is also different today is that billions of us have a mobile phone and increasingly a smart one. Companies want to facilitate anywhere, anytime access to anything from anyone through our devices," says Mr Purdy. "Yet the adoption of technology has occurred faster than our willingness to secure and authenticate it."

Our dissatisfaction with the insecurity of usernames and passwords already goes back nearly a decade, as do efforts to replace them. IBM developers discussed ditching them as early as 2008. Biometrics as a way to identify someone has existed for longer and is back in fashion. Now even mobile selfies are emerging as a way to verify people and payments.

"Authentication technology has evolved more in the last few years than it has in the last two decades," says Mr Purdy, whose company has four decades of experience in enterprise software, including access management. "But less than 10 per cent of companies out there have any form of dynamic authentication."

This way of verifying people is a lot smarter and secure. It goes beyond passwords and instead adapts to a user's situation and risk profile. Many of us have already experienced dynamic authentication if we've had to call up our bank to unlock a credit card overseas or answer questions to login to Facebook abroad.

"Authentication must evolve beyond today's password-centric framework. Organisations need to start developing a comprehensive risk-based strategy. If someone is trying to access a server remotely via a device in Beijing, the authentication requirements are going to be different from someone accessing them from a secured PC in a local office in Bradford," says Mr Purdy.

"This new type of authentication can recognise changes in our behaviour, it isn't static and context is crucial. For instance, is that person using the same device in their usual location? What else have they accessed lately? Does everything look normal?"

Facebook uses a similar type of authentication. Whenever a person logs on, servers look at data such as the network they're logging on from, what browsers or devices that person typically uses and the third-party apps they have connected to their account. If something is odd, Facebook requests users to verify their identity by sending a code to a person's phone or poses questions only that user can answer.

Social media isn't the only sector using adaptive authentication, financial services and healthcare providers are leading the way globally when it comes to this advanced form of security because of the potential loss to client data, money and credibility.

"Using adaptive authentication is a way to match user verification to the potential risk of access. It works silently in the background with little impact," explains Mr Purdy.

> Using adaptive authentication is a way to match user verification to the potential risk of access

"Since much of the analysis is done behind the scenes, the technology makes it easier for you. When the measured risk is low, it can verify who you are easily without the need for re-entering credentials. But when the risk is high, further authentication is needed from the user. Because this dynamic approach to authentication is especially important to users away from the office, it's important that we are able to deliver this experience on most devices."

This type of cyber security is also called risk-based authentication because different people need different levels of access to data in relation to their work; while some work on sensitive information, others don't.

Micro Focus has therefore embedded a so-called risk engine into its Access Manager software. "This gives each user a score depending on the access they need. We can easily set different levels of authentication since it is all about managing the level of risk. It asks questions – do you let them in as is or does he or she need more of a challenge? If a bit of data is so sensitive we might need to restrict access," says Mr Purdy.

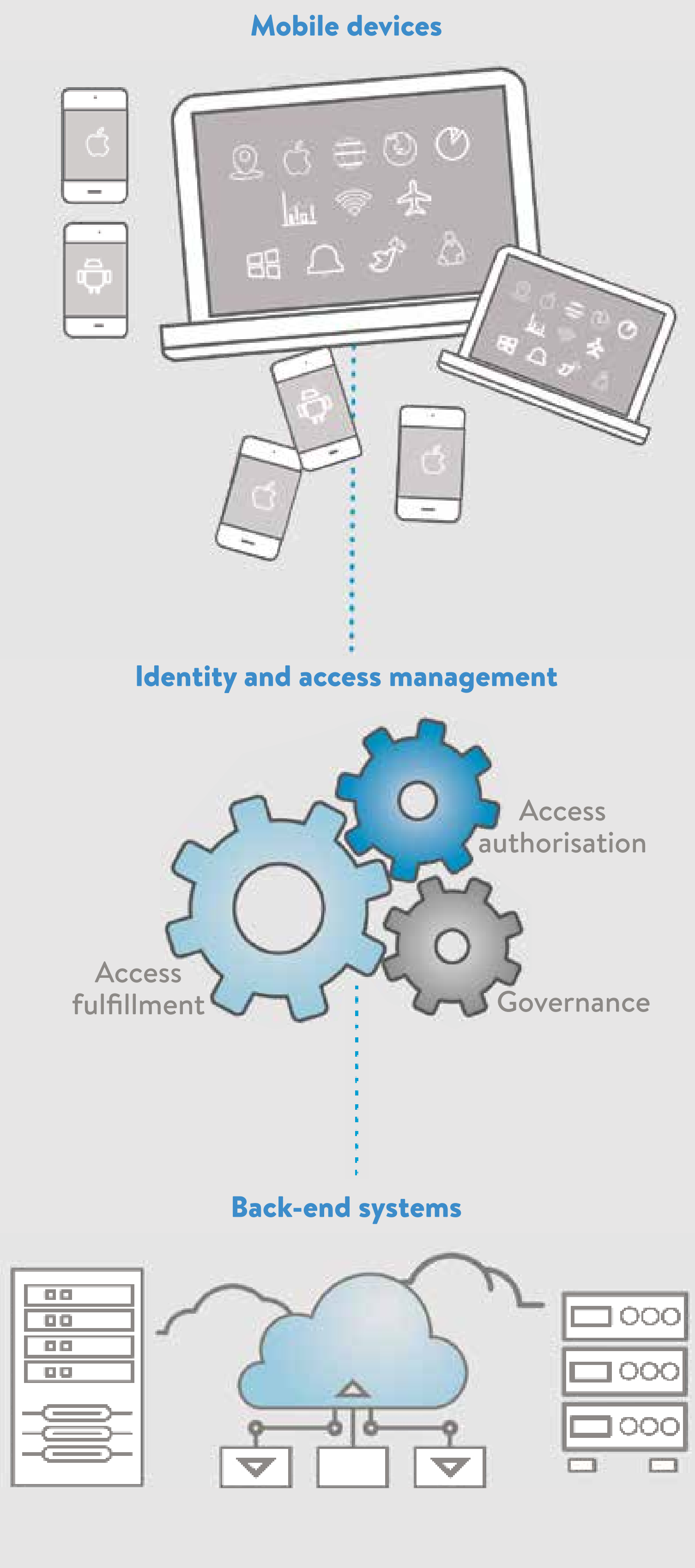
"Protecting sensitive information from outside threats, while keeping access simple for users, can be a complex challenge. Our focus is to use powerful new ways to verify a user's identity. Businesses want convenience since it enables commerce; they don't want lock down. So it is about getting the right balance between security and access."

Advances in smartphones are pushing the envelope for authentication. There is now a greater emphasis on location technology as well as behavioural biometrics.

"These are going to be powerful new tools in the industry. You want a dynamic, adaptive intelligence guarding you – one that evolves over time," Mr Purdy concludes.

For more information please visit www.microfocus.com

SIMPLIFY AND SECURE ACCESS TO YOUR MOBILE USERS



What makes criminal hackers want to hack?

Cyber criminals are driven by a diverse range of aims and ambitions – so what drives them to break into a computer and steal?

MOTIVATION
DAN MATTHEWS

01 MONEY

Financial gain is the daddy of all motives for cyber crime. According to Orla Cox, director of security response at Symantec, people in the UK suffered up to 2,215 ransomware attacks a day in the last 12 months. In most cases, the victim's data, including important documents, images and video is all encrypted, and access to it denied until a ransom is paid.

Research by SentinelOne covering 100 chief information security officers whose organisations have been targeted by hackers revealed that 64 per cent believed their attackers were driven by financial gain.

"Most forms of malware in circulation today are meant to make the authors money," says SentinelOne's chief of security strategy Jeremiah Grossman. He points to the CryptoWall ransomware, a Trojan horse that locks up files and requests payment for the key. By some estimates it has caused $325 million in damages.

Stealing this amount of money in the real world may be impossible. But not only can criminals take more via virtual channels than they can by walking into a bank with a shotgun, they can hide easily too, usually in territories thousands of miles from where their victims feel the pain. If there's no such thing as the perfect crime, this comes pretty close.

02 THE CHALLENGE

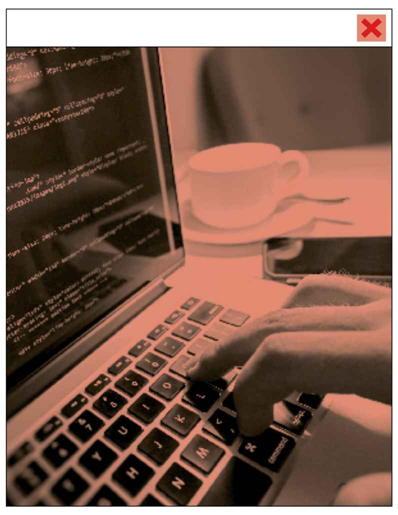
The term "hacker" is ambiguous. It doesn't come with a value judgment attached to it, so technology experts who fall under the definition range from ordinary people who love solving problems with computers to nefarious individuals applying their skills with criminal intent.

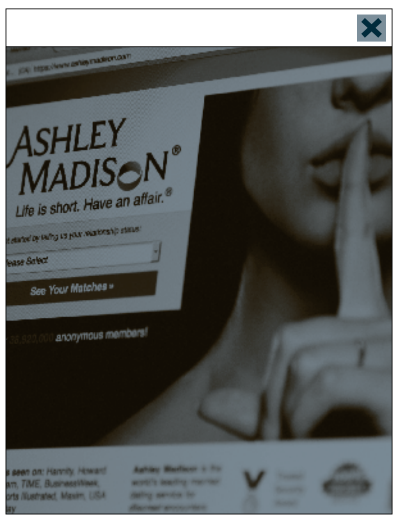
What binds these two groups is the thrill of the chase. They relish the chance to pit their wits against each other and stretch the envelope of their abilities. For some this means creating brilliant software in a competitive environment; for others it means concocting an infamous heist.

But a small group doesn't fit either category. They just want to see how far they can go. To these, a complex security protocol is like a Rubik's Cube with a thousand sides – a problem too tempting to ignore.

In 2001, British hacker Gary McKinnon began accessing secret files on computers owned by the US military and Nasa. Operating from his girlfriend's Aunt's house, he read, manipulated and allegedly destroyed files for more than a year before being apprehended by the authorities.

"The motive for these hackers is simple – breaking something not made to be broken and accessing something never intended for their eyes," says Paul Briault, director of digital security at CA Technologies.





03 HACTIVISM

Anonymous, LulzSec, Lizard Squad and Fancy Bears are all groups claiming to campaign for virtuous ends via criminal means. These and hundreds of smaller groups mostly target large organisations. They do so for reasons ranging from exacting revenge for perceived wrongdoing to uncovering security flaws which are then hastily patched up by the victim organisation.

Last year, a group calling itself The Impact Team swiped e-mail addresses and credit card data from the website of Ashley Madison, a dating organisation for married people wanting an affair. It published the data via the dark web and publicly shamed site users.

"The Ashley Madison data breach last year is one example whereby hackers threatened to release details of individuals in a database," says Paul McEvatt, senior cyber threat intelligence manager at Fujitsu UK and Ireland. "It highlighted the sophistication of cyber criminals and why more needs to be done to combat these multilayered threats."

In September, Fancy Bears stole and published athlete's medical data in a bid to "expose the athletes who violate the principles of fair play by taking doping substances". Meanwhile, in 2011, LulzSec targeted Sony in retaliation for the company's legal action against hacker George Hotz. It claimed to have compromised one million accounts.

04 REVENGE

For some, cyber criminality is a career, for others it's a moment of rage-fuelled madness. Disgruntled employees, spurned job candidates and people fed up with perceived mistreatment can now exact revenge in the virtual world.

Where once they slashed tyres or burnt out a stock cupboard, now the criminally unhinged have the option to bring down a company's computer systems instead.

In February, a former Citibank employee was sent to prison and fined nearly $80,000 after erasing company data and sending 90 per cent of its network into darkness. Lennon Ray Brown, 38, from Dallas, admitted damaging a protected computer after receiving a poor performance review from his line manager.

Fearing the sack, he shut down the Citibank system. Then he sent a text to a colleague. It read: "They were firing me. I just beat them to it. Nothing personal, the upper management need to see what the guys on the floor are capable of doing when they keep getting mistreated.

"I took one for the team. Sorry if I made my peers look bad, but sometimes it takes something like what I did to wake the upper management up."

05 SUBVERSION

Orla Cox at Symantec points to a number of recent instances of digital meddling in which espionage and supervision were the likely motive.

"Earlier in the year we saw a new wave of attacks carried out by two groups, one of which was the Carbanak group, targeting a number of financial organisations. An earlier attack by a different group also targeted financial institutions resulting in hundreds of millions of dollars in losses," she says. "Carrying out attacks online essentially makes it easier for these criminals to hide their tracks."

Fancy Bears, the group made famous by their leak of athletes' medical records, were accused of having links to the Russian state. The motive, it was hypothesised, was retaliation for restrictions imposed on Russian track and field athletes and para-athletes following accusations of widespread doping.

Meanwhile, in November 2014, a group calling itself Guardians of the Peace leaked private information about Sony employees on to the internet, including e-mails, salaries and even unreleased films.

The group launched the attack in response to the Sony film *The Interview,* which depicted the assassination of North Korea dictator Kim Jong-un. Guardians of the Peace demanded the film withdrawn and even threatened a terrorist attack on theatres.

06 NOTORIETY

Hacking is a competitive sport and cyber criminals are often motivated by a sense of achievement. If they can pull off the ultimate hack of, say, a global corporation or agency, then the kudos from their peers is huge.

As Jarrod Siket from ThreatQuotient points out: "Some individuals and groups are solely motivated by the recognition that comes with being the first to do something, or successfully disrupting a high-value or highly visible target."

Paul Briault at CA Technologies agrees. "Putting their name to what could be a globally discussed hack increases their notoriety. Being able to brag about their skillset is of huge value to hackers," he says.

"Hackers like to show off their intelligence, skillset and ability. Knowing that every business and organisation is attempting to keep them out and away from information only encourages them more. Hackers are often proud to make their presence and accomplishments known."

Social media platforms such as Twitter have clearly played a part in spreading the word – and the perpetrator's notoriety – about attacks and in some cases they have even helped co-ordinate hacks.

Although hackers such as Kevin Mitnick and John Draper have gained notoriety, as well as a criminal record, from hacking, most hackers are never famous.

Top hacker on the side of the good guys

Jamie Woodruff is an ethical hacker who helps companies keep out cyber criminals trying to break into computers to steal their money and secrets

INTERVIEW
EDWIN SMITH

"With cyber security," says Jamie Woodruff, "you get geeks, the guys who find the critical vulnerabilities, the bugs. Then you get the guys who are able to exploit people. That's my passion."

In his strong Lancashire accent, Jamie, 23, explains his talent for observing people's movements, speech and body language to find their weaknesses before targeting them with "social engineering" techniques. "But," he adds hastily, "I'm bound by a strict code of ethics."

That's because he operates as an ethical hacker and certified penetration testing engineer to probe companies' systems for faults, with permission. The idea is that they get fixed before a less scrupulous party takes advantage.

But that might not always be the case. The average company is the target of more than 100 cyber attacks a year, with a third of these being successful. What's more, according to research published by Accenture, a third of those successful breeches aren't discovered by the company itself.

For one of Jamie's recent projects he monitored a large financial institution for several weeks before eventually spotting a way in. The company would have pizza delivered by a well-known chain every Friday. So, he applied for a job there, got hold of a uniform and "walked straight past security and into the server room". After using some UV spray to see which buttons had been pressed on a keypad, he bypassed another layer of outdated security and gained access to the company's supposedly secure information.

To aid similar work he has a stash of ID badges, props and other uniforms from Royal Mail to UPS and FedEx. Disguised as an alarm technician, he gained access to another office building. "I got one employee to make me a brew, to make it seem like I was supposed to be there. I stole all their data within an hour and a half," he says.

But Jamie's skills extend beyond the art of disguise. On a recent trip to Norway he responded to a request to showcase "some proper hacking, some really scary stuff" by stealing the conference organiser's laptop along with his credit card data and passwords, and then using them to start the engine of his host's Tesla car remotely.

> I think a massive attack is imminent in the next few weeks

"There's so much security in Tesla vehicles, but the end-user logging into his account uses the same password for everything. So I got access to the car and started it remotely. If you're a hacker, you don't have to steal the keys," he says.

The same goes for banking apps. He says that a particular bank's app allows you to call the customer service team from within the app and ask to transfer money without passing any additional security checks. It requires a passcode to get to that stage, but many people still use the same code for the app as they do for the phone it's on.

> Once I understood hardware, I understood the graphics and started writing viruses when I was 12 or 13. Obviously nothing malicious

He is repeatedly at pains to stress he is utterly committed to remaining within the bounds of an ethical code. He also says that when a company tasks him with breaking into its systems, there are always some ground rules.

"So I can't just crowbar my way in and smash a fire alarm," he says. Neither can he cause physical damage or distress to employees or other people on the premises. But when I ask whether some of the skills that he employs were learnt on the other side of that ethical line, he's less forthcoming. "We'll not go into detail about that one," he says.

What Jamie will reveal is that he first became interested in computers aged nine, when his dad left him alone with the family's brand new machine. "I decided to see what was inside the big black box, so took it apart with a screwdriver and all of a sudden was looking at all the components," he says.

However, when he put it back together, he forgot to replace the fan and so ended up frying the central processing unit. This led to a trip to the computer shop and a chance to begin learning more about the hardware, a process that continued for several years. "Once I understood hardware, I understood the graphics and started writing viruses when I was 12 or 13," he says, adding quickly: "Obviously nothing malicious."

But while Jamie continued to experiment and learn with computers, picking up an A* in his IT GCSE, the rest of his time at school was not as successful: "I got Cs, Ds Es and Fs in everything else, and didn't really care at that time." He went to Blackburn College for a while, but dropped out and began working at an old people's home before deciding to have another crack at formal education. Despite having no A levels, he built a bot that automatically sent an application letter to practically every university in the country.

That got him a place at Bangor University and led to his entering a hackathon with a friend. He was singled out as the best performer of the weekend and won a prize, which was the cost of his certification to become an accredited penetration testing engineer. "All of a sudden," he says, "I had a purpose."

His exploits since have included hacking his way into Facebook and uncovering major flaws in Kim Kardashian's site, where data about thousands upon thousands of her fans was at risk. In both instances he alerted the parties in question and changes were made.

This is part of the reason that he is now a sought-after speaker at conferences and events for the likes of *WIRED* and BNP Paribas. The people who hire him, he reckons, want to raise awareness about the risks that businesses face in a way that quoting endless statistics doesn't tend to achieve.

So he tells audiences about technology such as a "pineapple", a device that can trick laptops or phones into thinking they are connecting to familiar networks such as Starbucks wi-fi, when in fact they're hooking up to someone who's going to take their data.

But, he says, one of the biggest weaknesses companies have is their senior people, who are often complacent when it comes to their own information and possessions, but also when it comes to allocating resources to defend against cyber attacks.

Jamie applauds Bank of America for announcing the company's cyber-security budget would effectively be unlimited, but admits that even for companies with a hefty war chest, "not every risk can be stopped".

To underline this, he points to the massive distributed denial of service (DDoS) attack that took place on October 21. Judged by some to be the biggest attack of its kind, it brought down numerous websites of reputable international companies, including Amazon, Facebook, *The Guardian* and PayPal, and even affected connected devices, such as intelligent light bulbs and thermostats. According to a report that Jamie believes to be credible, the attack was carried out with just 10 per cent of the server power available to the network that was responsible.

"Personally, I think that was a test. I think a massive attack is imminent in the next few weeks," he warns.

The good news is that a solution may be on the way too. At two of this summer's most high-profile hacker conferences, Def Con and the Black Hat security conference, there was a huge amount of interest in new types of systems that use artificial intelligence to learn when they are under attack and defend themselves.

However, the leading-edge technology isn't yet widely available or used. And, until it is, you can bet Jamie's expertise will remain in great demand.

Share this article online via
raconteur.net

COMMERCIAL FEATURE

ARE YOU PREPARED FOR A CYBER ATTACK?

Organisations can learn from each other to defend against cyber attackers, says ***David Stubley****, chief executive of 7 Elements, the UK security consultancy focused on technical security testing and incident response*

7Elements
Independent information security consultancy

At 7 Elements, we manage security incidents for our clients that cover a broad spectrum of threats, from highly capable advanced persistent threats through to opportunistic and untargeted attacks using commonly available exploit code. All incidents are unique and 7 Elements believe that preparation is key to any incident response.

However, it can be difficult for organisations to anticipate what exactly will be required in the event of an incident. For many, incident response procedures tackle scenarios identified through business continuity risks or following internal incidents. This results in an inward focus that leaves incident management procedures lacking.

An inward focus does not effectively anticipate the full suite of scenarios that an organisation may face during an incident as it does not take into account the evolving threat landscape and changing external environment. Without placing incident response measures in this dynamic external context, organisations may find their response measures lacking in the face of current attacks.

Gaining information about factors external to your organisation, such as threats, is a challenge, but organisations have an opportunity to gain insight by carrying out reviews of incidents that have made the headlines.

Groups conducting attacks, whether for financial gain or other motives, will frequently use the same methods of compromise. This is demonstrated in the recent attacks on the electronic point-of-sale systems in the US retail sector and the ongoing use of targeted phishing e-mails to gain access to corporate networks, among others.

The use of similar methods by attackers means organisations have an opportunity to identify attack approaches and vulnerabilities that could be applicable to them. Organisations should therefore look to use the experiences of others within their sector to enhance their own incident management procedures.

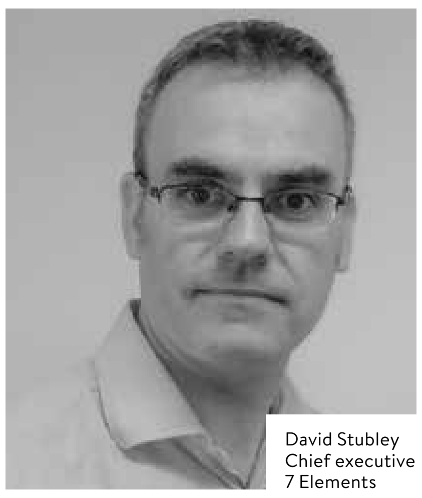
While the full details of an incident will not be publicly available, organisations can gain insight into the incidents of others through information-sharing forums and employees' individual relationships with their counterparts in other organisations.

It is likely that an organisation will be able to gain sufficient information to identify the vulnerabilities exploited by attackers and key attack vectors. This information can be used to review the incident and determine if the organisation is itself vulnerable to such an attack. Organisations should therefore conduct reviews of incidents that impact other similar organisations.

Once an organisation has identified whether it is vulnerable to a similar incident, it can then identify potential attack scenarios and play these out within the context of their environment. This is often done through security testing and red teaming.

An organisation will then be able to understand whether it has sufficient controls in place to prevent an incident and test their effectiveness in the context of a similar attack. By keeping abreast of the threat landscape, spotting trends within relevant industries and reacting to the external environment, organisations will be able to plan effectively for incidents.

Taking the time before an incident occurs to prepare correctly will inevitably lead to a robust and fit-for-purpose approach to cyber security-related incidents, and in the event of such an incident, the ability to respond effectively and rapidly.



David Stubley
Chief executive
7 Elements

So, on the basis of learning from others, the two key questions that all chief executives and chief information security officers should be asking on a regular basis are "Are we vulnerable to the attacks being reported in the media?" and "If we were compromised, would an attacker be able to gain access to unencrypted sensitive data?" Each question should then be followed with "What assurance activity have we done to confirm this position?"

By learning from others' misfortunes, organisations may be able to avoid the pain of going through a similar experience and should an attack occur, organisations will have taken the time to develop resilient incident response measures with which to tackle these anticipated threats.

7 Elements are an approved government provider of penetration testing and has recently been named 2016 SME Cyber Defender of the Year for their incident response services. For more information please visit www.7elements.co.uk

Smaller UK businesses are growing targets

Small and medium-sized enterprises are increasingly in the sights of cyber criminals, sometimes as a means to attack corporate associates where there are riches to plunder

SME FOCUS
FINBARR TOESLAND

SFIO CRACHO / Shutterstock

Cyber attacks against big businesses are nothing new, with high-profile companies falling foul of sophisticated online criminals at an alarming rate. A cyber attack on a smaller enterprise is unlikely to get anywhere near the level of publicity garnered by the hacking of a multinational corporation, but this doesn't mean there aren't many successful attacks against small firms on a daily basis.

Data held by small and medium-sized enterprises (SMEs) is becoming increasingly valuable to cyber criminals. According to recent research released by Barclaycard, 48 per cent of SMEs fell victim to at least one cyber attack last year and 10 per cent were targeted multiple times.

Cyber criminals are targeting SMEs in a growing number of ways, with ransomware attacks proving to be one of the most popular methods used to extract money. Ransomware is a type of malware that encrypts all files on a computer and demands money, usually untraceable bitcoins, for them to be unlocked. Not only do 36 per cent of ransomware victims report loss of business income due to the attack, but this type of cyber threat is expected to increase 300 per cent from 2015 to 2016, according to insurance research provider Advisen.

"The impact of a successful attack on hard-won reputation, supply chains and operations can be catastrophic for an SME," says Nick Wilding, general manager of cyber resilience at IT best practice organisation AXELOS.

In recent years, the average SME has gone from using predominately simple siloed solutions to embracing more interconnected systems. From bring your own device (BYOD), off-site working to the cloud, small businesses have never been more connected to their clients and therefore more open to threats. So why are so many SMEs still unprepared for a cyber attack?

Mr Wilding believes that SMEs usually have markedly different priorities than larger corporations, such as maintaining a strong cash flow and ensuring the right mix of skills and expertise is retained within their small teams.

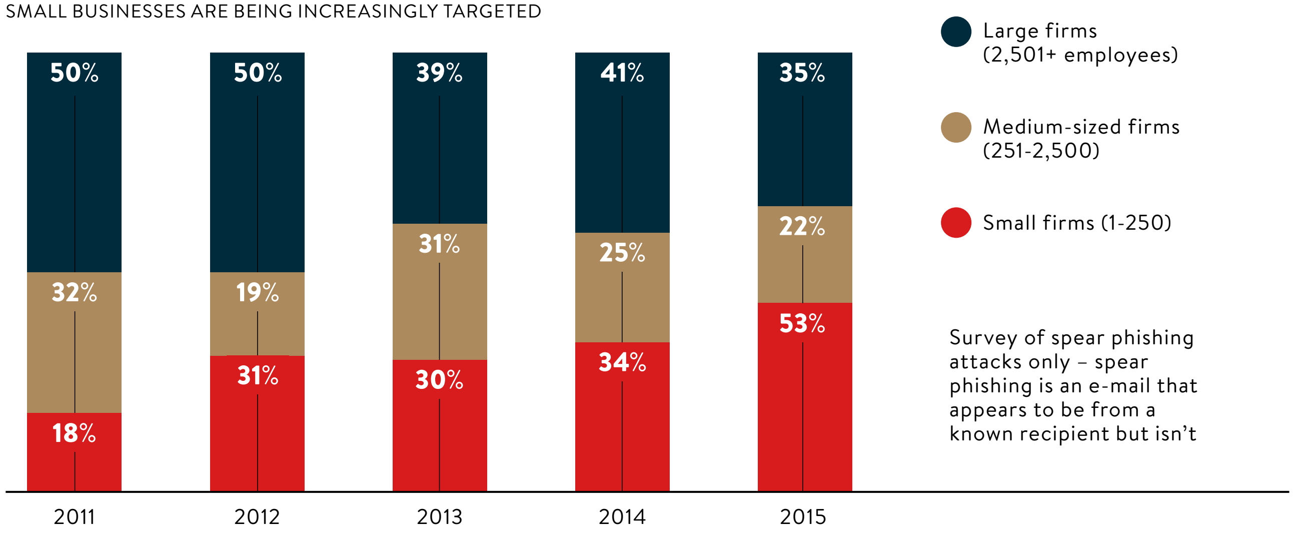
"These pressures all mean that cyber risk is often not seen as a critical business risk by SMEs. But one thing that links SMEs to large organisations is they are equally at risk to cyber attack – no one is immune," says Mr Wilding.

Patrick McLoughlin, director at marketing firm Accounting for Growth, agrees. "We take cyber risks very seriously, but as a small business we have so many different priorities to contend with, which means cyber issues aren't always at the top of the list. The problem is businesses don't take it that seriously until it's too late or you hear that it's affected someone you know," he says.

Cyber criminals are also taking advantage of the central role SMEs play in the wider economy and exploiting their online weaknesses to gain access to bigger targets. "SMEs are a growing target for hackers as they can be the pawns that lead to the 'crown jewels' within a much larger organisation. Many SMEs will be connected electronically to the IT systems of larger business partners, the companies that the cyber criminals really want to get at," says Kevin Bocek, chief security strategist at cyber security firm Venafi.

CYBER ATTACKS, BY BUSINESS SIZE

SMALL BUSINESSES ARE BEING INCREASINGLY TARGETED



Survey of spear phishing attacks only – spear phishing is an e-mail that appears to be from a known recipient but isn't

Source: Symantec 2016

27% of UK SMEs believe they are secure because they are too small to be of interest to cyber attackers

59% have been the victim of an attack

Source: Juniper Research 2016

The UK government has launched a range of schemes aimed at helping SMEs improve their cyber-security capabilities, with a recent scheme offering up to £5,000 to spend on cyber training and advice. Unfortunately, there is still a long way to go until SMEs are appropriately resilient to cyber threats. According to Barclaycard, only 15 per cent of small businesses are very confident they have adequate measures in place to defend against a cyber attack, indicating that government messages are falling on deaf ears or not being adequately amplified.

"I am not aware of any government push to advise or assist small businesses about cyber crime and how to protect against it," says Adam Tierney, ↾ managing partner at law firm Tierney & Co. "Ultimately, I think we need to be responsible for our own destiny in this respect and rely on ourselves. Paid help is out there if we can't do it ourselves, but perhaps if the government drew greater attention to the importance of cyber security and a means of getting impartial advice, this would help."

External cyber attacks are often viewed as the most pressing threats that SMEs need to protect themselves against, but an increasing number of fraudulent cyber activities are originating from within an organisation itself. Ryan Rubin, managing director at consulting firm Protiviti, believes that disgruntled staff who seek to steal company information and secrets can pose a serious danger to vital company data.

"Such events could be devastating for SMEs, for example, if their business plans or intellectual property is stolen. As there are usually key-person dependencies within SMEs, this presents a real risk to many," says Mr Rubin.

The movement towards increasing interconnectivity in businesses of all sizes can only be expected to provide new avenues for unscrupulous employees to take advantage of cyber-security weaknesses. A large number of cyber breaches are a direct result of human error, with Protiviti recently investigating a fraud committed by a finance clerk in one of their client's shared service centres. The employee had accidentally been given wider access to the client's supplier payment systems than they should have and close to £300,000 worth of unauthorised transfers were made.

Incidents like this are possible if the proper protocols for monitoring and managing user identities are not followed. Cyber criminals are now using social engineering techniques to exploit this weak link in security by tricking employees into handing over sensitive information. One method hackers use is pretending to be a supplier or client and e-mailing over what appears to be an invoice, but the attachment contains malware. These types of attacks are surprisingly effective as all it takes is a single employee to click on a link and the entire system is compromised.

> One thing that links SMEs to large organisations is they are equally at risk to cyber attack – no one is immune

"If criminals can trick the chief financial officer or finance director to transfer £20,000, with an e-mail that looks like it came from the founder, managing director or chief executive, then it doesn't matter how small a company is," says Richard Walters, senior vice president of security products at cloud business application provider Intermedia.

The ease in which cyber criminals can exploit human vulnerabilities should of course be a cause of concern for SMEs. Employees of small businesses should be aware of the methods used by cyber thieves. IBM's *Cyber Security Intelligence Index* found that 95 per cent of all security breaches involve some level of human error, highlighting the importance of educating staff in the best cyber-security practices.

"For SMEs, it's as much about education as technological solutions, as there isn't particularly a cost-of-tech barrier," says Paul Billington, managing director of digital marketing agency Prodo Digital.

Just because SMEs spend far less money and time implementing digital security solutions than major corporations, this doesn't mean that hackers are targeting smaller firms individually. "Any attacks against an SME will likely be by opportunists. There's no point in going out to get your network pen-tested, installing the latest firewalls and insisting all your staff are security-screened by MI5 if you don't work with any data that is sensitive," adds Ed Yau, Prodo Digital's head of development.

It can be difficult for SMEs to find the right balance between protecting themselves from malicious cyber attacks and creating unnecessary restrictions on employee device usage. Jon Moger, senior director at Aruba, a Hewlett Packard Enterprise company, says that while it's crucial to nurture creativity in an SME's workforce, a contingency plan should be put in place for cyber attacks.

"Inevitably, this puts a lot of pressure on IT to take an adaptive, trusting approach to device connectivity and data security," says Mr Moger. "There must be a mechanism for employees to provide feedback to IT, and a service level agreement should be in place for how to respond to employee input and requests." The success of IT policies can often be improved by simply listening to employee feedback, he adds.

With the threat from cyber criminals not expected to disappear anytime soon, SMEs need to adapt effectively to the preferred behaviour of their workforce. "Embracing the need for openness, innovation, collaboration and some degree of risk is good, but only when an organisation can understand and plan for the security risks these behaviours bring with them," Mr Moger concludes.

Share this article online via **raconteur.net**

TOP SIX SME CYBER SECURITY TIPS

01 CLOUD DATA

From Dropbox, OneDrive to Google Drive there is no shortage of cloud-based storage providers, but how safe is data in the cloud? Choosing a reputable service is of the upmost importance, but SMEs should also encrypt sensitive files before uploading them to the cloud and back up data locally or in another cloud account.

02 BYOD POLICY

Employees of SMEs are bringing their own devices into the office and using them for work projects more than ever before. BYOD may be convenient for staff, but if a comprehensive policy isn't in place that governs mobile usage, hackers can infiltrate the whole network through these unprotected devices.

03 SOCIAL ENGINEERING

Cyber criminals will try and gain the trust of an employee by pretending to be someone they're not and in the process gain access to important information. Employees should be alerted about the prevalence of social engineering attacks and told to look out for unusual requests purporting to be from colleagues or clients.

04 AUTHENTICATION

Simple passwords can be relatively easy to crack through phishing, brute-force attacks and other methods, leaving e-mail accounts and vital systems open to attack. Multifactor authentication is where a user must offer at least one more piece of evidence beside a password to prove their identity, providing another layer of security.

05 NETWORK DEVICES

An SME's network devices should be as protected as their digital assets, with unauthorised physical access easily leading to security being compromised. For example, accessible devices in office spaces should be monitored and if necessary moved to a more secure location.

06 ACCESS CONTROL

User accounts with administrative privileges should only be given to employees that have been authorised, with these special access privileges regularly reviewed. If a hacker was to get into a non-privileged account, the damage they could do is limited as they would only have the minimum level of access to the SME's systems and networks.