

# CYBER SECURITY

03

## NOW IT'S TIME TO GET TOUGH ON CYBER CRIME

Organisations have no choice but to mobilise against cyber attackers

06

## YOU MAY KNOW YOUR ATTACKER

Insider threats can be just as serious as hackers from the outside

10

## CYBER DEFENCE AS AN INVESTMENT

Canny investors can generate returns from cyber security

18

## COMPANIES CAUGHT IN THE CROSSFIRE

If governments go to cyber war, companies can become targets



# RSA

## SUMMIT LONDON

DISCOVER NEW STRATEGIES FOR SECURING MODERN IT

### 27 APRIL 2016

T: +44 (0) 1344 781613 <http://tinyurl.com/RSAsummit2016London>



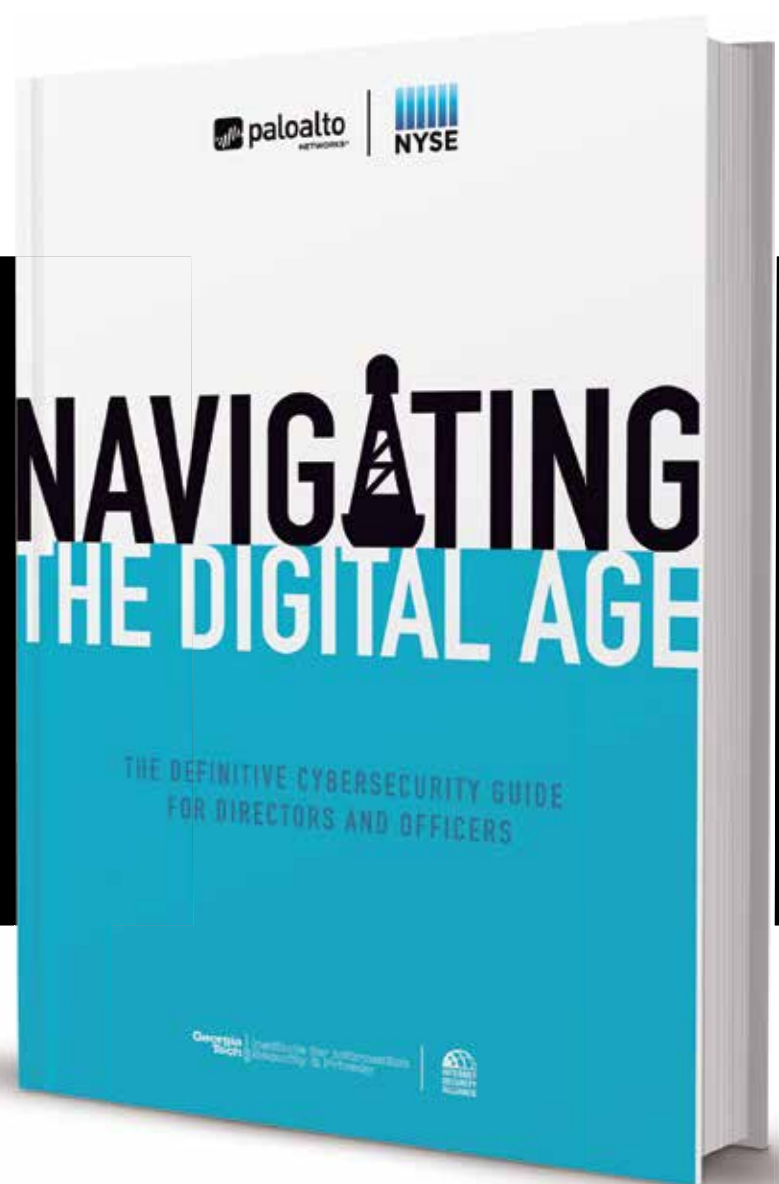
**REGISTER NOW**

# STATE-OF- THE-ART CEO. **BE READY.**

LEARN THE ISSUES.  
**MASTER THE SOLUTIONS.**



DOWNLOAD YOUR COPY &  
MORE INFORMATION ON THE LEGISLATION:  
[go.paloaltonetworks.com/regulation](http://go.paloaltonetworks.com/regulation)



New EU legislation around NISD (Network Information Security Directive) and DRR (Data Protection Regulation Reform) are advancing, with state-of-the-art cyber risk accountability becoming businesses' top priority. Take the appropriate, preventive steps to effectively implement the state-of-the-art security necessary to protect your business. Meet these needs with guidance from *Navigating the Digital Age*, the definitive cybersecurity guide for boardroom members and executive officers. Developed in collaboration with the New York Stock Exchange and Palo Alto Networks, it provides practical, actionable and expert advice on best practices for compliance, implementation, breach prevention and immediate response tactics.

Includes venerated voices such as:

- Visa
- The World Economic Forum
- Internet Security Alliance



# CYBER SECURITY

DISTRIBUTED IN  
THE  TIMES

RACONTEUR

PUBLISHING MANAGER  
**Michael Kershaw**

PRODUCTION EDITOR  
**Benjamin Chiou**

MANAGING EDITOR  
**Peter Archer**

HEAD OF PRODUCTION  
**Natalia Rosek**

DIGITAL CONTENT MANAGER  
**Sarah Allidina**

DESIGN  
**Samuele Motta**  
**Grant Chapman**  
**Kellie Jerrard**

CONTRIBUTORS

**DAN BARNES**  
Award-winning business journalist, he specialises in financial technology, trading and capital markets.

**DANNY BRADBURY**  
Freelance technology writer, he contributes to the *Financial Times* and *The Guardian* on topics ranging from computer networks to cultural issues.

**ANTHONY HILTON**  
Author, journalist and broadcaster, he is a former City editor of *The Times* and managing director of *The Evening Standard*.

**CHARLES ORTON-JONES**  
Award-winning journalist, he was editor-at-large of *LondonLovesBusiness.com* and editor of *EuroBusiness*.

**STEPHEN PRITCHARD**  
Technology, telecoms and science writer, he contributes to the *Financial Times* and *The Independent on Sunday*.

**STEVE RANGER**  
Editor-in-chief of *ZDNet* and *TechRepublic UK*, part of CBS Interactive, he has also worked for *Computing* magazine.

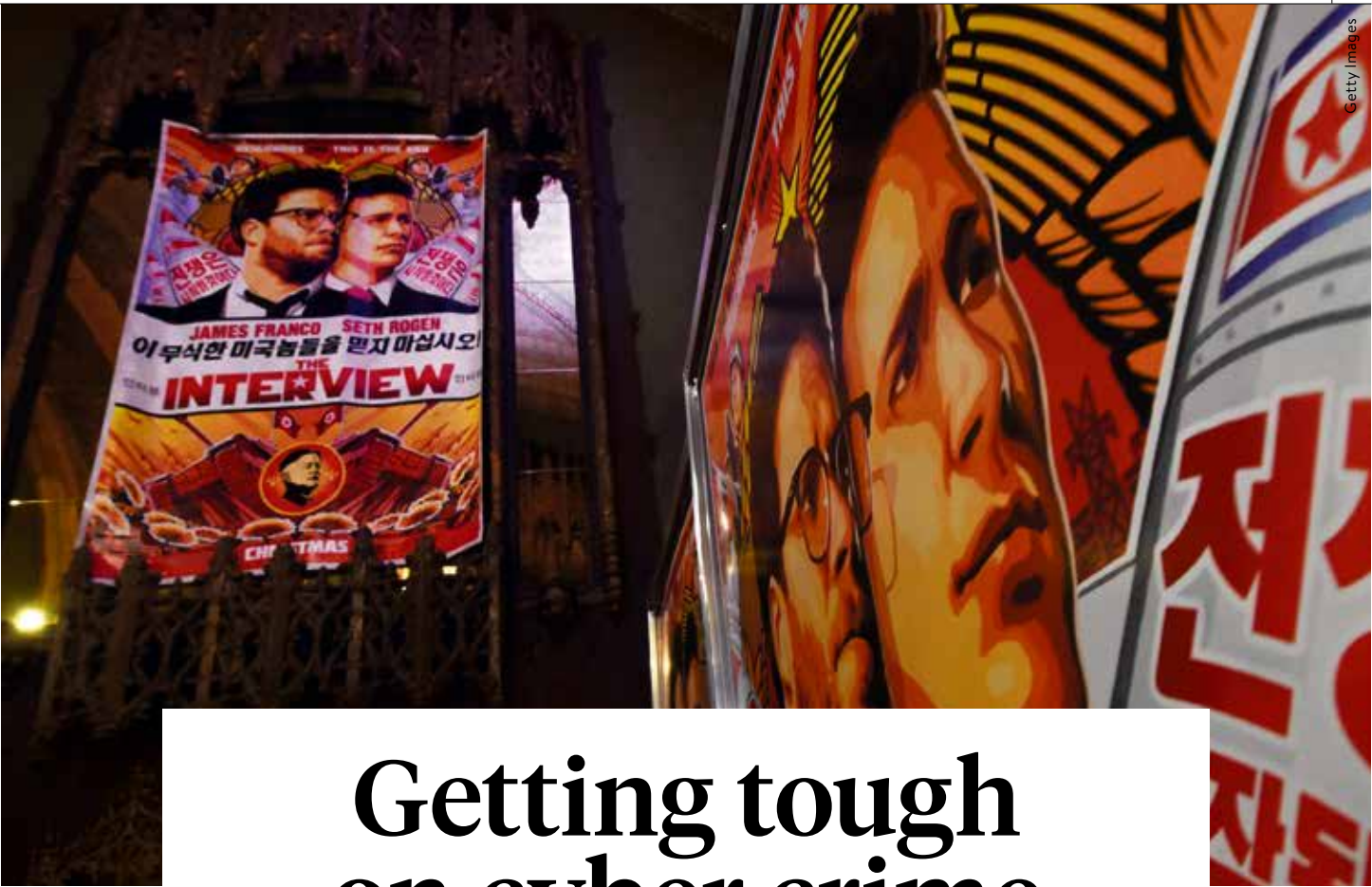
**GIDEON SPANIER**  
Head of media at advertising magazine *Campaign* and Broadcasting Press Guild chairman, he writes about business for the *London Evening Standard* and *The Times*.

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

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) 208 616 7400 or e-mail [info@raconteur.net](mailto: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, health-care, lifestyle and technology. Raconteur special reports are published exclusively in *The Times* and *The Sunday Times* as well as online at [raconteur.net](http://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



# Getting tough on cyber crime

Faced with an increasingly powerful and organised enemy, organisations now have no choice but to mobilise in the fight against the cyber attackers

Sony Pictures was hacked in 2014 by a group demanding the cancellation of *The Interview*, about a plot to assassinate North Korean leader Kim Jong-Un

OVERVIEW

ANTHONY HILTON

An unsuccessful American thief Willie Sutton was asked in court why it was that he robbed banks. His answer secured his place in history. He robbed banks he said “because that is now changing, the banks were the primary target.

Cyber criminals took this message to heart. In the past 30 years, cyber crime has evolved from the province of the amateur hacker in a suburban bedroom into a sophisticated organised international industry with its own supply chain of employers, contractors and specialist sub-contractors. From the beginning, though that is now changing, the banks were the primary target.

Banks have been forced to spend hundreds of millions of pounds on additional defences and to set up a system to pool information to aid the fight against this invisible yet highly dangerous enemy. But the fact that they were the obvious target bred complacency elsewhere. Mainstream non-financial businesses could be heard to say they had nothing much that anyone would want to steal. They did not think cyber was a major threat to them.

But this has changed. A succession of high-profile events, from the attack on Sony Pictures alleged to have come from North Korea to the loss of data at the mobile phone provider TalkTalk, cyber attacks are rarely out of the news. And with that has come a new realisation. It is often

not the actual theft of data which is the real cost to the company, it is the much longer lasting damage to the firm’s reputation, and to customer and investor confidence.

Such attacks cast a shadow over the competence of management; they raise doubts about the adequacy of controls; they precipitate a host of reputational and trust issues which can linger for years.

Months after the attack, the stock market value of TalkTalk was still almost £1 billion less than on the day the attack was announced.

So it was perhaps no surprise, but nonetheless welcome, that reports, circulated at the January World Economic Forum of business leaders in Davos, reflected a change of mood. The big change for 2016 is that everybody is now concerned.

And so they should be. A survey published last year by the Centre for Economics and Business Research put the annual cost of cyber crime in the UK at £34 billion, split not quite evenly between the costs resulting from the attacks and the costs of the extra spending on prevention.

Striking in a different way were the results of the annual *Information Security Breaches Survey*, prepared

by the business services group PwC for the Department for Business, Innovation & Skills. The 2015 version found that 90 per cent of large companies and 74 per cent of small companies had experienced some kind of breach in the last 12 months. But many displayed an alarming amateurishness in the way they defended themselves.

Interestingly getting on for half of these breaches were the result of internal lapses by employees, which underlines an important point. Many successful external attackers rely on an employee doing the wrong thing – something as simple as opening an e-mail attachment from an unfamiliar source – to gain their initial entry.

We should also dispel the myth that all the attacks are about money. Cyber specialist at PwC, Richard Horne, makes this point strongly. He divides attacks into four distinct categories:

- Attacks instigated by agencies of government or sophisticated terrorist groups which are seen as a way to make their presence felt without resorting to force of arms;
- Attacks originated by criminals whose interest usually is money or blackmail leading to money;

- Attacks for information, which are the modern version of industrial espionage where the objective is the theft of intellectual property or other economically valuable commercial secrets – suppliers and customers, contract terms, new product development and so on. And it may not be an organisation’s own data which is the target as some are attacked to get data on third parties with whom they do business;
- Attacks by rogue employees, some who are disgruntled and want to cause trouble, and others who believe they are fulfilling some higher purpose by whistleblowing.

The challenge for companies now they increasingly appreciate the scale of threat is to know what to do about it. There is no shortage of offers to help; there are thousands of companies offering cyber defences and more starting up every day. But as with all new industries which attract a flood of entrants, the majority will not survive, so the issue is less about who has the most attractive offer today and more about who has the resilience to be a long-term partner.

There is no simple way to solve this problem, but perhaps the best approach is to understand from the beginning that effective defence rarely comes cheaply. Cyber security is not simply today’s issue – it is one of the major business challenges of the next decade.

 Share this article online via Raconteur.net





# Limiting damage to protect reputations

Reputation can be the biggest casualty in a cyber attack, evidenced by high-profile resignations of company executives and plummeting share prices in the aftermath of a data security breach

BRAND REPUTATION  
GIDEON SPANIER

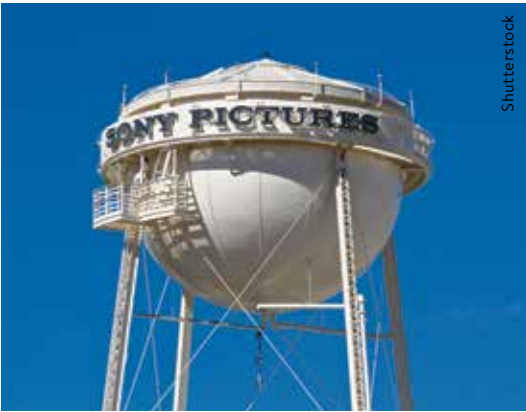
The main way that most companies interact with their customers and clients is now online, so a reputation for cyber security is integral to doing business and their brand.

Every company has regarded the threat of an IT failure as one of its principal risks for some time, but fears about wider cyber problems such as a data breach and online fraud have shot up the agenda in the last 12 to 18 months.

Andrew Griffin, chief executive of Regester Larkin, an agency that specialises in strategic crisis management, says: “The series of recent high-profile hacks and data breaches has bumped cyber resilience and preparedness up from an IT department-only issue to high on the executive team agenda.”

Emma Kane, chief executive of Redleaf Communications, a public relations agency, agrees: “Companies are increasingly concerned about the reputational damage that cyber crime can cause. It’s potentially incredibly damaging. In the most severe cases it can lead to a real lack of confidence in the integrity of a company and its ability to keep data safe.”

Johnny Hornby, founder of WPP-backed communications group The&Partnership, says the threats have also multiplied. “Today’s environment is radically different from that of just five years ago, when businesses were only targeted if they held a large and substantial prize,” he says. “Nowadays, opportunists armed with the digital equivalent of a set of lock picks and a crowbar may attempt an attack. So it’s critical that businesses of all sizes continually review the locks on their doors and the transparency of their windows.”



150,000 customers was compromised, although the breach was not as bad as it initially feared. However, the telecoms firm’s reputation took a pounding as it emerged that teenage hackers had breached the website with ease. TalkTalk’s share price fell and it lost customers.

Sony Pictures’ website and e-mail hack in November and December 2014 illustrated how cyber-security threats are also international, and potentially even state-sponsored, as North Korea was suspected of targeting the film studio in retaliation for a movie that lampooned the country’s leader Kim Jung-Un.

The leaked e-mails were embarrassing for Sony in Hollywood circles as they revealed that some of its senior executives had been privately bad-mouthing the stars and producers involved in some of its films. Parent company Sony’s share price fell nearly 10 per cent and, although it bounced back, Amy Pascal subsequently departed as co-chairman of Sony Pictures Entertainment.

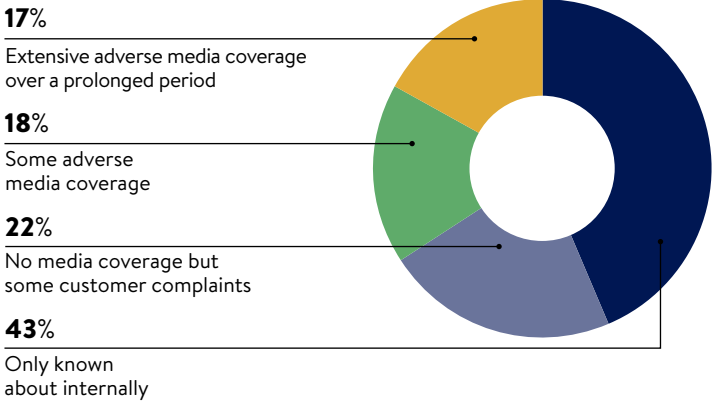
Investors might be willing to

Companies have taken heed after watching three recent cyber crises unfold – the hacking of customer information at telecoms firm TalkTalk, a major e-mail leak at Hollywood studio Sony Pictures and a data breach at American dating website Ashley Madison. In all three cases, there was a knock-on effect on the brand, customers and clients, and the share price.

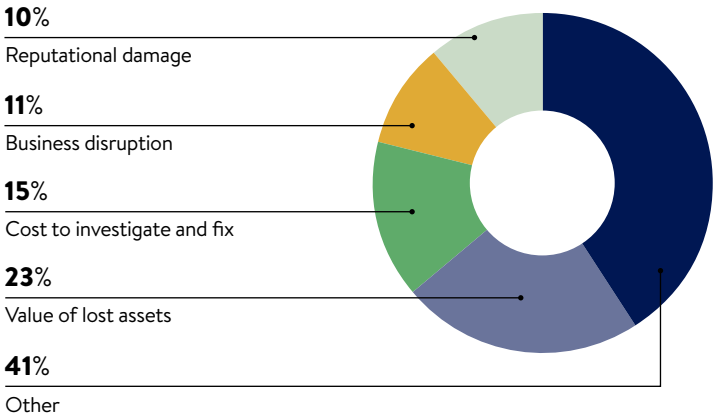
When TalkTalk’s website was hacked in October 2015, personal information belonging to more than

## TO WHAT EXTENT DID YOUR WORST CYBER ATTACK DAMAGE COMPANY REPUTATION?

SURVEY OF LARGE UK ORGANISATIONS



## WHAT MADE THIS INCIDENT THE WORST OF THE YEAR?



Source: PwC 2015

forgive a single data breach, but recurrent problems at the extra-marital affairs dating website Ashley Madison forced its chief executive Noel Biderman to resign in August 2015.

He was already under pressure because details of the website’s 37 million users were stolen and dumped online, and then his personal integrity came under fire because leaked e-mails raised questions about his own marital behaviour. The share price of parent company Avid Life

Media has halved since the data breaches emerged and Ashley Madison is facing the prospect of multiple legal cases.

Other companies from the BBC to Twitter have seen their websites get “taken down” in recent years by a so-called distributed denial-of-service (DDoS) attack, where multiple systems flood a targeted asset, rather than try to steal information.

Mr Griffin says: “DDoS or a data breach can have significant commercial impacts on an organisation, including loss of customers, significant recovery costs, loss of intellectual data and service disruptions. But the impact can also be reputational.”

Little wonder, then, that many businesses are now keen to improve their cyber defences and to prepare for the next possible crisis.

Tim Burt, UK managing partner of Teneo Strategy, the international advisory firm, says businesses must conduct regular audits of security measures and adopt the latest protective digital tools. “Companies whose reputations are particularly vulnerable to any breach should conduct ‘war games’ to prepare for the various crisis scenarios that arise following a breach,” he says.

Mr Griffin points out cyber security “is often unfamiliar territory” in the boardroom. “It presents new and unique challenges, requiring

## CASE STUDY: TALKTALK



TalkTalk’s cyber breach in October 2015 has been carefully studied by other companies as a case study on what to do and avoid in a similar crisis.

The telecoms company’s chief executive Dido Harding impressed some observers because she led from the front in interviews in which she candidly warned that millions of her customers’ data could have been affected.

TalkTalk temporarily suspended its sponsorship of *The X Factor* on ITV and switched its advertising to alert customers about the cyber breach.

However, Ms Harding soon came under fire when it emerged it was teenage hackers, not sophisticated criminals, who had got past TalkTalk’s weak online defences and that the cyber-breach was not as bad as she had first suggested.

More than 150,000 customers were still affected, but the damage to brand and reputation was greater. The company’s share price fell by a

third, it took a near-£80 million hit in costs and lost revenue, and 100,000 customers quit.

Tim Burt, UK managing partner of Teneo Strategy, says: “The company’s over-reaction, taking to the airwaves to claim it may have been a victim of cyber terrorism, exacerbated the consumer reaction.”

But Johnny Hornby, founder of communications group The&Partnership, which advises

TalkTalk, believes the telecom company did the right thing.

“Even if there is short-term pain, it’s better to be open and transparent from the outset in the event of an attack,” he says. “Dido Harding’s response during the TalkTalk cyber attack was a great example of this. She responded quickly and openly to both her customers and the media, put her customers first and resisted the temptation to spin a story.”

different functions and teams, such as the advent of the cyber incident response team or CIRT, to collaborate and manage the complexities of a cyber response.”

Mr Hornby, who worked with TalkTalk during its recent crisis, says a cyber breach doesn’t have to be devastating for a company’s reputation. “Customers put their trust in brands, but customers also live in the real world and I think understand that new threats like cyber attacks will happen,” he says. “What’s key for a brand is how it deals with such an attack, and how openly and transparently it communicates with its customers. A big challenge nowa-

days is the 24/7 media agenda, which demands answers immediately. Cyber crime is often complex and the extent of it is hard to define in an instant.”

Mr Griffin agrees that it is critical to communicate clearly and quickly to protect a company’s brand and reputation. “If you are perceived to act too slowly or with uncertainty, you can quickly lose the trust of your stakeholders, including shareholders and customers,” he says. “The timing of your communication and notification to customers and regulators is critical in a cyber incident.”

He says a company should have three priorities which he describes as “containing the issue, putting their customers first, and positioning themselves as the authoritative source of information”.

Ms Kane warns that a company needs to try to plan for every eventuality, including that a cyber hack or DDoS may knock out its own website or IT systems that are normally used to communicate. “Companies should prepare alternative channels for communicating to their stakeholders,” she says.

Experts also believe it is vital to conduct a post mortem in the wake

of any cyber-security breach. As Ashley Madison showed, customers and stakeholders will not tolerate repeated problems.

Mr Griffin says: “Companies must undertake a post-incident review to ensure lessons are identified and learnt. While many organisations are now implementing cyber-crisis preparedness programmes, the cyber ‘plans and playbooks’ are still evolving. We are yet to see the textbook response to a cyber incident come to the fore. But with every crisis, new lessons are learnt.”

Mr Burt adds: “The companies getting it right are the ones you don’t hear about – if you’re in the news because of a breach, it’s already too late.”

Mr Hornby spends much of his time advising clients on their communications and reputation, but he also believes it is vital that his company keep its own house in order.

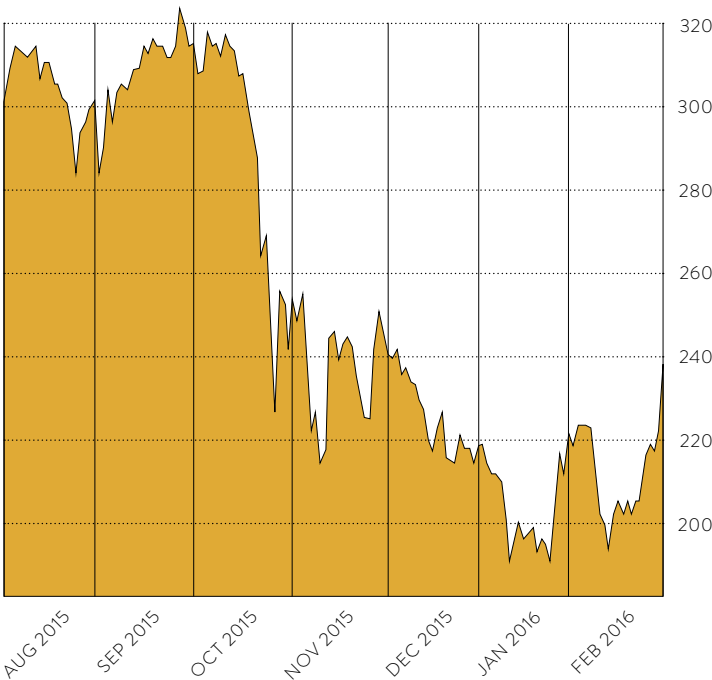
The&Partnership owns data subsidiary Rapier and Mr Hornby says it consistently reassesses its internal policies and systems to stay ahead of the curve on cyber security.

He has urged his own industry, advertising, to tackle the growing problem of ad fraud and fake views by computer robots. “It isn’t just about spend wasted on advertising that never gets seen by a human. Ad fraud damages brands,” he says. “It’s not hard to find examples of this – for all the work our industry does to build brands, it’s alarming how many of those brands’ content can be found on pornography and other deeply unpleasant websites.”

The battle against cyber crime is now an ongoing cost of doing business. As Mr Burt says: “Constant vigilance is required.”

“The companies getting it right are the ones you don’t hear about – if you’re in the news because of a breach, it’s already too late

TALKTALK SHARE PRICE (p)  
INVESTOR SENTIMENT WAS DAMAGED BY THE CYBER ATTACK ON THE TELECOMS FIRM IN OCTOBER 2015



# REPEL THE HORDES OF HACKERS...

*Moving to a secure managed network can defeat the cyber criminals trying to break into your systems*




The scale of malware threats is more than growing – it is exploding. In 2014 nearly six million malware strains were identified.<sup>1</sup> There have been 1,800 new distinct families of viruses detected in the past year alone.<sup>2</sup> Kaspersky Labs identified 12,100 new Trojans in mobile banking, up nine fold on the year before. The cost of a breach is huge – latest figures put the average value at \$3.79 million.<sup>3</sup>

The message is clear: you have to do everything you can to protect your organisation and customers. Most companies take the old-fashioned approach to security. This involves anti-virus software, a firewall and intrusion detection. But with attacks increasing at this rate it simply won’t cut it. Intruders will find their way in sooner or later.


Fortunately there is another approach. Move to a secure network and the vast majority of threats can be neutralised before they get anywhere near your firewall.

“The analogy we use is home security,” says Kathy Schneider, Level 3 senior vice president product and marketing in Europe, the Middle East and Africa. “Do you want criminals at your door, looking through your peep-hole? Or do you want them kept as far away as possible?”

Level 3 introduces four new elements to security. The first is prediction. Level 3 monitors its global network to know where malware is coming from and which patterns are emerging. It’s not easy work. Analysts at the Level 3 intelligence laboratory monitor 1.3 billion security events a day, witnessing more than one million



**\$3.79m**  
average total cost of a data breach in 2014  
Source: Ponemon Institute



**1.3bn**  
security events monitored by Level 3 each day

malicious packets, in order to make accurate predictions.

The second element is detection. The insights gleaned from monitoring the network mean Level 3 can spot sophisticated attacks and find the best ways to stop them.

Third is alerting customers. Level 3 will notify customers of key threats and provide a summary of what action has been taken to defeat them. Any requirement for further action can be decided.

And last is the extra element of security which is introduced by using a rigorously policed network. Data is scrubbed before it gets anywhere near the corporate firewall. This multi-layered approach is proven to reduce the chances of viruses, Trojans, spyware or any other malware from slipping through.

“Security used to be about repelling a handful of unsavoury characters

from your corporate data,” says Ms Schneider. “Now it’s like a horde of barbarians running at you.”

The threat escalation means many chief information officers (CIOs) can’t handle the issue alone. CIOs are already having to run their business-as-usual operations with flat or reduced budgets, while figuring out how to deliver innovation. This makes it hard to also build an expertise in security – a challenge that’s constantly growing and changing.

“CIOs are having to decide if they want to focus on innovating for their business model, product and customers, or on becoming a security expert. Put like that it really makes sense to move to a secure managed network,” says Ms Schneider.

Switching is quick. A DDoS mitigation service by Level 3 can be implemented within 24 hours. Other services can be adopted when needed, including a full outsourced security service.

Ms Schneider concludes: “My message to CIOs is to ask your current security provider if they are monitoring and cleaning traffic at the network layer? Do they have an intelligence lab predicting global threats around the clock? Are they tracking a thousand malware command-and-control centres. If not, then we’d love to speak with you about Level 3’s capabilities.”

To find out more visit [level3.eu.com/emeasecurityuk](http://level3.eu.com/emeasecurityuk)  
<sup>1</sup>G DATA Software AG, G DATA SecurityLabs Half-Year Malware Report, July–December 2014  
<sup>2</sup>Fortinet Threat Landscape Report  
<sup>3</sup>Ponemon Institute/ IBM, Cost of Data Breach Study: Global Analysis, May 2015



## INSIDER THREATS

DANNY BRADBURY

Cyber criminals must work hard to get hold of your data, but employees and others inside your company typically have privileged access to it. So just how dangerous are insider threats and what can we do about them?

Don't limit your perception of insider threats to just financial fraudsters, experts warn. They're certainly a risk, but there are others too, says Andrew Rogoyski, vice president of cyber security services at IT firm CGI and chairman of the cyber security group at UK technology industry group TechUK.

Insider threats break down into two broad groups – the malicious and the unwitting. Malicious actors may do more than steal money, Mr Rogoyski points out. Intellectual property theft is a potential problem, especially for companies based in knowledge industries. Plans for mergers and acquisitions, product designs and sales targets could all be at risk.

"There might also be sabotage; there might be people wanting to disrupt an organisation's ability to perform its work," he says. That could range from installing malware through to deleting files.

Sometimes, fraud and sabotage can overlap. In September, AT&T sued several former employees for installing malware on its networks. That was a form of sabotage, but for financial gain because the software enabled a local business to unlock customers' phones automatically.

Uneducated employees are just as threatening as malicious insiders, though. These are the workers who take sensitive company data home on thumb drives and lose it or accidentally post it online, potentially costing their employer untold amounts in legal fines and reputational damage. They don't mean to do it, but a lack of training and oversight can turn them from assets into liabilities.

There is one other kind of insider, warns Ian Beale, audit and compliance principal executive adviser at CEB, a membership organisation which advises on best practices and technology. Insider threats cover anyone with priv-



# You may even know your cyber attacker

Companies are increasingly worried about cyber attacks by shadowy criminals halfway around the world, but a greater enemy may lurk within

ileged access to company data, he explains, and this group has expanded as working practices have changed.

"It includes both full-time and part-time employees and contractors, either of whom can work remotely, at home or be travelling," he says. Insider threats can even extend to the digital supply chain,

where third-party contractors may in turn subcontract operations to others who then have access to your data.

These companies and individuals represent real threats. In November 2013, US retail giant Target lost 40 million credit card numbers after hackers infiltrated its systems. It later transpired that

the cyber villains infiltrated the company via hacked accounts at a third-party heating and air conditioning company which Target had contracted and had access to its network.

So there are many more kinds of people inside your IT systems, with potentially different motives, than you may think. How can you protect your valuable data from them?

The temptation is to watch everyone like a hawk, imposing strict controls that hem workers in. Beware, warns Mr Rogoyski. "That can have a damaging effect on morale and loyalty," he says. "You can create disaffected, disgruntled employees."

Rowena Fell, cyber and insider threat director at consulting giant EY, recommends a data-driven ap-

**01** Cyber attackers stole credit card numbers of Target's customers in 2013, gaining access through the retailer's third-party heating and air conditioning company

**02** AT&T sued several former employees in September 2015 for installing malware on its networks



“

Insider threats can even extend to the digital supply chain, where third-party contractors may in turn subcontract operations to others who then have access to your data

proach to insider threats, rather than simply scrutinising employees. "It's about protecting your critical information and trade secrets," she says.

Understanding where that information resides is a crucial early step in an insider threat prevention programme. This can drive initiatives that help to prevent different varieties of insider threat.

Managers can reduce accidental insider threats with an effective education and awareness programme to help prevent mistakes such as responding to fraudulent e-mails or taking valuable data out of the company. These should be a marathon, say experts, and not a sprint. Forget short-term awareness projects that people will forget. Instilling a culture of diligence into an organisation is a long-term process, perhaps backed up with exercises to test its effectiveness.

That still leaves malicious insider activity to deal with. "Organisations have to acknowledge that they may have a potential problem, and begin to put in place adequate procedures and checks on anyone who might need to gain access to data and systems," says Alex Stedmon, reader in human factors at the University of Coventry, who studies how psychology and security interact.

Companies should review users' access rights and refine them based on current activities, Dr Stedmon advises. Insiders should be able to see and do only those things that are essential for their jobs.

In some cases, companies can use IT systems to separate duties, meaning that no single person can approve a particularly critical operation, such as moving money above a certain threshold out of the company.

Proper vetting of employees can also be a useful way to prevent insider fraud, says Mr Rogoyski. This is common in government and is beginning to appear in commercial organisations, he adds. Managers should be asking their human resources departments how much due diligence they're doing on new employees beyond contacting references on a CV.

Insider threats are a clear and present danger, whether employees are disgruntled or not. If you haven't reviewed the dangers and created a strategy for dealing with them, now's the time. It's best to prevent the threat, rather than deal with the fallout afterwards.

## HOW TO SPOT A FRAUDSTER



Malicious insiders try to make themselves invisible, but they're often like black holes – even if you can't see them directly, you can look for evidence of their existence. Technology can help here, as

can a keen nose for discontent. "At a personal level, you need to start looking for what the textbooks would call a precipitating event," says Andrew Beckett, managing director in the cyber security

and investigations practice at risk solutions company Kroll. These are incidents that might spark revenge. Has an executive been passed over for promotion, demoted or disciplined?

These incidents can be analysed along with other signals, including personality traits. "You can look at psychological behaviour and general attitudes at work," he adds. "Some people just carry a chip on their shoulder."

Historical behaviour can provide clues. Have employees regularly complained about security at work or disabled security features that might have been put on the system?

If these signs are missed or missing, you can use technology to help you uncover potential fraud. Workflow systems can be configured to double-check the legitimacy of invoices or confirm that the amount paid was the amount asked for.

Beyond that, more sophisticated baselining systems can be put in place which analyse legitimate behaviour on your computer systems and then look for anomalies. Such anomalies might have a perfectly reasonable explanation, but you won't know about them unless you have software in place to alert you when they happen. At the very least, it will prompt you to ask some polite questions.

COMMERCIAL FEATURE

# C-SUITE MUST COLLABORATE ON CYBER SECURITY

*UK firms cannot combat cyber attacks without boardroom collaboration*

Companies are a work in progress when it comes to cybersecurity, an IBM study has found.

Following the survey of more than 700 C-suite executives in 28 countries on cyber security, IBM UK managing partner Greg Davis says what stood out for him was how the majority of organisations are still not managing security as a business risk.

“Security is not going away and is not a problem you fix once and forget, it is a business risk that needs continued mitigation and management in the same way as more traditional and established business risks,” he says.

Although the survey found that 68 per cent of C-suite executives view cyber security as a top concern and 75 per cent believe a comprehensive plan is important, IBM only classified 17 per cent of respondents as “cyber-secure”.

“There is a broad spectrum of cyber-secure maturity levels across companies in the UK. In general, the more regulated the industry, the more cyber-secure they tend to be. However, even more mature companies lag behind the latest thinking in terms of managing cyber risk,” says Mr Davis.

“In the financial services sector, you’ll generally find clients have to be more secure, they are at the top end of the spectrum, but as you come further down the curve you’ll find some industries are lagging in terms of investment and understanding of how to address the cyber-secure challenges.”

IBM’s global head of cyber security intelligence Nick Coleman points out that recognising security as a concern isn’t enough, it is about how that translates into practical solutions in the boardroom.

“Yes, a lot of senior leaders recognise the importance, but then as we start to drill down into the details, the question is really what to do practically? For example, 57 per cent of the HR officers have rolled out employee training – so nearly half haven’t. This is where cyber security gets put to the test,” he says.

While most C-suite executives are aware of how important cyber security is to their organisation, they are still confused about just who their companies are fending off and how to keep themselves safe. More than two-thirds of the respondents thought that rogue individuals were the

biggest threat, but a United Nations report recently found that 80 per cent of cyber attacks are driven by highly organised crime rings.

And although many C-level executives realise that collaboration across industry is necessary to defend against cyber crime, there’s a lot of reluctance when it comes to sharing their own information. Over half of chief executives agreed that more industry collaboration was needed and 53 per cent want cross-border information-sharing. But only 32 per cent of them were willing to share information about incidents externally.

However, this should be helped by new efforts from the UK government and European Union. “The government has been involved for some time in trying to help companies to share information through the Cyber Security Information Sharing Partnership (CISP), to which a number of companies have signed up,” says Mr Davis.

“The Network and Information Security Directive out of Europe is a good example of regulation where, as it’s emerged, it’s looking in good shape to help drive security up not just in the UK, but in Europe and beyond,” Mr Coleman adds.

And beyond regulation, there’s much that companies can be doing now to put themselves in the cyber-secure category. IBM found the leaders that were heading up the most secure firms had made IT security a regular agenda item for board meetings and were making sure all the C-suite were involved, not just chief information security officers (CISOs) and chief information officers (CIOs).

In the study, 77 per cent of chief risk officers and 76 per cent of CIOs reported that their organisations’ cyber security plans were well established. But only slightly more than half of chief executives agreed and the chiefs of marketing, finance and human resources were similarly sceptical.

CIOs and CISOs may be feeling confident in their technical measures to combat cyber crime, but they need to accompany that with business risk management from the other executives. Almost 70 per cent of respondents acknowledged that their plans failed to incorporate adequate C-suite collaboration across the board, with many executives feeling left out of the cyber security process.

## Securing the C-suite

Perspectives from the boardroom and C-suite

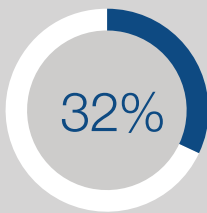
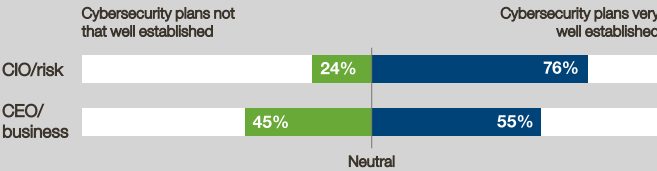
### The CEO dichotomy

Well over 50% of CEOs agree more external collaboration is needed to combat cybercrime, but less than one-third are willing to share their own information externally.



### The confidence paradox

IT and risk are more confident cybersecurity plans are well established than the CEO and business executives.

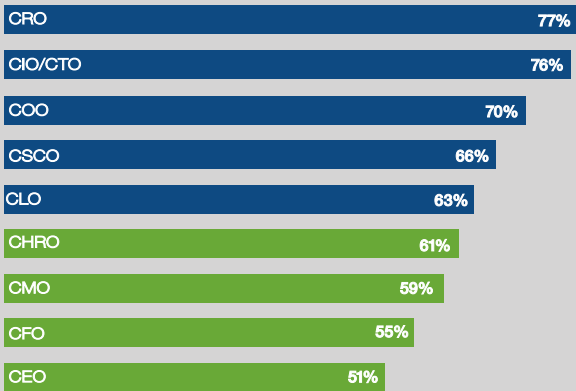


CEOs willing to share incident information externally

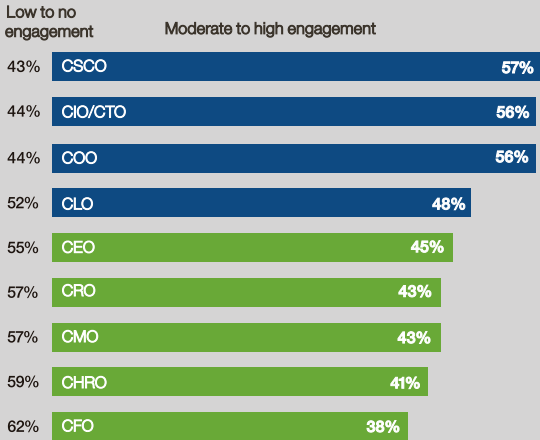


The C-suite is far more confident in the level of cybersecurity preparation than reality - or their own responses to detailed questions - would indicate.

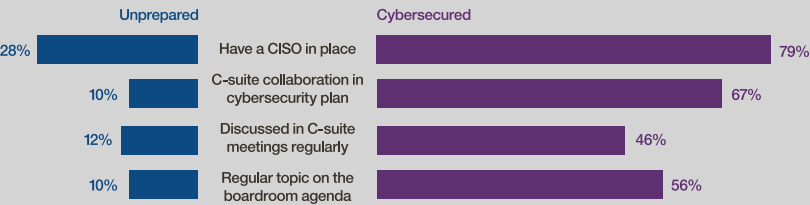
### Percent of C-suite that believe their companies' cybersecurity plans are well established



### Percent of C-suite highly engaged in cybersecurity threat management activities by role



### Being cybersecured



The significant factors that differentiate the cybersecured from the rest

- Having a CISO
- A plan that emphasizes C-suite collaboration
- C-suite level engagement and
- Transparency up to the board

To obtain your free copy of the full report, download the C-suite cybersecurity study - "Securing the C-Suite" [ibm.biz/csuitesecurity](http://ibm.biz/csuitesecurity)

To learn more about how IBM works with organizations to secure their digital infrastructure, please visit [ibm.biz/security\\_uk](http://ibm.biz/security_uk)

©2016 IBM Corporation GBU0084USEN-00

Keeping the cyber security conversation technical bars key executives from participation and this is particularly worrying for marketing, finance and HR. In the study, 57 per cent of chief marketing officers, 59 per cent of chief human resources officers and 62 per cent of chief financial officers said they were not involved in the topic of cyber security. But these sections of the business



Those firms that IBM considered cyber-secure were making C-suite collaboration a priority, as well as keeping cyber security regularly on the board’s agenda

hold the data that is most coveted by cyber criminals – customer, employee and financial information.

Those firms that IBM considered cyber-secure were making C-suite collaboration a priority, as well as keeping cyber security regularly on the board’s agenda. Every board member doesn’t need to become an IT expert, but they should know enough about the cyber security risks the firm faces to understand and monitor the controls in place.

To stay secure, firms need to evaluate the risks they face based on their industry, geography and ecosystem, and focus security on the risks to the key assets. It’s inevitable that people will, for example, click on links in e-mails, says Mr Coleman, but good organisations are mitigating some of the risk by doing annual training in conduct and

ethics to help employees understand the risks. They also have processes in place to deal with the situation when people do click on a malicious link or see something malicious.

Mr Davis says that in his experience, the UK and Europe generally are relatively sophisticated in their cyber security maturity, but being in the top quadrant shouldn’t make British firms complacent.

Mr Coleman concludes: “The UK has spent quite a lot of money and addressed it earlier than other countries, but there are large-scale breaches in the UK, the same as anywhere else. And large, sophisticated breaches are happening increasingly, which means we’ll have to continue to raise our game.”

[www.ibm.biz/security\\_uk](http://www.ibm.biz/security_uk)



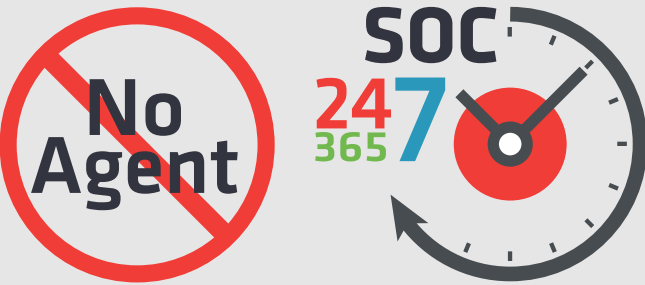


Precise Threat Detection  
and Remediation

DON'T  
PANIC



Rapid Incident Response  
Automated Detection and  
Elimination in as Little as 2 Hours  
Call +44 203 287 0999



www.cynet.com



# Catching hackers is not

Law enforcement agencies are fighting a tough battle against carry on hacking, but the bad guys can make mistakes and there

DETECTION  
CHARLES ORTON-JONES

The police made two big arrests in February. A Glaswegian 15 year old was hauled off for allegedly hacking into the FBI's systems. And just days earlier another British teenager was detained on charges of hacking the AOL account of the director of the CIA.

The arrests raise the question of how the police and cyber detectives catch hackers. Because before you can catch a hacker and create strong defences, it is vital to know how the cyber criminals work. Fortunately many former officers and security companies working with the police are willing to share at least some of their secrets.

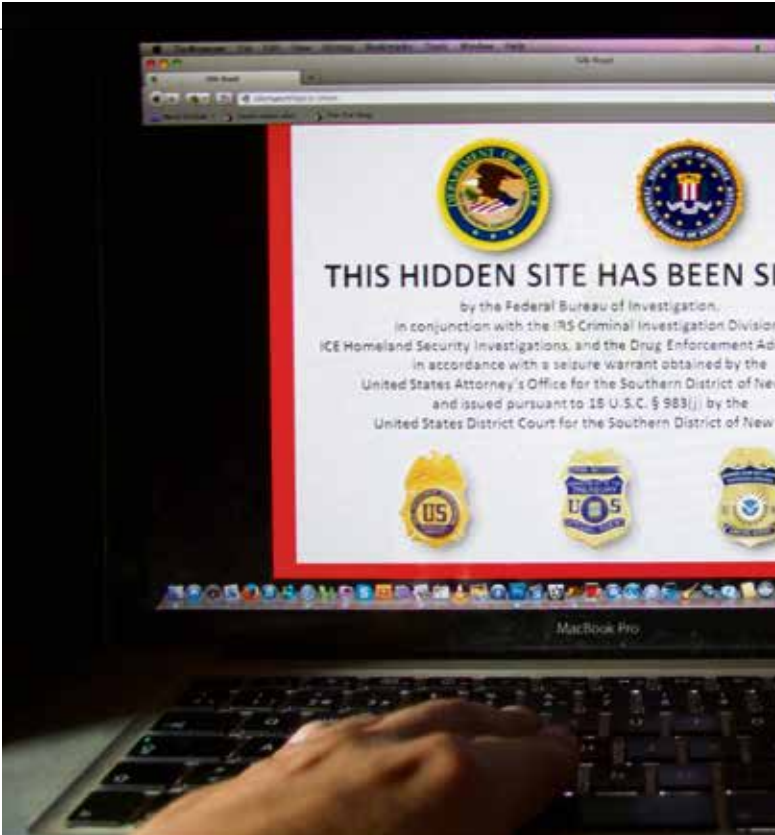
First up, catching a hacker is very, very difficult. Even a novice can hide their identity using "obfuscation" technologies. Leo Taddeo, a former New York FBI special agent in charge of fighting cyber crime, explains the problem. "Hackers use tools to disguise their IP address," he says. "Other technologies like Tor and encryption add other layers to make it difficult to identify them. These tools are widely available. They make it a resource-intensive and time-consuming task to find hackers."

Obfuscation tools are free and legal. They bounce traffic off multiple servers around the world. Furthermore, hackers will use only encrypted communication methods, and hide their activities using euphemisms and codewords. From this perspective, perhaps it's a miracle the police catch anyone.

So how do police manage it? Mr Taddeo says it's often a case of waiting for a perpetrator to slip up. "99.999 per cent of the time it is down to a mistake," he says. "Criminals are lazy or sloppy. They may not configure a tool correctly. They are unaware they are leaving a trail for law enforcement officers."

Greg Day, Palo Alto Networks chief security officer and board member of the UK National Crime Agency, offers an example of this sort of error. "Hackers may have an alias or tag. A few years ago a US criminal was caught after his girlfriend had the same tag tattooed on her body. She put a picture on social media," he says. "The law enforcement officers were very keen to know why she had that tattoo."

Even experienced criminals may get tripped up by a deed done in their callow days of youth. Andrew Conway, security researcher at Cloudmark, says: "They may not be very good at hiding their identity at first and, since the internet never



forgets, this may be used to track them down later. The Dread Pirate Roberts, Ross Ulbricht [founder of black marketplace Silk Road], was caught in part because he did not sufficiently disguise his identity in the very first post he made promoting the Silk Road."

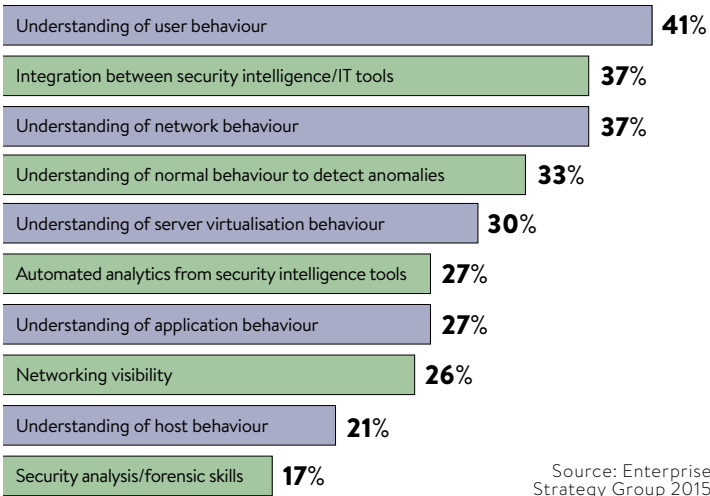
Forensic teams search for clues in overlooked places. Guy Bunker, senior vice president at cyber security firm Clearswift, says: "One of the critical pieces to understand is that there are at least two ends to an internet exchange. [US TV cook] Martha Stewart had a run-in with the legal authorities, and a lot of that hinged upon an e-mail having a sender and a recipient. While you could delete the e-mail from one place, erasing all instances of the e-mail was too difficult."

When the police have a potential lead they can use a few hacks of their own. Gunter Ollmann, chief security officer of Vectra Networks, says: "If law enforcement officers can install intercept software on a device used by the criminal, they can see all communications unencrypted."

"A popular tool is FinFisher, made by Gamma International. FinFisher is a commercial government law enforcement Trojan. It does everything you could possibly want, including key-stroke logging. It came to the public's attention during the Egyptian revolution, when the Egyptian police were alleged to be trialling it."

The FinFisher Trojan can be installed physically or remotely. For example, a telco can install it on to the

## MOST IMPORTANT FACTORS TO IMPROVE SECURITY VISIBILITY GLOBAL SURVEY OF 700 IT AND SECURITY PROFESSIONALS

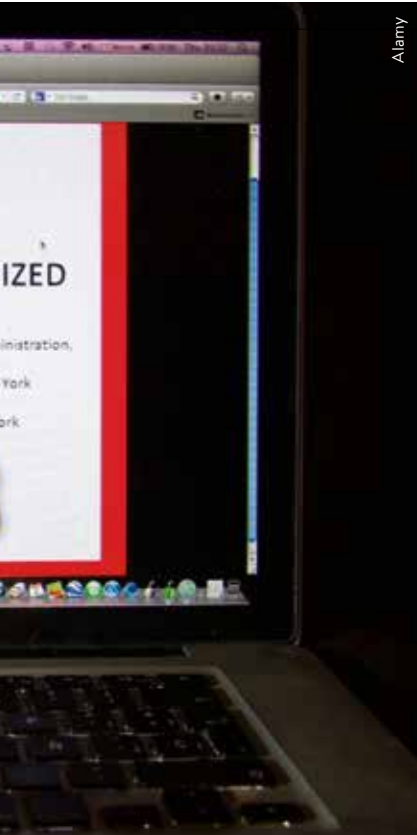


Source: Enterprise Strategy Group 2015








# going to get any easier

hackers, who cover their tracks and hide in cyberspace to have been arrests and successful prosecutions



Alamy

## FBI'S MOST-WANTED CYBER CRIMINALS

	EVGENIY MIKHAILOVICH BOGACHEV	REWARD Up to \$3 million	Alleged involvement in a racketeering enterprise that developed the Zeus software to capture online banking account details
	NICOLAE POPESCU	REWARD Up to \$1 million	Alleged involvement in internet fraud, posting advertisements for bogus merchandise on auction market sites
	ALEXSEY BELAN	REWARD Up to \$100,000	Alleged theft and sale of user databases from three major US-based e-commerce companies
	JOSHUA SAMUEL AARON		Alleged involved in a scheme to steal customer information from publicly listed companies and manipulate pre-arranged stock trading
	VIET QUOC NGUYEN		Alleged involvement in spamming more than one billion e-mail addresses and receiving commission on sales generated by subsequent internet traffic

Source: FBI

criminal's smartphone via a software update, if ordered to by a court.

Undercover work plays a role. The DarkMarket credit card fraud forum was cracked by FBI agent Keith Mularski, who took the guise of a spammer named Master Splynter. Undercover officers also infiltrated the LulzSec hacking group and Silk Road.

Money laundering can offer a treasure trove of clues. The FBI has had a number of successes looking at PayPal accounts. Cloudmark's Mr Conway says he was personally involved in the investigation of a wire fraud case. "When the secret service obtained the details of the suspect's PayPal account, they not only had his personal contact details, but also his customer list," he says.

But it's getting tougher, says Mr Conway: "Now that bitcoin and other cryptocurrencies provide a means of anonymous and largely untraceable funds transfer, that means is less useful."

Moving fast is the key to identifying hackers. One of the most famous successes of recent years was the take-down of the Citadel bot-net network. Citadel infected more than 11 million machines, with \$500 million in losses. The attacks were hosted on infected servers and sent victims to rigged websites via convincing, but fake, e-mails from well-known brands.

By the time the police identified the location of the target websites, the criminals had moved on. Microsoft vowed to smash Citadel. Its team turned to e-mail security specialist Agari to track attacks in real time. With the FBI and indus-

try body FS-ISAC joining the partnership, the criminals were traced to datacentres in New Jersey and Pennsylvania. Arrests followed and Citadel was crushed. "What is remarkable about the case is that it was led and funded by Microsoft, not by law enforcement agencies," says Pat Peterson, chief executive of Agari.

"Only when we had a court order could US marshals seize evidence and the FBI could investigate." Important moral here – often the best criminal detection work is done by

“  
Often the best criminal detection work is done by the private sector, alone or in partnership with the police

the private sector, alone or in partnership with the police.

Naturally, the quickest way to find a hacker would be to go direct to their location. That would mean getting through the obfuscation layers of VPNs (virtual private networks), Tor routing and IP anonymisers. Impossible?

Tor in particular is considered almost unbreakable. Andrew Beckett, Kroll managing director of cyber security and former head of penetration testing at GCHQ, says: "In-

telligence agencies spend millions trying to do so every year and only last year the Russian's tacitly admitted their inability to break Tor by offering a six-figure reward for anyone able to devise a reliable technology to decrypt data sent over Tor.

"The fact remains that for all the money spent by governments trying to break Tor, only a handful of users have ever been identified, and then at the end of a very expensive and labour-intensive process."

The conclusion for companies at threat is that the police cannot end hacking by detection alone. It is too expensive. Too time-consuming. Resources are too stretched.

Mr Taddeo, the ex-FBI New York cyber boss, says it's a losing war. "Any data point we look at tells us we are losing ground. The police can't keep up," he says. His new role as chief security office at Cryptzone focuses instead on beefing up security measures inside the corporate perimeter. "In this world it pays to harden your interior," he says. "All criminals need is one improper implementation of security and they can get access."

The police are doing their best. A freedom of information request by Veracode in 2015 revealed 3,829 British police officers have undertaken cyber security training, up 100 times compared with 2010. But even with these resources only a tiny fraction of the perpetrators will see justice. Catching hackers remains a tough, tough job.

Share this article online via raconteur.net



## Nuix to Resolve Manage the Threats

The Nuix Engine's unmatched speed and scale allow you to respond to cyber-threats efficiently when they happen and quickly minimise your losses—in data and financial terms. For incident responders, this means being able to capture data from hundreds of devices and locations and use advanced investigative techniques to analyse, visualise and report on the evidence you uncover. [This is why the world's leading financial institutions use Nuix for cybersecurity incident response.](#)

To know is to Nuix.  
Find out more at [nuix.com/know](#)



# Turning cyber defence into an

While the relentless growth in hacking keeps company executives awake at night, canny investors can generate re

INVESTING  
DAN BARNES

There are up to 250,000 cyber attacks each day, according to analysis by Bank of America Merrill Lynch (BAML), with approximately 70 per cent of those attacks thought to be going undetected. This wave of assaults may seem unstoppable, yet there are ways to fight back.

The cyber-security business is estimated by BAML to have been worth \$75-77 billion in 2015 and is forecast to reach \$170 billion by 2020. Getting exposure to the growth those firms may see as concern grows can offer investors, big and small, the chance to get a return from what would otherwise be a very damaging process.

Understanding what constitutes a cyber attack – and therefore defence – is paramount if investors are to get a breadth of exposure across the business.

“Most people have a connected device, be it a smartphone, a computer they use personally or at work,” says Andrew Chanin, chief executive of PureFunds, which offers a cyber security exchange-traded fund (ETF). “They are realising they are connected and they see credit card information breached at retail outlets they purchase their goods from, so they are realising this is something that is going to affect them.”

For the firms affected by cyber attacks, the cost of being hacked can relate to direct financial loss, the loss of intellectual property or a loss of business if customers and counterparties quit.

“The average cost of a cyber attack for a US company and listed US companies is up to about \$12.7 million,” says Sarbjit Nahal, equity strategist at BAML.

Businesses are not only motivated by losses, the authorities are increasingly taking an interest in how they protect themselves and their customers. MP Andrew Tyrie, chairman of the Treasury Select Committee, delivered an open letter to the head of the UK’s financial regulators in January arguing: “Legal, regulatory, structural and cultural changes are needed to the way that banks manage their cyber risks.”

He observed that co-ordination between supervisory bodies was needed as: “Currently, no one group seems to be directly responsible for developing a full understanding of the risks carried... by individual banks.” Without reform, “the public will remain more exposed than necessary to the risk of bank failure”, he concluded.

Spending on IT within banks is increasing considerably as a result; however, with hackers targeting

point-of-sale devices in shops and client data stored on websites, every business has to be aware of the risks.

“US corporates have seen their cyber budget grow at twice the rate of traditional IT budgets over the last three years,” says Mr Nahal. “We are now up to cyber accounting for about 6 per cent of IT budgets at across sectors.”

National security is also driving up spending on cyber security, with criminals and foreign government agencies being held responsible for attacks that can cause malicious damage as well as material loss. Threats are not always external or obvious as insiders account for more than 50 per cent of attacks, according to BAML, and as the internet of things enables more devices to become connected online, the array of possible targets has increased exponentially.

“Being hacked caused one of the big auto makers to recall 1.4 million cars,” notes Mr Nahal.

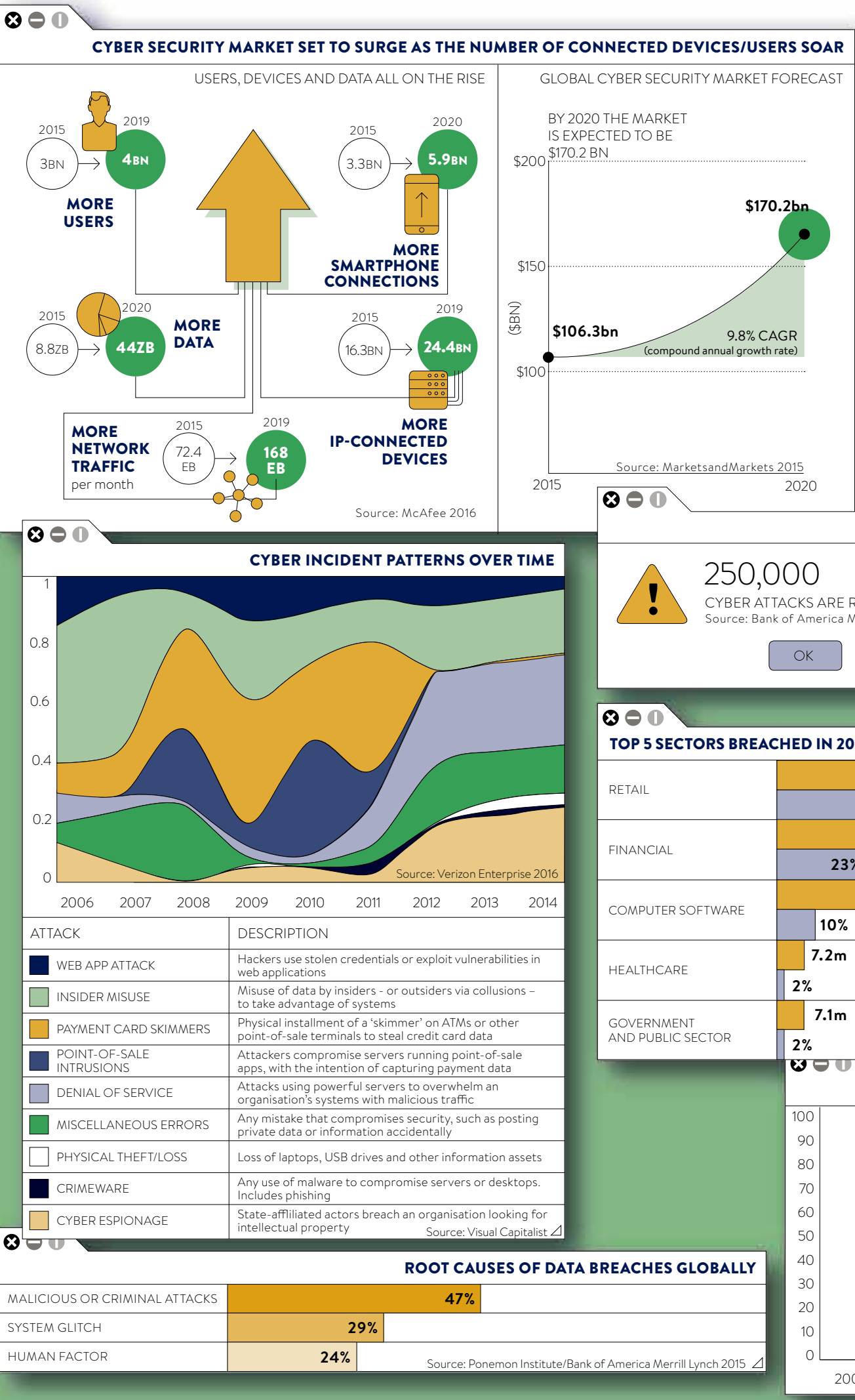
Firms that generate a return from increased expenditure on cyber security represent a range of services and technologies, from networks data travels on to anti-virus software on a computer desktop.

For investors seeking to benefit from any increased revenues they generate, getting the right mix of companies is essential. Typically this exposure can be gained by researching and picking individual stocks or putting money in a fund that holds appropriate investments, either a mutual fund or an exchange-traded fund.

Yves Kramer manages the Pictet-Security Fund for Pictet Asset Management, which invests in firms that cover IT security products, physical security products and security services. He says the fund is one way to gain exposure to cyber security while retaining diversity in the portfolio, which can be advantageous when markets are bad as this can cause niche stocks to see volatile price movements.

“We have between 10 and 12 per cent exposure to cyber security and I am happy we have reduced to that because [cyber security-focused] funds are seeing clients ask for redemptions,” he says. “We don’t perform much better than ETFs when things are great, but for sure when things are bad we do better, so it depends on the sort of risk investors want in their portfolio.”

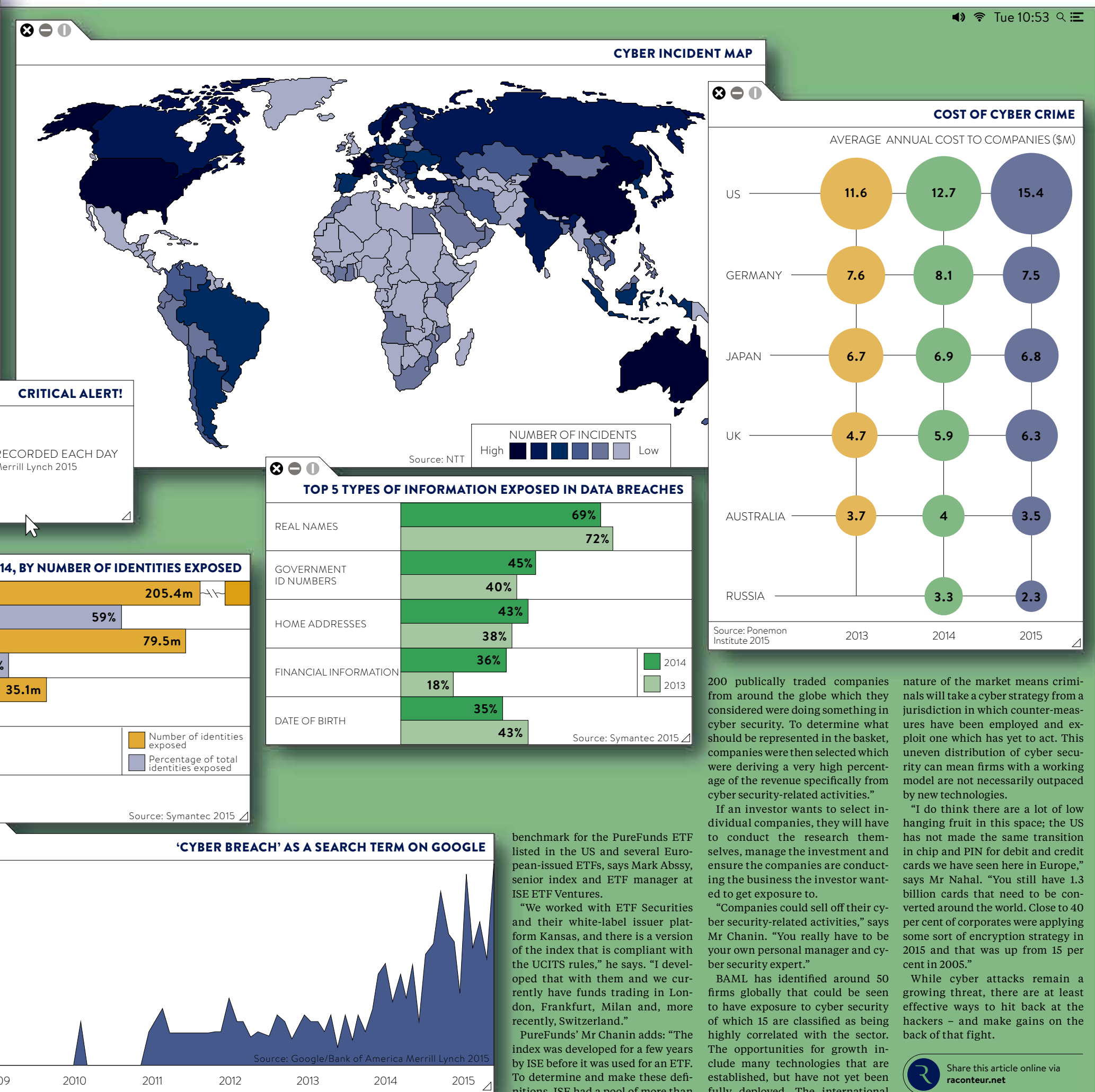
Investors who want to see more direct exposure can invest in ETFs that track an index of stocks which are specifically selected to represent the cyber security industry. The International Securities Exchange (ISE) has developed the ISE Cyber Security UCITS [undertakings for the collective investment in transferable securities] Index Net Total Return Index, which is used as the





# n investment opportunity...

returns from a global boom in cyber security as bosses defend against the hackers



## COMMERCIAL FEATURE

# PEOPLE POWER IS THE LOST KEY TO CYBER RESILIENCE

*Nick Wilding, head of RESILIA at AXELOS, says engaged employees can be the best defence against cyber attackers*



Corporate and personal reputations are hard won, but they can be ruined in an instant. As countless examples have shown, businesses large and small are being successfully attacked by cyber criminals with often catastrophic impacts.

The fact that so many organisations, of all sizes and in all sectors, have had their most valuable and commercially sensitive information compromised reflects the scale of the problem. It also highlights that no one is safe. All organisations are at risk and there are no silver bullets.

Cyber resilience can be described as the ability of any organisation to prevent, detect, respond and recover from the impacts of an attack with minimal damage to their reputation and competitive advantage.

But organisations can manage their cyber risks more effectively by adopting an organisation-wide strategy, led from the top, which effectively balances business opportunities and risks. Until this collaboration happens they will remain as vulnerable as anyone else.

So how resilient are organisations? Recent research by Ponemon, among 450 security and IT professionals, reported that only 29 per cent of organisations rate their cyber resilience as high. Only 15 per cent of respondents reported collaboration in the organisation as excellent and

nearly one third said collaboration was poor or non-existent.

In a resilient organisation, protecting your most precious information is as much about preparing for an attack and agreeing response plans and responsibilities to deal with one when it happens as it is about detecting and defending against attacks.

“Cyber resilience comes down to having an organisation of people who are cyber aware, curious, ask the right questions and who are not just ticking the box... Gary Warzala, senior vice president and chief information security officer, PNC Bank

It's often reported that approximately 90 per cent of all cyber attacks succeed as a result of human error – all of us are targets. Cyber criminals, like those in the real world, are opportunists and they are adept and persistent at exploiting these “unlocked doors” into any organisation.

Your people can be your best defence against the risk of a data breach. Leave them to their own devices (literally) and they may become your greatest vulnerability, but spread awareness via engaging, adaptive, regular and fun learning, and they will help to protect the organisation from within.

As phishing attacks and social engineering continue to account for the large majority of successful cyber attacks, influencing and improving human behaviours must sit at the heart of any effective organisation-wide strategy. Future success depends on all of us recognising our part in the operational health of the organisation and feeling valued in that responsibility.

Boards are ultimately responsible for the security of client data, commercially sensitive information and critical systems, and they need to lead the required collaboration across the organisation. They have to set the right tone from the top. Do they see themselves as responsible and accountable? Do they talk about security in their staff communications? Are they interested in latest attacks? Do they ask for and discuss regular intelligence on cyber risks and vulnerabilities? Your information security team might know what constitutes effective resilience, but are all departments, including human resources, legal, marketing and communications, on the same page?

## TEN TIPS FOR BUILDING YOUR CYBER-RESILIENT ORGANISATION



01

Understand the business strategy and what the most valuable information and critical systems are. Assess the cyber security capabilities company-wide and question whether it supports the business priorities, and establish that the right information security people and skills are in place to support the cyber strategy.



06

Consider certified training in cyber resilience and identify “cyber champions” within the various teams across the organisation.



07

Build the willing collaboration between the business, security teams and IT because no one can do it alone or without effective co-operation across the organisation.



02

Ensure the board sets the right tone from the top, addressing the importance of security when talking to employees, by seeking regular updates on how their organisation is affected, and by asking relevant and informed questions.



08

Create proactive, engaging, regular awareness learning programmes for all employees, regardless of role or responsibility. To be effective these should be short modules with refresher sessions incorporating the latest threats and providing simple pragmatic tips for employees.



03

Focus on identifying and managing information risk. Ensure there's a robust process for communicating risks across the enterprise.



09

Appreciate that your organisation is as much a target as any other. Identify what an effective and robust incident response plan looks like when a crisis occurs, and ensure this is tested.



04

Ensure there's a clear, honest and accurate assessment of the effectiveness of the security controls environment. Are controls consistently deployed across the organisation and regularly reviewed to ensure efficiency?



10

Demonstrate the business value of all the above. Ensure buy-in from all departments and make clear the risks of failure to take the issue seriously.



05

Seek out available best-practice guidance such as *RESILIA*, the Cabinet Office's *10 Steps to Cyber Security* and the UK government-backed Cyber Essentials scheme. Adopting the principles outlined will help reduce the risk of cyber attack.

## A VIEW FROM THE BOARDROOM

*“Out of nowhere, hard won reputations are at risk,” says Jim Baines, chief executive of Baines Packaging, Peekskill, New York*

He says: “Cybercrime wasn't on my radar. It was just an item way down on the agenda. Something I expected my IT Department to handle. My CIO had it covered. I thought. I expected.

“It never occurred to me that I might be a target. The stories you read in the press are usually about an employee who's walked off with a valuable bit of IP on a USB stick, or criminals after credit card numbers. But board members... CEOs? They're immune. Right?

“Wrong. They're actually the best targets. The biggest targets. They're

‘whales’ that smart hackers want to harpoon. We know all the secrets. We have privileged access to all the lucrative parts of our organisations.

“It makes perfect sense. Why start at the back door when you can go in right through the front? And board directors are just as human as anyone else. They make mistakes. They're careless. In fact, they're vulnerable because they think they're immune.

“That's what I thought. My company, which I built from nothing over 30 long, hard years when I put everything on the line, is now losing clients, losing money and, most crucially, has lost credibility. My reputation has been damaged with my peers, my friends... even my family.

I'm fighting back, but it's hard.

“You need to know that you are a target. Everyone on your board is a target. No one is immune; everyone is vulnerable, however powerful or successful they may be.

“You need to know that and act. Now.”

**Extract taken from *Whaling for Beginners* published by AXELOS, which follows Jim Baines's story as he realises just how close to home cyber attacks can strike and that his company's very survival now hangs in the balance. To read more please go to [www.axelos.com/best-practice-solutions/resilia/whaling-for-beginners](http://www.axelos.com/best-practice-solutions/resilia/whaling-for-beginners)**

This is just as true of small and medium-sized businesses as it is for the global corporates. The FTSE 100 might be the big prize, but small and medium-sized enterprises are equally at risk, often representing an easier route into larger organisations providing fertile ground for hacking groups to exploit.

AXELOS has developed *RESILIA*, a portfolio of cyber resilience best-practice publications, certified training, all staff awareness learning, leadership engagement tools and a tool to help assess your current cyber resilience posture. It is designed to put people at the centre of an organisation's cyber resilience strategy, enabling them to recognise effectively, respond to and recover from cyber attacks.

The critical thing to remember is that if you are a business and you are connected to the internet, then you

are a target and you will be attacked. Cyber criminals can target you from anywhere in the world. It's a low-risk crime and once they get what they came for they can melt away leaving little or no trace.

Becoming the victim of such an intrusive crime can be devastating and many companies never properly recover. Without adopting an organisation-wide strategy that understands your critical cyber risks, and which involves and engages all your people to be your champions in protecting what's most critical and valuable to you, it is just a matter of time before you'll be expected to respond to a successful attack or significant data breach.

**For more information visit [www.axelos.com/RESILIA](http://www.axelos.com/RESILIA)**



# The perfect cyber crime is so very easy to pull off

It's make-believe, but it could happen to you – hacking the internet of things could play havoc with your life and invade your privacy

INTERNET OF THINGS  
UNDERCOVER RACONTEUR

He's always been a bit arrogant my chief technology officer. But when he claimed our security set-up was impenetrable I knew he'd gone too far – even the FBI gets hacked these days. How could we be totally safe? He was talking nonsense.

Then I started reading about the internet of things (IoT). It's a fabulous technology. Lightbulbs you can control with your phone and cars report engine faults direct to the maker.

My chief technology officer (CTO) loves this stuff. It's also notoriously insecure. So I got an idea. I'd prank him. I called a techie mate of mine. We ran a covert survey of the CTO's house. I'll be honest – we never went through with our mad scheme. We just made a report. Then we showed it to my esteemed CTO. The look on his face was priceless. Here's what we found.

## DAY 1 SURVEILLANCE

Home CCTV is commonplace. And my CTO is a big fan. He's got cameras inside and outside. And boy are these hackable. Cyber security firm Imperva Incapsula reported in October that CCTV cameras are being hijacked to launch DDoS (distributed denial-of-service) attacks across the internet. Incidents are up 240 per cent on 2014. Incredibly, many owners fail to change the default password. Researchers at Context Information Security recently hacked the Motorola Focus 73 outdoor security camera, tilting it, zooming it and redirecting the video feed. It even provided a way to gain access to a home wi-fi password. It was clear we could spy on my hapless CTO and watch his every move. Spooky.

## DAY 2 PENETRATION

The key to hacking is the wi-fi router. Get into that and we would have access to every device in the IoT sphere. Is it hard? Turns out it is disturbingly easy. A 2015 report by HP found an average of 25 vulnerabilities per IoT device. Seventy per cent did not encrypt communications, 60 per cent had security glitches in their user interfaces and 80 per cent failed to require passwords of sufficient complexity. For example, Pen Test Partners demonstrated how to steal a user's Gmail credentials by going through a Samsung smart fridge. It's that easy.

## DAY 3 PRANK TIME

We wanted to give my CTO a bit of a scare. And when we looked at our options we were spoiled for choice. How about cranking the volume on his TV up to maximum? Or boiling his kettle non-stop (bit dangerous)? Context Information Security demonstrated a method of hacking into internet-connected lightbulbs to gain control of a Canon PIXMA printer and then ran a game of Doom on the printer display. Their estimation was 2,000 vulnerable printer models connected directly to the internet. We were sorely tempted to print out "We are watching you!" on a loop to make the point.

## DAY 4 NOW WE GOT SERIOUS

We wanted to prove that IoT devices could offer a real threat to our corporate secrets. If we could hack into his home network then it would be easy to steal company data. Our chosen way in would be via his baby monitor. A report by security analytics firm Rapid7 showed how nine baby monitor models could be hacked. The holes were trivial to "exploit by a reasonably competent attacker" and can "quickly provide a patch to compromise the larger, nominally external, organisational network". Translation – we could hack his system. QED.

## DAY 5 OUT OF THE OFFICE

The IoT is everywhere. This means we have opportunities to cause trouble no matter where our target is located. In September *WIRED* magazine showed how hackers can take control of a Jeep Cherokee. The air-con starts spewing freezing air. The wipers turn on. Brakes and steering could be controlled. The hackers previously disabled the brakes on a Toyota Prius. We've seen traffic lights hacked. A survey by Unisys found 70 per cent of critical infrastructure managers reported at least one security breach in the past 12 months. There's no escape.

## DAY 6 WE ALMOST WENT TOO FAR

My techie mate pointed out that our target's wife still used a Windows XP laptop and, being a bit old fashioned, didn't apply updates. Huge mistake. An attack on the Windows Remote Access Tool or RAT would give us access to her webcam. A plethora of sleazy internet forums show how the RAT tool can be abused, with horrifying results. We could activate the webcam while she's watching Netflix in bed. The very thought made us shudder.

## DAY 7 FULL-SCALE PANIC

The more we looked at ways to exploit the IoT, the more we panicked. Drone attacks? They are coming. Texas-based firm Praetorian flew a wi-fi-enabled drone over Austin, Texas and found almost 726 IoT devices in 18 minutes. It was looking for devices using the ZigBee communication protocol, which had been shown to be insecure. That is insecurity on a galactic level. We are not the only one's thinking of this. James Clapper, US director of national intelligence, told a senate committee last month: "In the future, intelligence services might use the IoT for identification, surveillance, monitoring, location-tracking and targeting for recruitment, or to gain access to networks or user credentials."



# Hidden web of shame, deceit and death

The Dark Web can be a dangerous and murky den of criminality – ironically the brainchild of US government agents, it is now colonised by organised cyber criminals

## DARK WEB

DAVEY WINDER

“The Dark Web is an online community accessed by groups with a range of agendas that want to protect their anonymity – whether this be online criminals, activists or those wishing simply to maintain their online privacy.”

These are the words of Rik Ferguson, vice president of security research at Trend Micro and a special adviser to European Union law enforcement agency Europol.

When he investigated the Dark Web he found that light drugs were one of the most traded items, with hard drugs, pirated games and stolen accounts alongside. “Many Dark Web users, or at least those who frequent the top marketplace, go there to purchase illicit drugs,” he says. But what, exactly, is the Dark Web?

Invisible to search engines such as Google, the Dark Web is made possible by darknets – networks which can only be accessed with specific software and authorisation – through networks where connections are made between trusted peers.

The best known, and by far the most popular, darknet is the Onion Router (Tor), which was created by the US Naval Research Labs in the 90s as an enabler of secure communication and funded by the US Department of Defense. To navigate it you use the Tor browser, similar to Google Chrome or Internet Explorer apart from keeping the identity of the person doing the browsing a secret. Importantly, this secrecy also applies to what the user is looking at.



It is because servers hosting websites on the Tor network, denoted by their .onion (dot onion) designation, are able to mask their location, originally to enable government drop-sites and information silos to exist without trace, that when Tor software went public in 2003, the Dark Web became a reality.

This combination of hidden servers and anonymous users enables a .onion version of Facebook for those who fear being spied upon, and empowers political activists to continue protests while protected from regimes that would take away more than their liberty. Unfortunately, Tor is also used by the criminal fraternity as a dark marketplace.

Using a crawler bot that scraped the .onion sites accessible to it,

“The Dark Web treads the line between being a saviour of free speech and a criminal marketplace of the most extreme kind

researchers at King's College London recently attempted to map criminal activity on the Dark Web. The results suggested some 57 per cent of Tor sites host illegal content. What the study didn't find was evidence of Islamic extrem-

ism, claiming a near absence of jihadi activity.

Indeed, that around 40 per cent of the crawled Tor activity does not fall under the label of criminal endeavour reveals the dichotomy of the Dark Web; it treads the line between being a saviour of free speech and a criminal marketplace of the most extreme kind.

Perhaps the best known example of a dark market was Silk Road. Shut down in 2013 after an FBI sting operation, which would eventually see its creator, Ross Ulbricht aka Dread Pirate Roberts, jailed for life, Silk Road was like an eBay of criminality. The closure of Silk Road has not meant that criminal activity on the Dark Web has shut up shop alongside it, however.

“Today, anything and everything is available on the Dark Web from guns and explosives to designer drugs and paedophile material, from hacking code to identities and credit cards,” says Andrew Beckett, managing director at security intelligence specialists Kroll. “What is more surprising is the growth of online services and support around these activities, and the way they are run as big businesses.”

While five years ago you could buy a DDoS (distributed denial-of-service) attack to take down a site of your choosing for around £35 per day, now that has dropped to £20. This is what has become known as Cybercrime-as-a-Service (CaaS) and those wishing to create a sophisticated attack are spoilt for choice on the Dark Web.

But have successful law enforcement investigations, such as the Silk Road case, changed the Dark Web operationally?

“It is only natural for criminals to become more suspecting and hesi-

tant, for malware vendors to disappear and for the expert-level fraudsters to go deeper underground after a major bust,” says Limor Kessem, senior cyber security evangelist at IBM Security and a Dark Web expert.

Ms Kessem has witnessed the gradual departure of banking Trojan developers from the Dark Web as they realised just how dangerous their activity was and how some of the best-known developers were being arrested. Anyone wanting to access the more “elite” marketplaces on the Dark Web will not only have to know precisely how to reach them, but also need to know someone within the community who can vouch for them and possibly pay a joining fee.

“In some cases they have to prove that they are criminals or show their ‘work’ in some way,” she says, concluding that for everyday folk or criminal chancers these boards are almost impossible to join.

Assuming you are among the criminal fraternity with access to Dark Web markets, what are the trading tools that are considered essential for doing business in the shadows of the internet?

A Tor browser is something of a given, however most serious criminals will ensure the devices they access the Dark Web from remain free of as many traceable artefacts as possible.

“Most will utilise USB bootable operating systems such as ‘Tails’ to make sure that nothing is saved to their hard disks,” says Adam Tyler, chief innovation officer at security specialists CSID. “Tails is a Linux-based OS [operating system] that can be started on pretty much any computer and forces all internet connections through Tor, while encrypting all files and e-mails, and leaving no traces on the host device. Most payments are made using bitcoin, but the career criminals know better than to use it without proper precautions.

“Due to an ability to connect links between addresses and identities, many choose to utilise ‘bitcoin tumblers’ to attempt to evade identification or association.” Tumblers effectively launder the currency by a user transferring their bitcoin into a tumble pool and then withdrawing a collection of unrelated coins to the same value.

As Kroll's Mr Beckett concludes: “The expansion of the Dark Web looks set to continue as criminals find evermore innovative ways to monetise their activities and offer them as a service. The ability to hide this activity from law enforcement and to mask the financial transactions by using bitcoin or bartering only increases the attractiveness.”

Tor, or the Onion Router, harbours hundreds of illegal sites where you can hire a hitman, buy drugs or trade weapons

## DIFFERENCE BETWEEN THE DEEP AND DARK WEBS

### DEEP WEB

This refers to the broad section of the internet that traditional search engines are unable to access, including password-protected web forums, chat services like Internet Relay Chat, file sharing and peer-to-peer technologies such as BitTorrent

### DARK WEB

This is a sub-component of the Deep Web that is not only inaccessible to mainstream search engines but only visible to users who have installed specialised software, such as Tor or I2P, enabling access to these regions of the internet. Many forums, websites and marketplaces on the Dark Web offer highly anonymised environments to conduct malicious activities, and purchase illicit goods and services

Source: Flashpoint

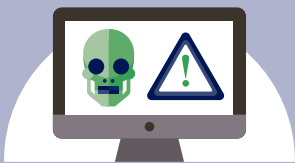


DARK WEB SHOPPING LIST OF CRIME



**CREDIT CARDS**  
**(£3-£10 each)**

Credit cards remain easy to buy on the Dark Web with US-based cards available for £3 each, while EU and UK cards are more sought after and can be sold for three times as much. A premium is placed upon card data guaranteed not reported stolen at the time of sale.



**INFECTED COMPUTERS**  
**(£15 PER 1,000)**

A sad reflection of how easy it is to infect a computer and turn it into a “bot” which can then be used as part of a botnet to launch DDoS attacks for example, is how cheap they are being sold. The more you buy, the cheaper they get with 10,000 bots going for £100.



**LOYALTY ACCOUNTS**  
**(£15-£1,000)**

There is increased buying interest for loyalty accounts that can be used by criminals to pursue profitable social engineering attacks. Hotel loyalty account data can sell for as little as £15, while eBay profiles with a very high reputation status can reach as much as £1,000.



**RECREATIONAL DRUGS**  
**(£25+)**

Although the ill-fated Silk Road was the best known illegal drugs marketplace on the Dark Web, the deals have not stopped since its demise. Recent research reveals average prices of £70 per gram of cocaine, MDMA at £25 a gram and ten tabs of acid for £75.

**HACKERS FOR HIRE**  
**(from £100)**

If you look hard enough you will find hackers, complete with customer feedback ratings, offering services from as little as £100 for hacking an e-mail account up to £500 or more for corporate espionage, reputational damage and so on.



**US CITIZENSHIP**  
**(£4,000)**

The option to “become a US citizen” is provided in a package, containing a passport, social security number, driving licence and birth certificate, can be bought, along with supporting documentation. Fake passports are sold separately for £650 and counterfeit driving licences are £150.



**HANDGUNS**  
**(£450)**

Perhaps surprisingly, not a US-only market. Handguns are being traded within Europe and can be purchased with prices starting from £450. Delivery might be problematical though, even with promises of weapons being stripped and dispatched in pieces.



**ASSASSINS FOR HIRE**  
**(£25,000+)**

Yes, you can even rent the services of a hitman on the Dark Web. Sellers of such services require the bitcoin fees to be placed into escrow and, once the hit has been carried out, the funds are released. Don't expect much in the way of references or customer feedback.



COMMERCIAL FEATURE



CYBER THREAT DEMANDS A NEW APPROACH

*It's time for a new cyber security approach, shifting focus to prevention and leveraging global threat intelligence sources to protect critical information assets*



The internet economy now accounts for 8 per cent of GDP in G-20 economies. As we become increasingly dependent on technology and as threats to data have become more sophisticated, responses have evolved in tandem. The European Union is introducing new laws to improve confidence, impacting both consumers and businesses. This is a pivotal year for cyber security and data protection in the EU and therefore the UK. Last year, the EU preliminarily agreed on two new pieces of legislation – General Data Protection Regulation (GDPR) and Network and Information Security (NIS) Directive. GDPR, which replaces the 1996 Data Protection Directive, stipulates rules on protecting EU residents' personal data. GDPR applies to entities that control or process such data, even if they're not based in the EU. The NIS Directive establishes security requirements and incident notification obligations for “operators of essential services” and “digital service providers”. Both laws are expected to be published in final form early this year, when implementation timelines start – essentially a period of two years. The NIS Directive directs member states to ensure that entities in scope take “appropriate and proportionate technical and organisational measures to manage risks” to security of their networks and information systems, and that measures “have regard to the state of the art...” GDPR similarly directs data controllers to implement such measures “with regard to the state of the art” to protect the rights of data

subjects, and directs data controllers and processors to implement such measures “to ensure a level of security” appropriate to risk. Both the NIS Directive and GDPR are opportunities to manage cyber and data protection risks with a new approach. Although the ink is not dry on either law, they refer to “state-of-the-art” processes and technologies.

“To evolve our digital world continually, we need next-generation capabilities that match the state-of-the-art cyber world, so cyber security empowers trust and enablement of IT

They require companies to identify and manage security risks dynamically. Notification requirements make it essential to prevent incidents before they happen. Retrospective incident detection could be too late, and won't protect companies from reputational risks and regulatory scrutiny. Companies will have to keep pace with capabilities to protect EU residents' personal data and sensitive business data. Chief information security officers and chief information officers face many challenges – identifying and mapping data assets, assessing

risk, determining what state of the art means for them, and documenting and continuously improving security policies and practices. Greg Day, vice president and chief security officer, Europe, Middle East and Africa, for Palo Alto Networks, says: “Businesses have built out security on outdated principles, leveraging people skills as glue holding together fragmented approaches. Challenging businesses to leverage state of the art requires them to re-examine fundamental principles to manage today's risks and enable modern digital business. “This requires a conscious decision to focus on preventing business impact, not simply responding to something – next-generation capabilities designed for today's internet, not the old capabilities on which the internet is based. “Companies can no longer afford to keep extending what's broken. They must go back to fundamental principles and adopt a cohesive, automated and integrated single-analysis approach. They must work at internet pace, providing consistent coverage across today's modern digital world – devices, networks, datacentres and the cloud – leveraging collaborative and automated cloud intelligence and analysis to keep pace with the modern attackers. “To evolve our digital world continually, we need next-generation capabilities that match the state-of-the-art cyber world, so cyber security empowers trust and enablement of IT.”

MOBILE  
STEPHEN PRITCHARD

By 2020 a staggering 4.6 billion people will own a mobile device. This figure, from industry trade body the GSMA, shows just how ubiquitous mobile phones have become in a few decades.

These devices are changing the way we work and how businesses operate. Mobile phones and tablets are replacing landlines and PCs, with everyone, from executives to field engineers, carrying what amount to miniature computers.

But our addiction to mobile devices brings with it security risks. As businesses depend more on mobiles, so the devices will carry evermore sensitive applications and data.

And, because mobile phones and tablets are very personal devices, often bought and owned by the worker, companies may have few controls over how or where they are used. But companies cannot tell their employees to go back to their old ways of working.

"You can't roll this back – you have to support mobile," says Kevin Bocek, chief strategist at security firm Venafi. "Everything is touching mobile now. If you have a mobile app that talks to something in the datacentre – that is mobile."

This raises the risk that if hackers or other criminals obtain a mobile device, or can break into it, they can use it to penetrate deeper into a company's network.

And, although mobile devices are actually more secure than early PCs, there is growing pressure for the industry to give security forces and law enforcement agencies "back doors" to the devices which bypass security, as the ongoing dispute in the United States between Apple and the FBI shows.

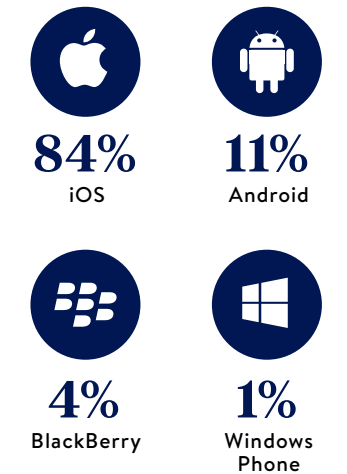
"A phone can be the keys to the kingdom – it is a really rich target," cautions Ben Johnson, chief security strategist and co-founder of Carbon Black, also a security firm. "The people using tablets and phones are often the executives, the people who have the most sensitive material."

This, he suggests, means organisations need to act now to lock down mobile devices, before they present a real risk to security.

Some of the steps businesses can take to secure their mobile devices are similar to measures for secur-



MOBILE VULNERABILITIES BY OPERATING SYSTEM



Source: Symantec 2015

# Cyber crime on the move with mobile

Smartphones and tablets loaded with apps and sensitive company data represent a security risk in the wrong hands

ing PCs – installing anti-virus software, ensuring operating systems and applications are up to date, and making sure employees set strong passwords and PINs.

The mobile industry itself is also acting to make their devices more secure. BlackBerry, for example, recently launched the PRIV, a highly secure phone based on the Android operating system.

Apple already encrypts data on its handsets as well as messaging services such as Facetime, one reason for its current dispute with the FBI.

There is a wide range of applications for mobile device management which allow IT directors to lock or wipe lost or stolen phones. These range from free tools, such as Apple's iTunes, to more comprehensive systems from Microsoft and specialist companies such as MobileIron.

Companies, though, might be reluctant to eat into their IT budgets to bolster mobile security, especially as the number of security incidents attributed to mobile devices remains small.

Verizon, the US-based mobile operator, calculates that 0.03 per cent of mobile devices were infected with any truly malicious malware. But the threats to mobile devices are not limited to the type of high-profile virus attacks that affected desktop computers ten years ago.

Instead, hackers are looking to steal business data, gain access to companies' networks, to accounts belonging to "privileged users", such as IT administrators, and possibly capture personal data, such as a user's location and passwords, or

financial information, for identity theft and other criminal purposes. According to Verizon, more than five billion Android mobile applications are vulnerable to attack.

And businesses might be wary of installing mobile management applications for legal or contractual reasons. If an employee brings a personal device to work, companies will have fewer options to control that device than if they buy the workforce company phones.

In some countries, especially Germany, there are strict rules on employee monitoring and this can also make it hard to ensure mobile security.

As a result, some businesses are reacting by buying more devices for staff and moving away from bring-your-own-device programmes that allow personal mobile kit at work.

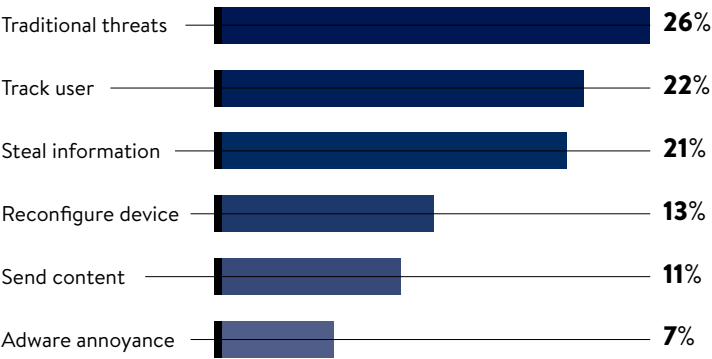
But even then, there are risks associated with using mobile devices that are simply different to the risks posed by a PC on a fixed network and those risks might be growing. "A desktop PC is hardwired to the network. Mobiles access thousands



**4.6bn**  
people will own a mobile device by 2020

Source: GSMA

MOBILE THREAT CLASSIFICATIONS



Source: Symantec 2015

“A phone can be the keys to the kingdom – it is a really rich target

of different networks and they are out in the field doing that,” says Chris Underhill, head of IT and security at consulting firm CSP.

And, not only do phones have computing power on par with a PC of just a few years ago, but they have far more sensors, from the camera and microphone to an accelerometer that records how fast the device is travelling.

“There are new ‘threat vectors’ that need addressing, which tend to accompany mobile – radios, social and sensors,” says Rob Bamforth, of industry analysts Quocirca. “Does that make mobile security more difficult? Probably not, but the risks are less tangible so perhaps easier to miss or ignore. That’s what makes them more of an issue.”

Jon Collins, industry analyst at GigaOm, says: “Mobile devices have blown any traditional ideas we might have about security right out of the water. Ultimately the focus needs to be on data.

“First that is in terms of both what personal information an individual is prepared to give up via the device and via apps. Second in the corporate sphere, it is what corporate data should be accessible, and therefore potentially vulnerable, on the device.”

This suggests that companies might need to restrict the applications staff run on mobile devices, especially personal ones, and also limit mobiles’ access to sensitive networks. But few experts suggest that companies can roll back mobile working.

“I can’t see any executives pushing back on mobile,” says Kris McConkey, who heads the cyber threat detection and response team at consulting firm PwC. “There is a lot more recognition that the next generation [of employees] expects to be able to work more freely. But that also means a growing ‘attack surface’.

“Firms should take the same basic approach they do to a lot of security issues. Limit privileges, and keep apps and operating systems up to date. They should think about what introducing mobiles or putting business applications on them does to the security landscape.”



## COMMERCIAL FEATURE

# BUILDING CONFIDENCE IN AN ERA OF 'DATA SPRAWL'

*Cyber security must keep pace with the rapid rise of digital technology and the internet of things*



The digital world faces a crisis of confidence when it comes to cyber security. High-profile breaches are reported in the news almost every week and it seems no industry sector or territory is immune from the threat.

But with the spread of digital technology and its greater uptake by people and businesses, the danger is about to increase unless technology brands mobilise more effectively to do something about it.

With the arrival of a hyper-connected world and the internet of things (IoT), the number of devices connected to the internet, from thermostats to automobiles, is set to soar in the next decade. As well as enhancing lives and freeing up time it will open innumerate new aspects of people's daily lives to influence from "dark forces".



**We want customers to be more productive and more secure regardless of what they are working on, be it an iPhone, BlackBerry, Android tablet or some other device**

Yet rather than step up efforts to repel hackers and virus writers, there has been a step change in corporate approaches to the threat. Corporations are starting to accept

they might be attacked and are putting greater weight on what to do when systems are compromised than on preventing attacks in the first place.

"People just don't have confidence in a hyper-connected world yet," explains David Kleidermacher, chief security officer of BlackBerry, a company at the very forefront of mobile enterprise security innovation. He argues that companies should redouble efforts to keep the hackers out or else a bad situation will get steadily worse.

"With the IoT there will soon be tens of billions of connected devices all over the world, both personal and corporate, that must be protected and secured. Eventually the figure is predicted to reach trillions. This is not an environment in which people should be wondering whether the internet is safe."

In other words we need to stay the course on prevention. Although working on contingency planning is vitally important, prevention is a more desirable outcome and one that will instill confidence in digital technologies in the future, helping to realise their full potential.

This is a challenge BlackBerry is investing time, energy and resources in. While some technology companies focus on creating apps and widgets, BlackBerry is focused on privacy and security. It's a culture that has developed over many years from the ground up and is unmatched in product life cycles.

"Ask anyone at BlackBerry what is their chief concern, and they will say it's privacy and security. It's in

the company's DNA, so we see it as our responsibility to show other companies the way forward in this area," says Mr Kleidermacher.

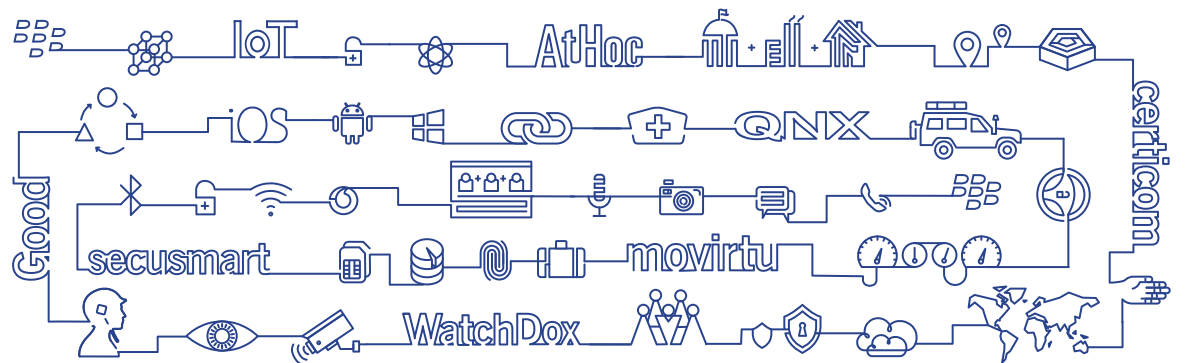
A major reason digital channels are so fragile is the enormous ecosystem of devices and services on offer. In order to create an effective security strategy, organisations must identify a baffling and ever-changing array of devices, and work out how they all interrelate.

This complexity breeds weaknesses, with hundreds of vendors launching new and more powerful services into communication networks every year. For BlackBerry, therefore, the goal is to create end-to-end solutions that ensure productivity is matched with privacy and security across all devices.

"We want customers to be more productive and more secure regardless of what they are working on, be it an iPhone, BlackBerry, Android tablet or some other device," says Mr Kleidermacher. "This includes IT administrators who want back-end services that work across the board and grow with flawless updates."

"Our enterprise mobility management platform supports a broad range of devices and operating systems, allowing businesses of all sizes to free up their workforce and take advantage of all the good stuff mobility brings without exposing sensitive corporate data."

Moving beyond enterprise-level systems, the burgeoning IoT requires a fresh approach to security that protects consumers



THE WORLD'S MOST TRUSTED ENTERPRISE SOLUTIONS

too. In the future connected devices will range from cars to medical devices, meaning a breach could have devastating consequences.

Anticipating this very real threat, BlackBerry has created a complete division of specialists working on IoT-specific solutions. They build security that is simple to use as well as effective, allowing people outside the IT field to protect themselves easily.

"It's no good making 16-digit passwords because people just won't use them; the solutions have to be easy to implement," says Mr Kleidermacher. "When people think about security, they often think about end-points, where data originates and where it is accessed, but it's possible to secure data wherever it goes."

He describes a hypothetical example of a patient sending a picture of an X-ray to a doctor for assessment. Once it is sent the patient has lost control of the data and it could end up in places he or she doesn't want it to go, say an employer or an insurance company.

"Files can be encrypted, but that doesn't go far enough," he adds. "Now, when I share a file, I can attach permissions to caveat its use by giving the receiver only a limited time to



**The danger is about to increase unless technology brands mobilise more effectively to do something about it**

view the file or preventing them from forwarding or modifying the message.

"In this growing sprawl of data and devices it's vital that end-users are able to take control by tying security to the data itself and not just the devices that access it. You can't know where your data is going otherwise."

BlackBerry has taken numerous further steps to alleviate the crisis of confidence in technology. It has sought out inter-governmental security certifications as well as national standards and where industry standards do not exist it has looked for independent partners to help create them.

It has recently been working on a security standard for medical devices in conjunction with the US Food and Drug Administration, because one didn't exist, and an insulin pump connected to the internet, for example, must come with certain guarantees.

In addition to creating new independent cyber security assurance standards, BlackBerry is leveraging its own team of expert hackers, augmented by the recent acquisition of UK consultancy Encryption Limited, to help BlackBerry's customers improve their security development life cycles, and assess their systems and applications for vulnerabilities.

Why? As Mr Kleidermacher concludes: "You can't raise the cyber security bar until you first know how to measure its height."

[uk.blackberry.com/enterprise.html](http://uk.blackberry.com/enterprise.html)





# Caught in the crossfire: companies on front line

If governments and rogue states go to war in cyberspace, companies big and small can become targets as state-sponsored cyber warriors attempt to cause chaos

CYBER WARFARE  
STEVE RANGER

Cyber warfare seems so much like an idea from science fiction, or perhaps the plot of a cheap airport thriller, that it's hardly surprising most companies don't think of it as a significant risk to them. But the evidence of the last few years would suggest that they should start thinking a little harder, because the risk is high and rising all the time.

There's no one definition of cyber warfare; indeed many countries use different definitions which suit their own agendas, so the term can cover quite a wide range of online activities performed by states against their opponents.

These might range from low-level threats such as spreading propaganda and disinformation via social media through to cyber espionage – stealing secrets by hacking. And all the way up to using digital weapons to create damage in the real world – the nightmare scenario of hackers attacking the power grid,

TOP 20 COUNTRIES BEST PREPARED AGAINST CYBER ATTACKS  
SCORE OF CYBER SECURITY COMMITMENT AND PREPAREDNESS

01		0.824	11		0.706
02		0.794	12		0.706
03		0.765	13		0.706
04		0.765	14		0.706
05		0.765	15		0.676
06		0.735	16		0.676
07		0.735	17		0.676
08		0.706	18		0.676
09		0.706	19		0.676
10		0.706	20		0.647

Source: ABI Research/ITU

SUSPECTED STATE-SPONSORED MALWARE



STUXNET

Computer worm discovered in June 2010, designed to disrupt machinery, such as those in nuclear power plants, by attacking industrial programmable logic controllers



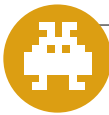
DUQU

Thought to be related to the Stuxnet worm and discovered in September 2011, Duqu hunts for information that could be used in attacking industrial control systems



FLAME

Discovered in May 2012, Flame is designed to carry out cyber espionage by stealing computer display contents, files, data and even audio conversations



GAUSS

Discovered in August 2012, Gauss is designed to monitor online banking accounts by stealing browser history, cookies, passwords and system configurations

for example, and switching off the lights for everyone.

Some of this might seem far-fetched, but governments around the world are spending billions on building up armies of hackers and stockpiles of cyber weapons, making it evermore likely future battles will be fought with electronic weapons as well as tanks and jets.

That's because developed countries are extremely reliant on the electronic systems which run the banks, keep retailers' supply chains operating and keep the power on. Any piece of computer code which could interfere with the smooth-running of these systems would be just as valuable as a battalion or two in a conflict.

"You could wage a fairly effective war against a country by stopping its banking system. Most of us do our banking online so what if you launched a massive denial-of-service attack against lots of banks and stopped the banking infrastructure being effective, you could do a lot of damage to a country," says Professor Alan Woodward of the University of Surrey.

Unlike on the traditional battlefield, geography is irrelevant. Digital attacks can be launched from anywhere, against any target. All you need is enough computing power, internet access and skill. And thanks to the often anonymous nature of the internet, it may be very hard to work out exactly who is behind the attack, making it much harder to strike back.

So if a rogue state did want to launch a cyber attack against another country, the most obvious target

would be what's known as the critical national infrastructure, such as energy, transport, financial services or food – the essentials we all rely on.

That critical national infrastructure is made up of many big companies, but also smaller suppliers, many of which may never think they could be a serious target for state-sponsored hackers. "These supply chains are very deep and therefore include a surprising number of companies," says Ian Glover, president of security industry group Crest.

Organisations must assess the risks to their business and make sure they have the internal skills or know-how to procure expert advice to design, manage and test their ability to protect themselves, he says.

Even small companies that might be suppliers to the larger players could be targeted, exactly because they are smaller and thus less able

to protect themselves against attack. "They can get caught in the crossfire in a number of different ways," says Professor Tim Watson, director of the Cyber Security Centre at the University of Warwick. If a small company makes a vital widget, without which a bigger company or an army grinds to a halt, this could make it a target.

And, of course, industrial secrets are another tempting target; you might

not be taken offline, but stealing plans for your next product could be just as damaging.

Any organisation that derives its corporate worth from the intellectual property it generates should

Governments are spending billions on building up armies of hackers and stockpiles of cyber weapons, making it evermore likely future battles will be fought with electronic weapons as well as tanks and jets

ONE STEP AHEAD

of malware, hackers and the industry

Check Point SOFTWARE TECHNOLOGIES LTD

Schedule your free security check up today

checkpoint.com/resources/securitycheckup



## ARTIFICIAL INTELLIGENCE AT WAR

First the good news about artificial intelligence or AI – security companies are already looking at how to use it to fight back against hackers.

New AI-powered tools can be “taught” to understand how a computer network usually operates, which then makes it very easy for such systems to spot unusual behaviour that could indicate a hacker is on the loose – like a computer copying a top-secret database in the middle of the night, for example.

But there’s also the bad news. As we increasingly rely on AI to make decisions for us, this increases the risk that those systems can be tricked by even smarter systems, without us realising.

It’s something that US director of national intelligence James Clapper warned about in a report to the Senate Armed Services Committee last month.

“AI systems are susceptible

to a range of disruptive and deceptive tactics that might be difficult to anticipate or quickly understand. Efforts to mislead or compromise automated systems might create or enable further opportunities to disrupt or damage critical infrastructure or national security networks,” he warns.

Another problem is that at the moment cyber weapons are extremely expensive and complicated to build because they have to be specially designed for each target. Automatic cyber weapons incorporating AI could seek out vulnerability and adapt to the defences of different targets without assistance from a human operator, making cyber warfare much easier to execute against many more targets than hitherto possible.

This could lead to some interesting moral questions in future – if these autonomous AI weapons do damage, who is really responsible?

think very carefully about whether they could be a target, says Professor Woodward. “If you look at the vast majority of cyber attacks, they’re actually stealing ideas, stealing intellectual property because it’s extremely valuable.”

Companies tend to think of their cyber security risk in terms of their IT systems, such as e-mail, customer databases or websites. These are important and certainly essential to the smooth-running of most businesses.

But these aren’t the only electronic systems that keep businesses running. Many are now putting their industrial control systems online. These systems might control anything from factory systems to things as prosaic as the air conditioning. Connecting them to the internet is handy for remote monitoring, but can create a major security risk. And the rise of the internet of things means more and more devices are being connected up to the internet all the time.

“You’d be absolutely astonished at what is connected to the internet,” says Professor Woodward.

These systems are vital to the smooth-running of a business, but are often forgotten about, hard to upgrade and hard to make secure, all of which makes them a tempting target for hackers. It doesn’t matter how well your servers are protected with firewalls and other tech if a hacker can switch off the air conditioning to the datacentre which means they all overheat and break down.

All of this means this isn’t a job the board can simply dump on the IT department.

“With the greatest of respect, a lot of boards don’t know how the PC at home works, and think this is an IT problem and they delegate it down to the IT department, that it’s their problem – it’s not,” says Professor Woodward.

Rather, making sure that a company is protected is the responsibility of many different elements of the business.


Certainly IT has to be involved, but also human resources making sure that staff know what to do and what not to do, while the board has to be educated about the risks and be ready with a plan if the worst happens. Non-executive directors can be a handy source of information and counsel.

“The responsibility for worrying about it has been delegated implicitly by the rest of the organisation to IT and it needs to be pervasive. You don’t just put technical controls in; the most effective controls will be the cultural ones and the IT department aren’t the best placed to introduce those,” says Professor Watson.

This doesn’t get IT off the hook though as they still have a responsibility to explain the risks to the board.

“It’s all very well to blame the board, but they are rational and they are running a business, and if somebody comes to you and says, ‘I need to spend this sum of money on this nebulous threat and I can’t tell you what you are going to lose’, the board quite rightly is focused on business processes,” he says.

The threat may seem too great to cope with, but the reality is that the vast number of security incidents, including some very high-profile ones, are preventable. The first step is to consider whether your organisation might be a target and why, and to make sure cyber-security best practice is understood and adopted across your organisation. That should help keep cyber warfare in the realms of thrilling fiction, rather than your grim reality.

 Share this article online via [raconteur.net](http://raconteur.net)



dimension data 

accelerate your ambition

## Risk less, achieve more with cybersecurity.

If you believe you can do anything, we’re here to help you do it.

### Security steps up to meet the digital age

The chief information security officer (CISO) faces a new headache: digital complexity. The digital world has changed how organisations communicate with the wider world. The rapid increase in how we use technology to communicate has led to more data and more points of entry – or breach – and, because this is happening at such a rapid pace, security hasn’t been able to adapt fast enough. We saw this in the explosion of hacks and breaches in 2015 and, in 2016 and beyond, CISOs must look at new policies and processes in order to address this.

Information security has to be re-evaluated and realigned as part of digital transformation. Social media plays a fundamental part in this journey. People aren’t holding back on social media – they’re sharing more than ever. Sadly, cybersecurity policies haven’t accounted for this. Social media use and cyber security measures will have to gain alignment fairly rapidly as organisations strive for a greater depth of security. For example, a disturbing new trend is “whaling” – where threat actors target senior executives online with ransomware, demanding money or using their information fraudulently. The challenge here is to protect an individual and not just their cyber presence.

Forensics will be even more important in the coming year. As people use different types of technologies in the digital enterprise, these technologies will all be increasingly subject to exploitation. As the stakes get higher, businesses will, for example, need to continuously scan the ‘Dark Web’ as cybercriminals become more bold and deliberate in their tactics.

The reality is that no enterprise, no matter its size, can avoid security incidents. Instead, the enterprise must be able to anticipate them, and have the intelligence data to identify and respond to these threats, often in real-time. Organisations should take a “one-two punch”: the first is to engage a managed security services provider – to provide details about possible or real threats to systems. The second is to augment these insights with deeper threat analysis and reporting. And this is where data will give organisations a much stronger security stance.


### Accelerate your digital business

  
digital infrastructure

  
hybrid cloud

  
workspaces for tomorrow

  
cybersecurity

 [dimensiondata.com](http://dimensiondata.com)







# Identity-Powered Security

## Balancing user access with company security

Security breaches are high risk. You need to spot, stop and protect sensitive information from all external and internal threats.

NetIQ® integrated solutions are designed to manage the identity and access lifecycle. We call our approach Identity-Powered Security, and it consists of three complementary disciplines:

- **Identity Governance Administration**

Provide correct access so users can do their job

- **Access Management and Authentication**

Stop insider credentials being abused by outsiders

- **Activity User Monitoring**

Detect and disrupt misuse of privileged rights

