CYBERSECURITY

INCIDENT RESPONSE

Speed is key in tackling data breach fallout

In the age of social media and public relations crises snowballing out of control, the ensuing hours after a data breach can make or break a company's reputation

Nick Easen

Massive cyberattacks appear to go in waves and we're probably due one soon. Marriott, British Airways, Facebook, Dixons Carphone are just some of the big names that have been smacked hard in the corporate face. Bruising data haemorrhages seem to be a regular occurrence, while the dreaded fallout on social feeds, tabloid headlines and 24-hour online media can be legion.

"Once more unto the breach, dear friends, once more" is not so much a line from Henry V and the Bard himself, but more a 21st-century hue and cry from the public relations, C-suite and cybersecurity teams as they clamour to shore up tattered brand images and stymie any financial losses.

"One of the first challenges in dealing with a cyberattack is time. Incidents can go viral and global in an instant. Organisations will be dealing with short timeframes to manage reputational risk, recover data and prepare a co-ordinated response to regulators, third parties and affected customers," says Dr Paul Robertson, cybersecurity, privacy and resilience director at EY.

We also have to face up to the fact we live in a post-GDPR world. Companies have 72 hours to fess up to a cyberattack or face crippling fines under the EU's General Data Protection Regulation. As the clock ticks in those early hours, the pressure can be extreme.

"Consumers are becoming increasingly savvy about the value of their data. Transparency, particularly when responding to breaches, will become even more crucial to business success in the future," says Tim Rawlins, director at NCC Group.

> **One of the first challenges in dealing with a cyberattack is time. Incidents can go viral and global in an instant**

There's no doubt that a proactive response must be delivered alongside an honest plan to tackle a breach, even if its knee jerk, otherwise it's carnage.

"The saying that 'a lie can travel halfway around the world before the truth has its shoes on' is very real when it comes to social media. A misrepresentation of the facts can become a 'fact' very quickly and is then often picked up by traditional news sources," warns Richard Horne, cybersecurity partner at PwC.

"Cyber-crises are also different to many others in that directly after the event, the affected organisation often has very few facts to work with. Maintaining stakeholder confidence when you have no facts is a challenge and especially because these facts can take days, weeks, even months to uncover."

At the same time, we live in an era when there's a toxic cocktail of high breach fatigue among consumers and low public trust in companies that hold our precious data. Arguably, it's how businesses have handled attacks globally that has led to this state of affairs.

"The reporting of incidents has generally been poor and often doesn't highlight the real scope of a data breach, with incident reports littered with non-definite words such as 'could have', 'might be' and so on," says Professor Bill Buchanan, cybersecurity expert at Edinburgh Napier University.

"In the case of British Airways, every customer should have stopped transactions on their credit card – in fact, it should have happened automatically – as the breach involved virtually everyone who entered their credit card details on their website over the period of the hack."

In the summer of 2018, the details of around 380,000 airline bookings were compromised when hackers obtained names, streets and email addresses, as well as credit card numbers, expiry dates and security codes; certainly enough information to steal from people's bank accounts. In textbook style, British Airways immediately contacted customers when the breach became clear.

"Within the incident report, you had to scroll down the page to see the advice related to credit cards. At the time, the announcement was your passport details were safe and that your card details were at risk. You can see that PR teams will try to soften the scope of a data breach, but this doesn't help the media or the general public understand the scope of an attack," says Professor Buchanan.

Look closer and you may realise that our data infrastructure has been built using methods created in the 20th century and we're now having to re-engineer our data-fed world to deal with security in the 21st, including the cloud, mass digitalisation of supply chains, the internet of things, robotics and artificial intelligence, as well as the merger between physical and cyber-realms, the so-called fourth industrial revolution.

Next-generation intelligence-driven security is needed. "Before a breach, businesses struggle to know whether they need to invest and struggle to understand what the impact of inaction will be on their business. They know this after a breach, of course, but at which point it's too late," says Nigel Ng, vice president of international sales at RSA Security.

Many organisations are now being more proactive and less reactive. As Cesar Cerrudo, chief technology officer at IOActive, puts it: "This is no longer an IT issue, but a business imperative." Although preparedness is more prevalent in the likes of say financial services than in healthcare.

Big companies now have so-called fire-response policies and cyber-breach simulations bringing IT, public relations and customer service teams together as they work on dry runs and responses. However, there's increasing realisation that a more holistic approach is needed.

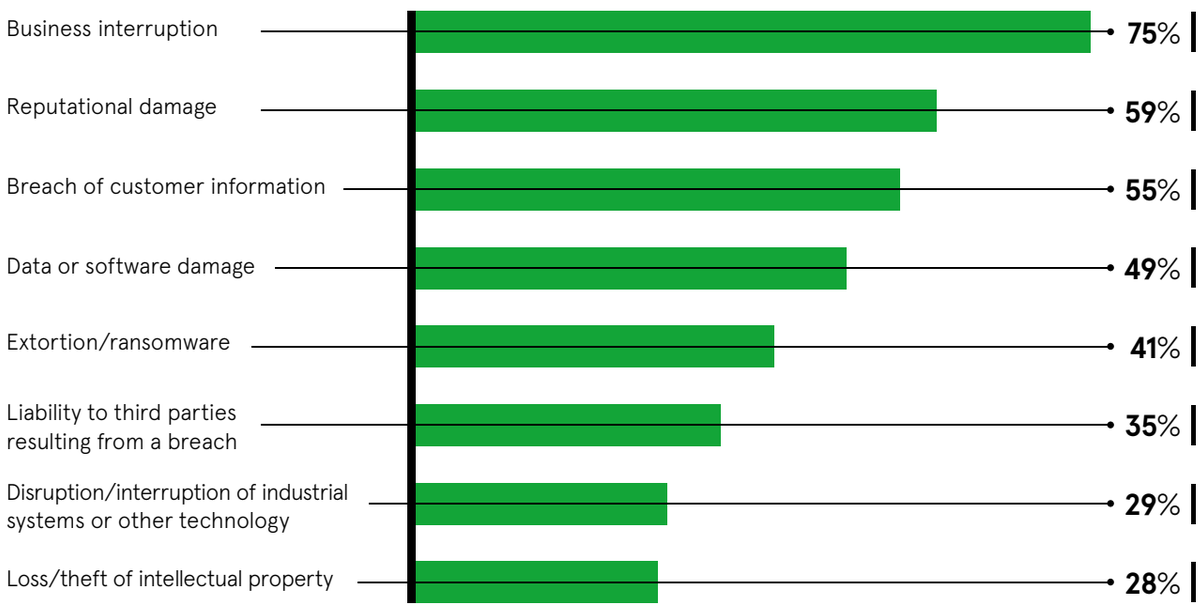
"Embedding security into an organisation's DNA goes far beyond just raising awareness or training people; everyone needs to understand how the business decisions they make can impact cyber-risk," says Mr Horne. However, this still doesn't tackle the issue of reviving public trust, which is sorely needed before the next round of breaches.

"It is often difficult to tell the difference between say a bank which invests heavily in their cybersecurity and one that doesn't," says Professor Buchanan.

"For those affected, it is often financial loss, which worries many people, and therefore we need ever-increasing levels of security. Our 'Wild West' of data-handling and data-mining needs to end sometime soon. Maybe there should be cybersecurity ratings for companies, where they would be extensively audited for the detection and response to incidents." There's a thought.

MOST CONCERNING CONSEQUENCES OF A CYBERATTACK

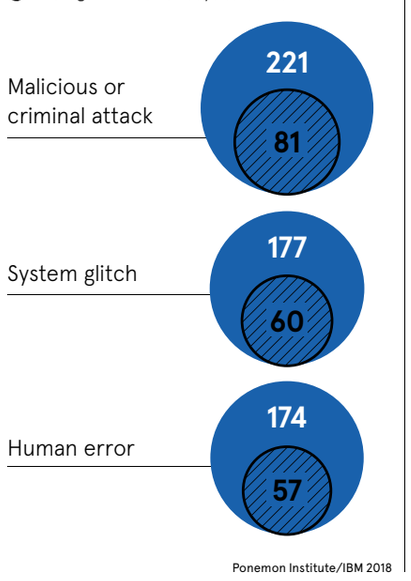
Percentage of executives who believe the following would have a big impact on their organisation



Marsh/Microsoft 2018

TIME TAKEN TO IDENTIFY AND CONTAIN A DATA BREACH, BY ROOT CAUSE

Survey of 477 companies that experienced a data breach in 2018



Ponemon Institute/IBM 2018

Distributed in
THE SUNDAY TIMES

Published in association with
airmic

Contributors

Davey Winder
Award-winning journalist and author, he specialises in cybersecurity, contributing to *Infosecurity* magazine.

Kate O'Flaherty
Freelance tech writer specialising in cybersecurity, her work has appeared in *The Guardian, The Times, The Economist, Forbes,* and *Wired UK.*

Matthew Staff
Former editorial director, he is now applying his multi-sector B2B experience across numerous industry titles.

Nafeez Ahmed
Investigative journalist and editor of *Insurge Intelligence*, he has contributed to *The Guardian, Independent, VICE* and *The Atlantic.*

Nick Easen
Award-winning journalist and broadcaster, he writes on science, technology, economics and business, producing content for *BBC World News, CNN* and *Time* magazine.

Nick Ismail
Content editor of *Information Age*, he writes for technology leaders, helping them manage business-critical issues for today and in the future.

Oliver Pickup
Award-winning journalist, he specialises in technology, business and sport, and contributes to a wide range of publications.

Tim Cooper
Award-winning freelance financial journalist, he has written for publications including *The Spectator, London Evening Standard, Guardian Weekly* and *Weekly Telegraph*.

raconteur reports

Publishing manager
Reuben Howard

Associate editor
Peter Archer

Managing editor
Benjamin Chiou

Head of production
Justyna O'Connell

Digital content executive
Fran Cassidy

Design
Grant Chapman
Sara Gelfgren
Kellie Jerrard
Harry Lewis-Irlam
Samuele Motta

Head of design
Tim Whitlock

/raconteur.net
@raconteur
@raconteur_london

raconteur.net /cybersecurity-2019

Commercial feature

CAUGHT IN THE CYBER CROSSFIRE

2017 attacks on Ukraine showed a domino effect of damage into enterprise networks worldwide

64 countries affected

$10bn in damages

An estimated **10%** of all computers in Ukraine were wiped

5hrs to spread across over 2,000 companies

INDUSTRIES AFFECTED

- Shipping
- Pharmaceuticals
- Financial
- Energy
- Health services
- Transportation

Companies must prepare for 'cyber cold war'

The burgeoning global trade war is set to trigger a series of cyber-espionage attempts between nation states, and enterprises are likely to be caught up in the crossfire. With current security approaches failing to prevent breaches, a paradigm shift is required

Growth of the internet in the 1990s fuelled an era of globalisation defined by a rapid pace of innovation, open trading and cross-pollination of technology across borders. However, populist movements in recent years have sought to reverse this tide and return to more protectionist postures. Fracturing trust among world leaders last year resulted in a rising number of trade sanctions and embargoes between nation states.

These trade disputes restrict nation states from acquiring technologies and intellectual property (IP) vital to their local industries and security, while enterprises in affected countries also risk losing access to new innovation and information.

The result is the emergence of a cyber cold war reminiscent of the late-1940s to early-1990s when nation states frequently acquired technologies and IP via espionage. But rather than sending in spies to physically steal information, the difference this time is the theft will be carried out through targeted data breaches launched remotely.

It's not only governments and security agencies that should be worried about these attacks because businesses are likely to be caught in the cyber-crossfire, according to Luke Somerville, head of special investigations at Forcepoint Security Labs.

"It's often IP supplied to governments by private organisations that other nation states want to get their hands on, such as the designs for components, which may make their way into critical tools and infrastructure," he says. "If they're no longer able to access that expertise on the open market, they will target those companies with a high calibre of cyber-attack to steal them instead.

"Even if your company has no direct link with a target, you could still be affected. Beyond the general risk of collateral damage – the malware used on the 2017 cyber-attacks on Ukraine, for example, spread globally – you may be a target if you supply a government supplier or are even further down the chain. Compromising your systems may make it easier for the attack to flow up the supply chain and reach the real target."

The cyber cold war means enterprises must ensure they have the right security in place to protect themselves from these kinds of cyber-attacks and prevent theft of their IP. Businesses certainly can't be accused of not trying to do this as worldwide spending on information security products and services will exceed $124 billion this year, according to Gartner, but established approaches appear to be failing.

The number of vulnerabilities, data records, new malware samples and malicious programs continue to grow each year, and large-scale data breaches are covered in the media on a regular basis. Executives are kept awake at night worrying about the impact a cyber-attack could have on their business and are well within their rights to ask why the extensive funding they're putting into security is not providing the protection they need?

> **The answer lies in understanding the points at which people and data interact**

"The current paradigm is broken," says Duncan Brown, chief security strategist, Europe, Middle East and Africa, at Forcepoint. "There are tonnes of technology deployed out there, which is effective to a degree, but not stopping the breaches. The paradigm is to constantly try to second guess the hackers, essentially by looking in the rear-view mirror, but it's a fool's game.

"The attack community is much more creative than that. The paradigm needs to change. We can't keep spending all this money where it is palpably not working. Broadly, there are two main ways to prevent theft of your critical data: hope and pray, or get on the front foot and organise yourself to expect an attack. Many are still in the former mindset."

Forcepoint, a cybersecurity software provider, advises all companies to expect to be breached and to plan accordingly with a full incident response plan in place. Often the worse damage comes not from the attack itself, but the way the organisation responds. Equifax and TalkTalk both suffered significant damage to their brands by responding to their respective data breaches in a poor and knee-jerk manner.

In the world of cybersecurity, knowledge sharing is also crucial. While many organisations tend to prefer to isolate themselves and keep intelligence in-house, this can restrict the overall ability of businesses to prepare effectively. A competitor to your products and services is still an ally in a cyber cold war and should be seen that way.

Most of all, however, companies must now be prepared to switch their whole approach to security, focusing on understanding where their valuable assets are rather than on a physical perimeter or stopping attacks from getting in.

"The technology keeps being superseded by new threats," says Mr Brown. "When a new threat vector is revealed, everybody scrambles around trying to fix it. We'll never have a 100 per cent view on the threat landscape, so we need to flip the paradigm and focus on what we can control."

The answer lies in understanding the points at which people and data interact. Human interactions with data underpin every organisation, so tracking and analysing those interactions in detail enables companies to understand what's abnormal. Once they know what's abnormal, they can quickly and accurately detect when something is wrong.

Forcepoint calls this approach human-centric behaviour analytics. Downloading a certain file may be normal for one employee, but abnormal for another. Understanding that context enables organisations to know what it is in control of and, by establishing a base line, determine what is safe from what is unsafe. It puts them on the front foot.

"We're trying to orientate the security strategy in an organisation around behaviour of people and their interaction with critical data, then use the technology to provide the telemetry that informs the model," says Mr Brown. "By understanding what the normal behaviour pattern is you can apply different risk assessment to each user.

"Lots of companies really can't predict how they're going to be attacked, but they worry about it a lot and this vulnerability stops business from doing what needs to be done. By understanding user behaviour and the key data assets, you can free up that business. Human-centric behaviour analytics is the core engine that gathers the telemetry, and by gathering all of the telemetry from our various security systems, we can get a very accurate sense of how users are behaving on a network and interacting with data."

>$1trn to be spent on cybersecurity over the next seven years

Cybersecurity Ventures

88% of surveyed Forcepoint customers are concerned about potential attacks on the critical infrastructure their organisation relies on

TechValidate. TVID: 900-9BB-779

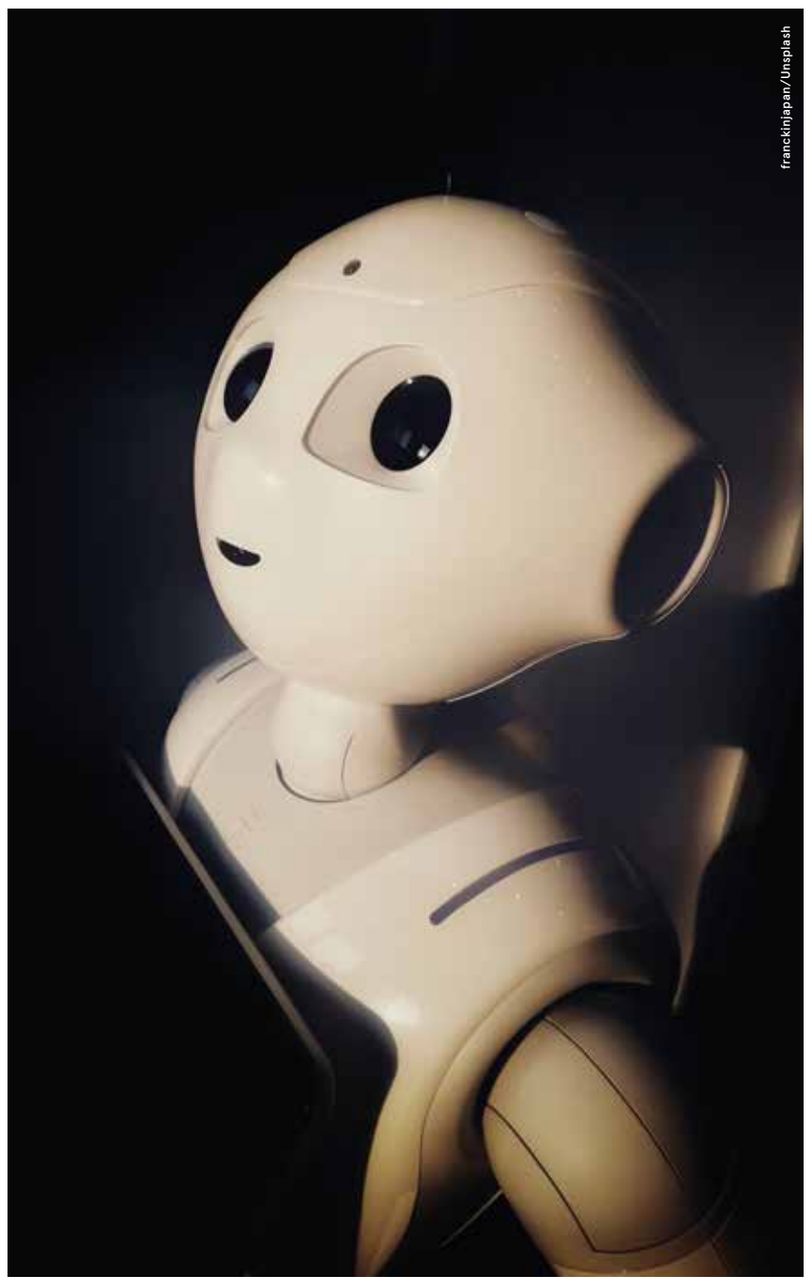
For more information please visit www.forcepoint.com

FORCEPOINT

ARTIFICIAL INTELLIGENCE

Fighting fire with fire: the dark side of AI

Use of artificial intelligence (AI) in cybersecurity is enabling IT professionals to predict and react to emerging cyberthreats quicker and more effectively than ever before. So how can they expect to respond when AI falls into the wrong hands?



franckinjapan/Unsplash

Nick Ismail

Imagine a constantly evolving and evasive cyberthreat that could target individuals and organisations remorselessly. This is the reality of cybersecurity in an era of artificial intelligence.

AI has shaken up the cybersecurity industry, with automated threat prevention, detection and response revolutionising one of the fastest growing sectors in the digital economy.

However, as is so often the case, there's a dark side. What if cybercriminals get their hands on AI, and use it against public and private sector organisations?

"The edge in cyberdefence is speed. AI is transforming cyberdefence, allowing businesses to detect evermore complex threats from evermore sophisticated attackers," says Andre Pienaar, founder of C5 Capital.

Nevertheless, the more AI security solutions, the more cybercriminals will adopt the technology; it's a case of fighting fire with fire. Newton's Third Law describes the situation aptly: for every action, there is an equal and opposite reaction.

Before the advent of AI in cyberattacks, the security landscape was already challenging. But the use of AI in targeted criminal attacks has made cybersecurity more treacherous. Not only are attacks more likely to be successful and personalised, but detecting the malicious piece of intelligent code and getting it out of your network is likely to be much more difficult, even with AI security in your corner.

Adoption of AI by cybercriminals has led to a new era of threats that IT leaders must consider, such as hackers using AI to learn and adapt to cyberdefence tools, and the development of ways to bypass security algorithms. It won't be long before a continuous stream of AI-powered malware is in the wild.

"In the short term, cybercriminals are likely to harness AI to avoid detection and maximise their success rates," says Fraser Kyne, Europe, Middle East and Africa (EMEA) chief technology officer at Bromium. "For example, hackers are using AI to speed up polymorphic malware, causing it to constantly change its code so it can't be identified. This renders security tools like blacklisting useless and has given old malware new life."

What about some particular threats? AI-based malware, such as Trickbot, will begin plaguing organisations more regularly. This particular Trojan, a piece of malicious code that can enter a network in a way not dissimilar to Homer's Trojan Horse, is able to propagate and infect systems automatically. Changes can be made by the malware's authors on the fly, so it is very difficult to detect and remediate against.

TOP BENEFITS OF AI IN CYBERSECURITY

Percentage of cybersecurity professionals who agreed with the following

- AI-based technologies provide deeper security than what humans alone can provide: **60%**
- AI-based security technologies simplify the process of detecting and responding to security threats and vulnerabilities: **59%**
- AI-based security technologies will decrease the workload of IT security personnel: **34%**

Ponemon Institute/IBM 2018

> **Hackers are using AI to speed up polymorphic malware, causing it to constantly change its code so it can't be identified**

85% of organisations have not fully deployed automation in their cybersecurity processes

Ponemon Institute/IBM 2018

The autonomous benefits of AI security apply to cybercriminals and their nefarious activities, enabling them to analyse large stolen datasets in the blink of an eye and in turn create personalised emails or messages to target unsuspecting individuals.

AI trumps human every time as was shown in an experiment conducted by two data scientists from security firm ZeroFOX. The AI, called SNAP_R, sent spear phishing tweets to more than 800 users at a rate of 6.75 tweets a minute, capturing 275 victims. The human, by contrast, sent malicious tweets to 129 users at 1.075 tweets a minute, capturing only 49 individuals. It's no contest and another reason why hackers are adopting AI as it takes less effort and yields greater rewards.

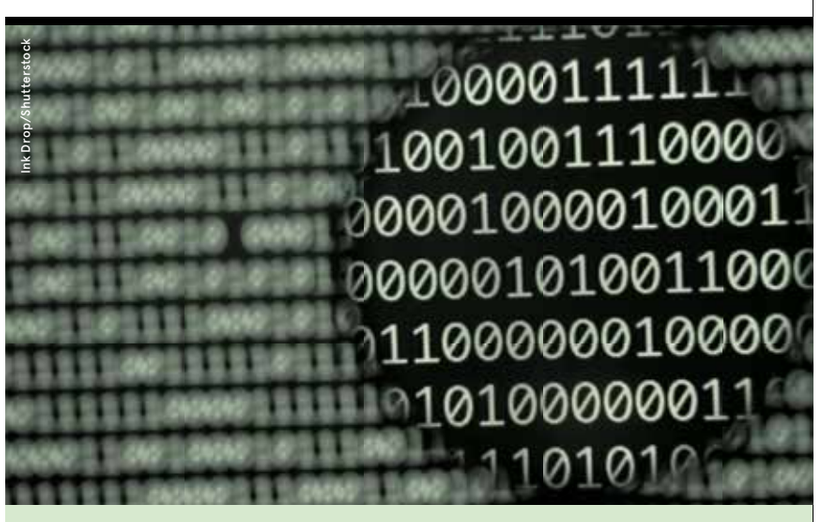
"Traditionally, if you wanted to break into a business, it was a manual and labour-intensive process," says Max Heinemeyer, director of threat hunting at Darktrace. "But AI enables the bad guys to perpetrate advanced cyberattacks, en masse, at the click of a button. We have seen the first stages of this over the last year with advanced malware that adapts its behaviour to remain undetected."

To cope with this emerging AI security threat, organisations need to adapt their security strategies to not only accommodate AI and innovation, but also prioritise protection of the corporate gold: data. In the digital economy, the main aim of hackers is to exploit data; it's where the money is. Also, crucially, AI does not represent a silver bullet.

"Organisations should use data-centric security models underpinned by information assurance to protect data, as well as continue all the innovations surrounding AI, while continuing to adopt a prevent, detect and response strategy," says Dan Panesar, vice president and general manager, EMEA, at Certes Networks. "This combination is the best way for organisations to protect themselves in this digital world."

Cybersecurity, while not the only consideration, must be front and centre in the minds of IT leaders. The consequences of a breach are certainly great enough to keep any chief executive awake at night.

Make no mistake, we're engaging in cyberwar, when AI is both the weapon of mass destruction and part of the sophisticated solution. And the AI arms race is just beginning.



Ink Drop/Shutterstock

Isolating the threat

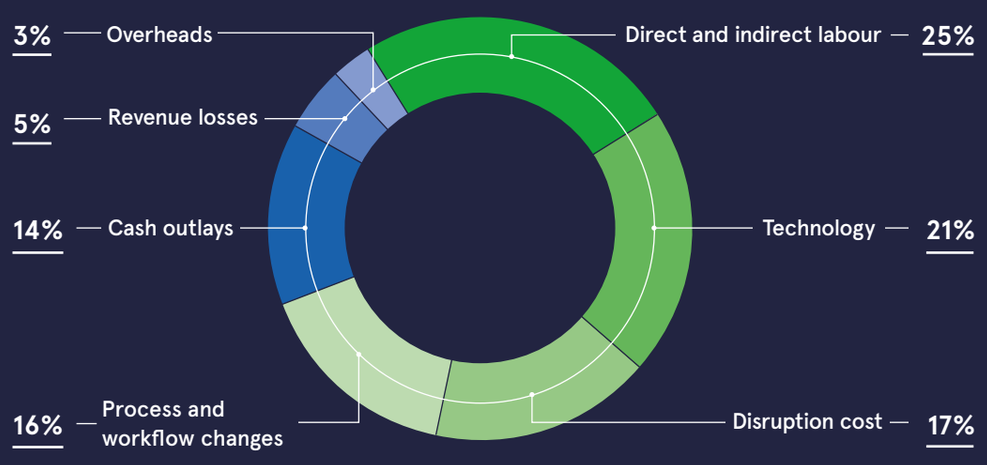
Application isolation, developed by Bromium, is a unique technology that renders malware harmless by allowing it to execute fully in a completely isolated, contained environment. As the malware is trapped in a micro virtual machine, it has no means of escape and no data to steal, ultimately preventing damage to the enterprise. This helps to protect against the most common attack vectors, such as malicious downloads, plug-ins and email attachments. It also provides unique threat data. By allowing malware to run, security teams can track the full kill chain to see what it is trying to do or steal. As this data is captured in the virtual machine, AI can then be applied to spot patterns, identify gaps and recommend next best actions for response. Knowing how an attack works enables organisations to deal with it in minutes and mitigate the threat. However, it is important this solution is used alongside other protection tools to secure an organisation.

THE INSIDE THREAT

Employees, contractors and third parties with access to company data should all be considered when it comes to enterprise security. And while malicious insiders – such as disgruntled workers out to cause harm – pose a serious threat, accidental lapses in security through carelessness or negligence are still to blame for a large portion of data breaches and other cyber incidents

BREAKDOWN COST OF INSIDER INCIDENTS

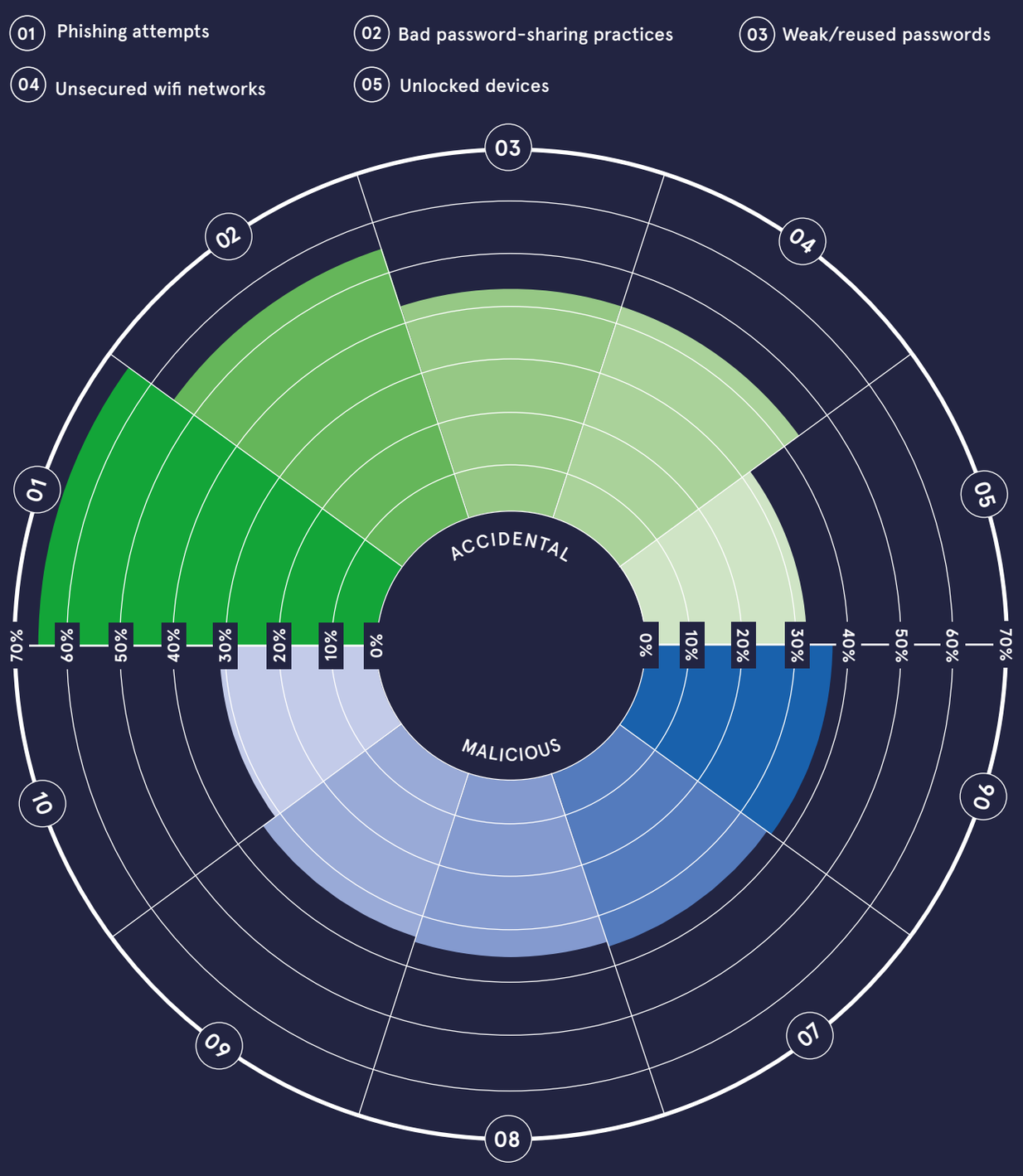
Taken from a survey of 3,269 separate incidents from large organisations in 2018



Ponemon Institute 2018

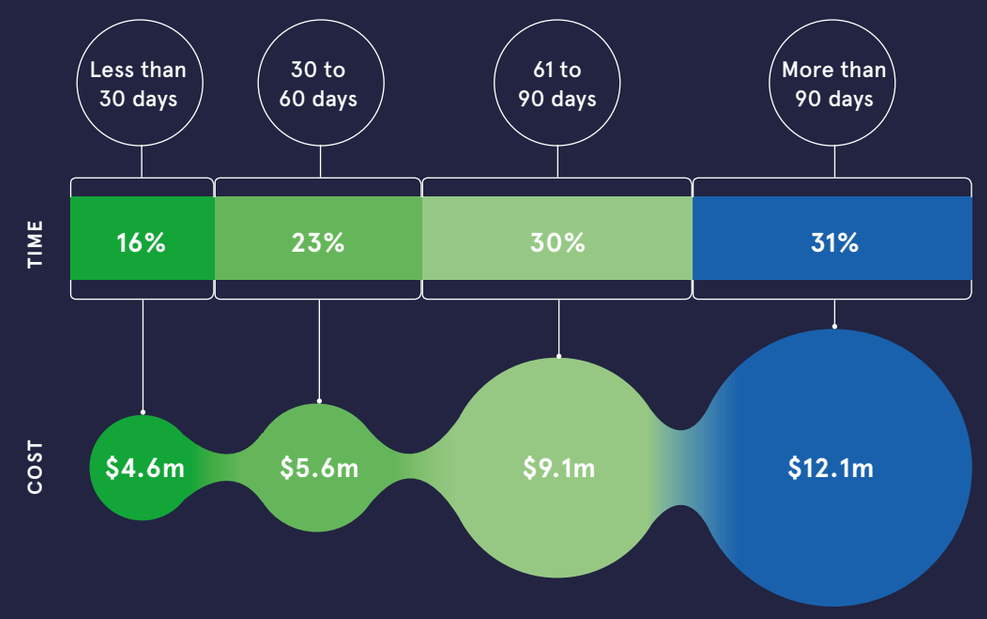
WHAT'S ENABLING INSIDER THREATS?

Percentage of cybersecurity professionals who believe the following are enabling insider threats



TIME AND COST TO CONTAIN INSIDER INCIDENTS

Taken from a survey of 3,269 separate incidents from large organisations in 2018



Ponemon Institute 2018

DETERRENCE AND DETECTION

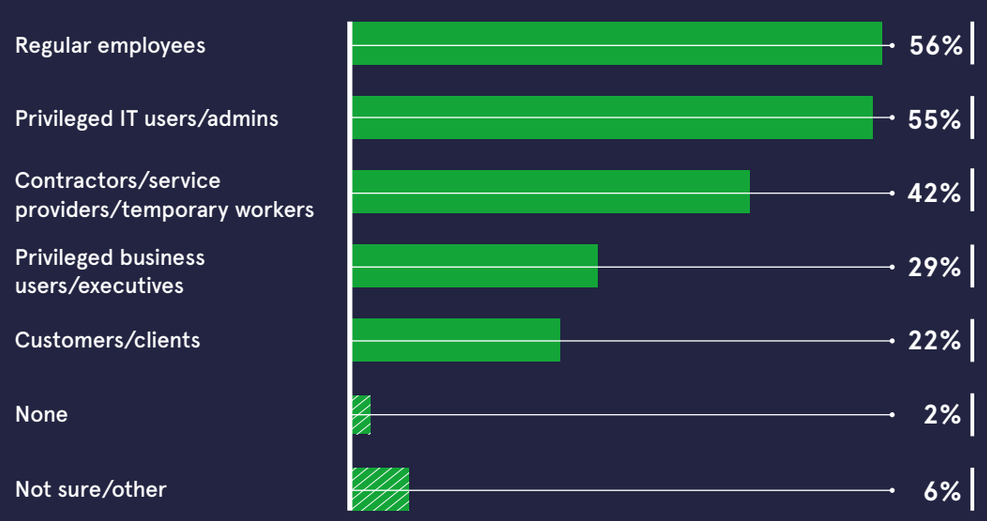
Most common controls companies have in place, ranked

Deterrence		Detection	
01	Data loss prevention	01	Intrusion detection and prevention
02	Encryption of data	02	Log management
03	Identity and access management	03	Security information and event management
04	Endpoint and mobile security	04	Predictive analytics
05	Cloud access security	05	User and entity behaviour analytics

Cybersecurity Insiders 2018

WHAT INSIDERS LOOK LIKE

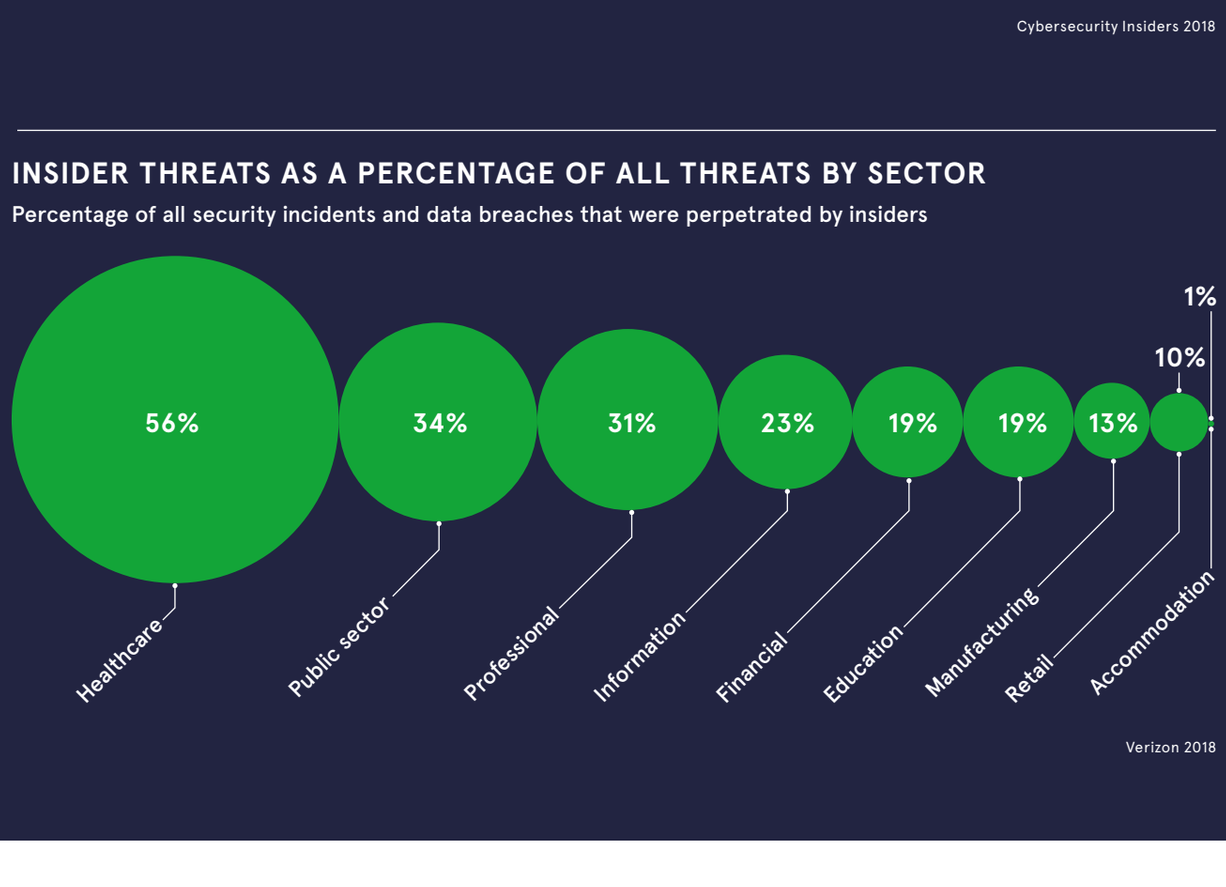
Percentage of cybersecurity professionals who say the following presents a security risk



Cybersecurity Insiders 2018

ACCIDENTAL BREACHES WORRY EXPERTS JUST AS MUCH AS MALICIOUS ATTACKS

Most concerning insider threats to cybersecurity professionals



Cybersecurity Insiders 2018

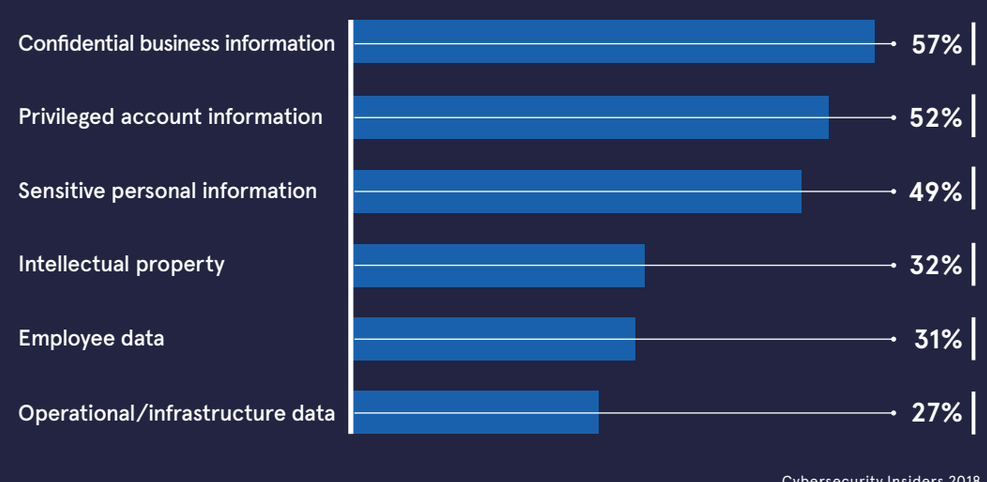
INSIDER THREATS AS A PERCENTAGE OF ALL THREATS BY SECTOR

Percentage of all security incidents and data breaches that were perpetrated by insiders

Verizon 2018

TARGETS OF INSIDER THREATS

Types of data most vulnerable to insider attacks



Cybersecurity Insiders 2018

EMPLOYEE ENGAGEMENT AND INSIDER THREATS

Five reasons why staff engagement needs to be part of your cyberdefence

Optimising employee engagement has many benefits, not least bolstering cybersecurity and reducing the likelihood of insider threats

Oliver Pickup

Education

While almost three quarters of cyberattacks are perpetrated by people outside an organisation, more than a quarter involve insiders, according to Verizon's *2018 Data Breach Investigations Report*. Furthermore, human error is the root cause of close to one in five breaches. Education of the workforce, therefore, is critical.

"The vast majority of data breaches can be traced back to an original phishing email, or series of emails, whereby employees are used as targets to obtain data," says Luke Vile, cybersecurity expert at PA Consulting. "This first contact is often a 'stepping stone' cyber-approach.

"Engaging employees on cybersecurity ensures they are more alert during these early-stage phishing attempts, and when alert they are more likely to report contact and stop a breach before it happens."

Moreover, Matthew Buskell, assistant vice president at Skillsoft, believes organisations cannot rely on the IT or security departments. "A recent (ISC)²-commissioned survey identified a glaring skills gap on the horizon," he says, "projecting that the overall cybersecurity skills shortage is set to rise to 350,000 workers in Europe by 2022."

Happiness

It's impossible to quibble with the logic that a happy worker is a productive worker. A happy, committed worker is also unlikely to turn rogue when it comes to cybersecurity. "A main reason for companies to invest in employee wellbeing and engagement is that discontented staff pose a clear security risk, especially when resigning or leaving the organisation," says Louis Smith, insider threat specialist at Fidelis Cybersecurity.

"Individuals who feel wronged by the company might feel they have something to gain from sabotaging intellectual property or conducting IP theft."

Jake Moore, cybersecurity expert at ESET, agrees. "Employees are your best asset, yet they are also the weakest link. They are able to spot signs that not even artificial intelligence can see, such as a begrudged staff member, and pick up on such signs," he says.

Most employees demand flexible working and PA Consulting's Mr Vile says organisations must ensure this policy, to boost happiness, is secure. "With many employees now routinely working from home, or working out of multiple offices, it extends the digital boundaries of an organisation far beyond its traditional office space," he points out. "Whenever digital boundaries are expanded in this way, it makes it harder for security to stretch and cover everybody."

Togetherness

Now more than ever, thanks to the introduction of cloud solutions, cybersecurity simply has to be a company-wide commitment, from top to bottom. "Some 92 per cent of cybersecurity teams surveyed in *The Oracle and KPMG Cloud Threat Report 2019* said they were concerned that individuals, whole departments or lines of business were in violation of their security policies for the use of cloud applications," says John Abel, vice president of cloud and innovation at Oracle.

"In almost half of those cases, the unauthorised apps being used resulted in improper access to data and the introduction of malware that can quickly spread across an organisation.

"The increasing number of connected devices and the growth in mobile working has led to an exponential increase in opportunities for cybercriminals, making it even more important for employees to be engaged and prepared to spot threats.

"Our research also revealed almost one in four companies that had been the subject of a cyberattack in the past two years said 'increasing employee awareness and training' led to the biggest improvement in the security of the organisation, showing just how powerful employee engagement programmes can be."

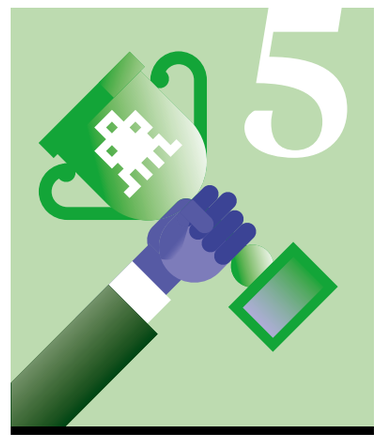
Empowerment

If an organisation's cybersecurity is only as good as its weakest link, it is crucial to empower all employees and give them a reason to be diligent. "Encouraging employees to question requests, double check on records and be just a little paranoid are all critical in improving overall cybersecurity posture," says Aaron Zander, head of IT at HackerOne.

"Companies that blame employees for poor passwords or bad behaviour with email aren't spending enough time, money or energy driving home security. Preventing phishing attacks can be closely tied to corporate culture."

Behaviours need to change, says Mr Zander, who asks: "Is it normal for an executive to demand something like a bank transfer to a vendor, or a large purchase from a random site with no questions asked either because of fear or sternness? Welcome to phishing heaven. It's up to IT and security teams to enable, empower and educate employees as part of strengthening the weakest links."

Audra Simons, head of Forcepoint Innovation Labs, adds: "Engaged employees tend to be more conscientious, compliant and ultimately become a positive force within the organisations."



Motivation

In the same way an organisation with a clear and inspiring vision is more likely to attract and retain talent, by educating the workforce about cybersecurity using a fun and engaging approach can reap big rewards. "Studies show that the stick doesn't work," says PA Consulting's Mr Vile.

"One innovative solution is to go beyond mere cyber-awareness training and develop more 'gamified' approaches, boosting the engagement of employees and leaders through exciting role plays and scenarios involving 'games' with cyberattacks and attackers," says Thomas Calvard, lecturer in human resource management at the University of Edinburgh Business School.

Adenike Cosgrove, cybersecurity strategist at Proofpoint, took this approach with Royal Bank of Scotland (RBS) staff. "Through an ongoing programme of ethical phishing simulations based on actual fraudulent messages from the wild, RBS determined their employees' susceptibility to real-world attacks," she says.

"Users falling victim to these fake phishing messages on multiple occasions received comprehensive training, which led to a significant 78 per cent reduction in the likelihood of users clicking on nefarious campaigns."

CLOUD

Experts fret as cloud attacks intensify

As the adoption of cloud technology surges, protecting organisations against evolving threats on internet-facing infrastructure has never been more critical

Oliver Pickup

Marnix Hogendoorn /Unsplash

Multifarious benefits of cloud computing make the disruption of digital transformation worthwhile, business leaders are assured. However, a recent torrent of automated attacks on cloud infrastructure's vulnerabilities has precipitated a somewhat gloomy outlook, raining on the cloud's silver lining.

In September, for example, Xbash – an advanced, data-destructive malware strain that combines cryptomining, ransomware and botnet capabilities – was identified. How can organisations that have come to depend on the cloud for the smooth running of their business combat these morphing, multi-vector cyberthreats?

"Cloud security has never been more critical," warns Max Heinemeyer, director of threat hunting at Darktrace, a global leader in artificial intelligence-powered cybersecurity. "Xbash is a very sophisticated example of an automated attack because it can target both Linux and Windows servers, and has multiple payloads.

"Automated attacks against internet-facing infrastructure, like Xbash, are not new. What has changed is that the number of devices that are internet facing and potentially vulnerable has increased exponentially. This is in no small part due to the advent of the cloud. Attackers are innovating rapidly, and we can expect attacks on the cloud to get faster and more furious."

Charaka Goonatilake, chief technology officer of Panaseer, another cybersecurity giant, agrees. "What's different in the cloud era is the ease with which exploitable software can be spun up and exposed to the world on the internet," he says.

"Vulnerability search engines, such as Shodan, continually trawl the internet for these exploitable weaknesses and make it effortless to identify masses of targets to attack. Combined with the fact that highly sophisticated malware, such as Xbash, is readily available off the shelf, makes for a very low barrier for nefarious actors to carry out lucrative attacks from the comfort of their own homes."

Hardik Modi, senior director of threat intelligence at Netscout, expands upon this worrying theme. "There are numerous instances of such open-source packages like Hadoop, Mongo and ElasticSearch which remain exposed to the internet, and there have been waves of reports of installations that have been exploited and encrypted," he says.

"This can have severe consequences for businesses of all sizes, since they may not be in a position to recover such data. Indeed, our telemetry shows a Hadoop YARN installation is attacked about once a minute. A vulnerable installation would be attacked immediately. These measures vary wildly across the industry and as a result there remain huge exposures for the internet ecosystem at large."

Alarming figures illustrate the growing issue. "In January, 1.8 billion records were leaked online," says Dr Guy Bunker, senior vice president of data security organisation Clearswift. "Today it is possible to collect and analyse billions of pieces of sensitive data in almost no time at all. It can be transferred across the internet to a partner who shares it with another and another, further enriching it with more data.

"These large datasets are not only useful for business, they are also a honeypot for cybercriminals who will steal it and then sell the information on the dark web. Security is only as strong as the weakest link."

Adam Philpott, McAfee's president, Europe, Middle East and Africa, points out C-suite ignorance. "We currently estimate that the average organisation generates over 3.2 billion events per month in the cloud, of which 3,217 are anomalous and 31.3 are actual threat events," he says.

"Also, most organisations underestimate how many cloud services they actually use, with the average using approximately 1,935, a figure that has seen a 15 per cent growth from last year. In contrast, the average organisation thinks it uses just 30 cloud services."

Consider that the number of connected devices is expected to rise to 20 billion by next year, according to Gartner, organisations will use some 40 per cent of these and each one opens up a new vulnerability. Gartner also projects worldwide public cloud growth of 17 per cent this year. How then can organisations maintain adequate cybersecurity in this increasingly vicious online war zone?

Improving general cyber-hygiene and significantly greater education in this area, from top to bottom of an organisation's hierarchy, is imperative. Adam Louca, chief technologist for security at IT infrastructure provider Softcat, says: "The current cybersecurity skills gap means defending cloud infrastructure from compromise is one of the biggest challenges of modern business.

"Cloud companies must do more to educate their customers on best-practice security configuration. Businesses must continue to invest in security skills training, and onboard new talent to close the widening gap between their security needs and the resources they have to protect themselves."

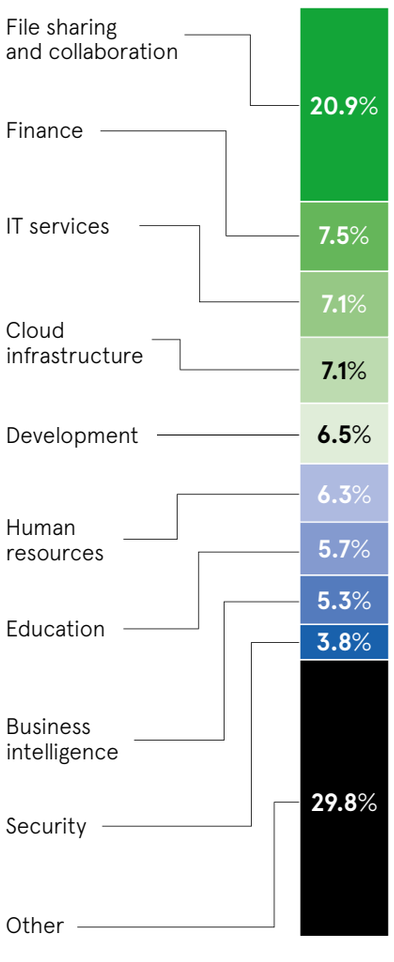
Another level of protection is gained by using tech against tech, says Alan Duric, co-founder of Wire, an end-to-end encrypted communication and collaboration platform. "Automated attacks on cloud structures are directly related to businesses using insecure and unreliable communications platforms like email, Slack and WhatsApp," he claims.

"Firms need to invest in secure communications platforms that are end-to-end encrypted, while ensuring all mobile devices used by the business are hard-wired for security, and built with security and privacy from the ground up."

It's clear that those who take a breezy attitude to cloud security risk being blown away in this stormy climate.

WHAT THE CLOUD IS USED FOR

Percentage of cloud services in use by category



McAfee 2019

21%

of all files in the cloud contain sensitive data

McAfee 2019

ESB Professional/Shutterstock

How to improve cloud defences

What should organisations be doing to shore up their cloud security defences? "They need to harden their cloud applications and infrastructure, and incorporate processes that continuously check enterprise applications for vulnerabilities," says Dave Klein, senior director of engineering and architecture at cloud and datacentre security specialist Guardicore.

"Further, they must incorporate patch, kernel and application updates into the provisioning and management scripts they use to spin up workloads within the clouds. Additionally, application designs need to be modified to add two-factor authentication for exposed services.

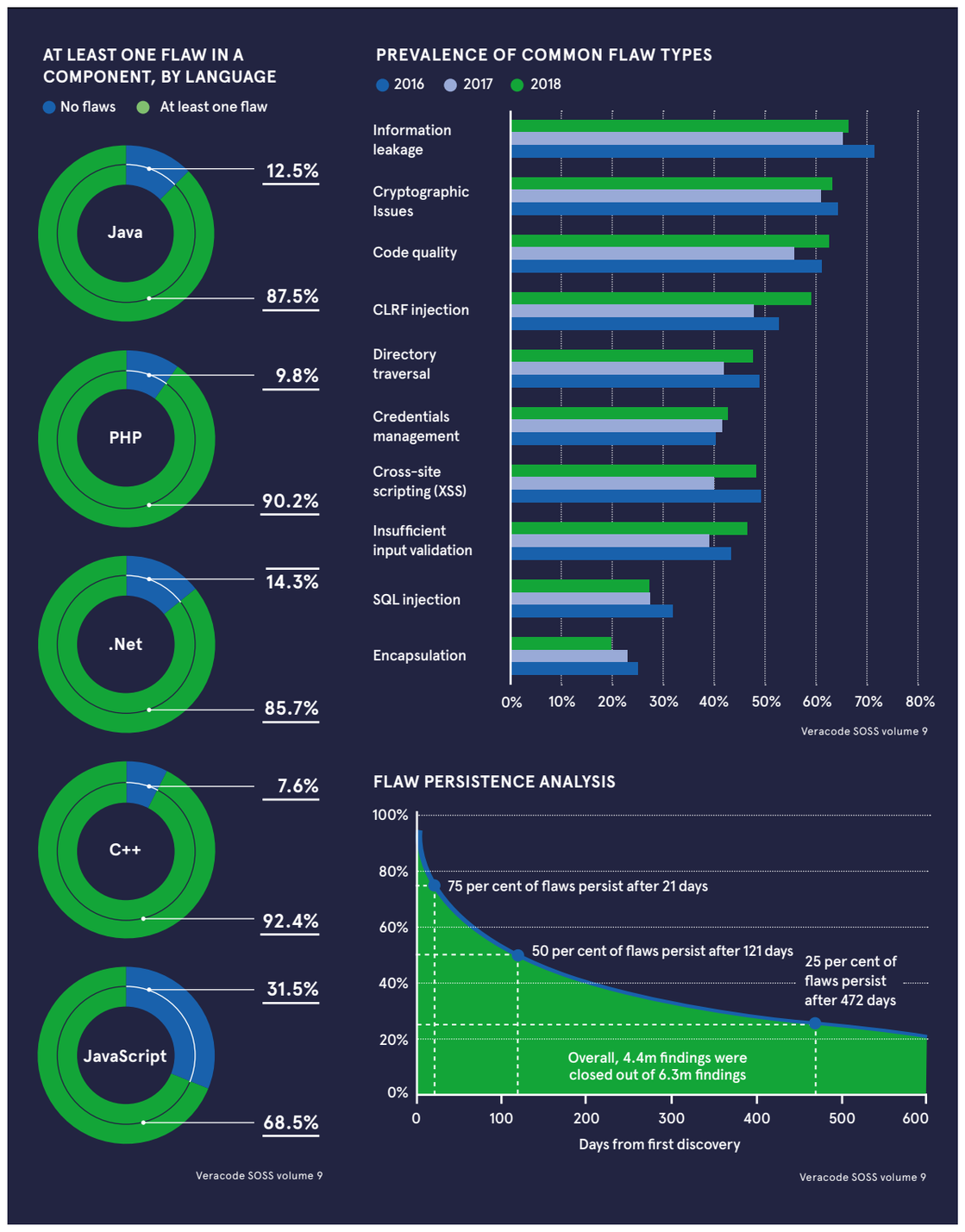
"Finally, since current cloud topologies are woefully lacking in segmentation, leaders absolutely must improve their segmentation game. Even by taking just the very basic steps to isolate, segment and micro-segment their cloud environments, leaders will impede an intruder's lateral movement and thus make it harder for attackers to succeed."

Dr Guy Bunker at Clearswift urges security professionals to "start thinking like their attackers". He asks: "How can they make it as difficult as possible to obtain the information and then to use it?"

Encryption is part of the solution. McAfee's Adam Philpott believes a collective, proactive approach is critical. "I would suggest auditing your Amazon Web Services, Azure, Google Cloud Platform or Infrastructure as a Service configurations," he says.

"Further to this, try to understand where your most sensitive data lives, and assess your access and sharing privileges. Once you have an understanding of this, lock down and apply data loss prevention to your most sensitive locations. Remember, if your data is a collaborative effort, so should your security be."

"What has changed is that the number of devices that are internet facing and potentially vulnerable has increased exponentially



Software leaves businesses open to hackers

The rise of open source software has provided a wealth of benefits for developers and businesses alike. But a lack of knowledge around how to write secure code, and use code from open source libraries securely, is causing enterprises to unwittingly allow hackers to compromise their systems

Consumer demand for internet-connected devices and the software applications that power them has rocketed in the last ten years. Smart applications now spread beyond smartphones into other devices, with web-enabled television, doorbells and security cameras increasingly commonplace. Software is a pervasive and crucial driver of innovation in commerce, helping organisations to be more agile and competitive.

The functionality of these devices and applications are determined by source code written by developers. According to the *AppSec Market Report,* around 111 billion lines of new software code were created in 2017. Within that massive volume of new code inevitably comes millions of software vulnerabilities and the security problems compound themselves with age.

The growing reliance on software in both business and society means data breaches are more impactful than ever and hackers are actively targeting vulnerabilities in the code. In Verizon's *Data Breach Investigations Report 2018,* web applications were identified as the most common source of data breaches and security incidents.

"Software applications are the prime target for attackers who want to get hold of an enterprise's assets and data," says Paul Farrington, chief technology officer, Europe, Middle East and Africa, at Veracode. "Web and mobile applications account for more than a third of data breaches, and attacks at the application layer are growing by about 25 per cent annually."

While 20 years ago software was mostly developed in-house using custom code, Gartner forecasts that seven out of ten applications are now running on open source databases.

Developers face overwhelming pressure to push out more software in shorter timeframes. Open source libraries can help by providing pre-built pieces of code that deliver specific functionality without having to build it from scratch. Consequently, 90 per cent of the code in many applications may originate from open source libraries. Open source software enables developers to fulfil business requirements more quickly and at less cost, but also introduces new risks.

When software is released as open source, it means the original author intends to give the code to developers to use freely, study and enhance. The amount of collaboration these projects can foster brings forward some of the greatest advancements in tech and it makes the software more accessible for individuals who cannot afford licensing fees.

The benefits of open source code can be so alluring that businesses forget about the risks involved with using public, unvetted chunks of software throughout their applications. Vulnerabilities in open source code are prized by hackers simply because of the prevalence of their use. Once a hacker discovers a vulnerability in a widely used open source package or library, they can exploit potentially thousands of systems running that code, amplifying by many degrees the impact of the vulnerability.

"It's really key to ensure developers not only think about the theoretical risk, but are also given tools to highlight the proven risks that exist in the software

According to Veracode's *State of Software Security* report, 88 per cent of Java applications contain at least one vulnerable open source component. This is noteworthy because just a single vulnerability in a piece of open source code can hit hundreds of thousands of applications.

"The open source community is really exploding and the desire for businesses to move faster is encouraging developers to make use of open software, which reduces the cost for enterprises and means delivery timelines can be hit faster than ever before," says Mr Farrington, who predicts there are more than five million unique open source components that exist in various software repositories developers interact with. "Soon, this will become hundreds of millions because of the rate of contribution from developers," he says.

Developers are no doubt aware of the security flaws in open source software. For example, the Apache Struts vulnerability was behind the massive data breach that exposed the personal information of 143 million Americans in March 2017. But while they may appreciate the imperative of creating secure code, knowledge of how to do so is lacking.

Education and awareness will ultimately empower development teams to improve how they create secure code. Veracode provides tools that enable developers to identify and correct security defects within seconds of writing code, while also telling them whether or not the open source building blocks they are using have any vulnerabilities in them.

Automation technologies such as artificial intelligence and machine-learning are accelerating the ability to look for defects in software, but it will be an appropriate balance between machines and humans that is most successful. While computers are excellent at looking for the traits of potential defects in data at speed and scale, they can't do without our human ability to prioritise how to address and remediate flaws.

"We use machine-learning to identify and pinpoint potential vulnerabilities with ever-increasing accuracy," says Mr Farrington. "However, humans are great at finding the sequence of steps hackers must undertake to compromise that system. We use the appropriate blend of automation and human ingenuity. We call these people manual penetration testers, looking for security defects to prove they exist in systems."

Developers must ultimately think about where the software will sit once it goes into production or lands on a user's device. Applications may exist in hostile environments, far longer than originally envisaged, and hackers may do anything to subvert them. As such, developers should seek an understanding of secure code and work in tandem with security teams to remove friction from the development process.

"As the use of containers continues to drastically reduce the time required to deploy and scale software, we are at the forefront of developing techniques to ensure we secure the applications that exist in containerised environments," says Mr Farrington. "However, addressing the problem at source, when the developers actually write the code, is going to be how we address the problem at scale.

"It's really key to ensure developers not only think about the theoretical risk, but are also given tools to highlight the proven risks that exist in the software. Veracode pinpoints what we call the 'vulnerable methods' so we can show developers the line of fire between the code they write and the security exploit that is just waiting to happen in the open source software. That's a game-changer for software development teams who don't have time to deal with noise."

To get a clear picture of the state of software security, including data on open source risk, which vulnerabilities peers in your industry are finding most often, and how organisations are reducing their software risk, please download Veracode's *State of Software Security Volume 9* at www.Veracode.com/sossreport

VERACODE

Commercial feature

Boardrooms seek well-rounded approach to cybersecurity and privacy

With buy-in from the very top, organisations are merging security, risk and governance to form a holistic view of the threats they face and a broad solution to achieving protection

The crucial relationship between an organisation and its customers has been increasingly defined by data in recent years as new insights breed better products and services. However, this has also meant fears of a damaging data breach have sharply elevated, making it a board-level issue and a concern across the whole business.

This has also forced organisations to re-evaluate their approach to security, risk and governance, which were typically viewed and managed as separate domains. New requirements, such as the European Union's General Data Protection Regulation, have brought the areas of security and privacy closer together and empowered people to be more aware of how their personal data is being used.

In this new reality, keeping security, risk and governance separate is detrimental to an organisation's overall ability to protect itself. Companies implement security controls to enforce appropriate activity, but knowing what's appropriate and determining what needs to be done requires governance and a strong understanding of the risk levels.

"They're all part and parcel of the same process," says Travis Grandpre, senior director of security, risk and governance marketing at Micro Focus, the UK's biggest technology company. "Security becomes the enforcement mechanism, risk becomes the measure and governance the decision-making.

> **We have some of the best, innovative technology in the marketplace, spanning not just security, but many other parts of the enterprise**

If you bring all of those teams together around that uniform process, you can be much more effective and start providing a lower-risk environment."

Companies must also recognise the clear relationship between identities, applications and data, and how each can become a vulnerability if not protected as well as the others. When silos are prevalent across an organisation, it can be easy for an individual with a background in DevOps, for example, to only think about application security.

By neglecting to think about the data the applications operate on or the users who interact with them, they can end up running into different kinds of security challenges. Making a change in one area can also have an impact on others that are out of view. "If they're not careful, they can set the organisation up to be blindsided," warns Mr Grandpre.

In the rush to meet the demand for greater security, venture capitalists have inadvertently heightened the likelihood of such silos in an organisation. Having injected more funding into the security industry in the past year than the last four combined, the result is an abundance of point solutions that tackle very narrow pieces of the security problem, creating even greater integration challenges and making it difficult to achieve a holistic view.

By providing perspective and integration across not just security, risk and governance, but the whole enterprise, including DevOps, hybrid IT and analytics, Micro Focus is well suited to organisations that wish to eliminate harmful silos and achieve a well-rounded approach to securing their business.

"We have the ability to connect all these teams, solve new use-cases and couple different businesses and buying centres, which allows organisations to bring in technology that's been built to solve security challenges in a much more impactful way than the many point vendors out there in the market," says Mr Grandpre.

The benefits of bringing together security, risk and governance spread beyond protecting the organisation from threats and ensuring data privacy for customers. Cybersecurity is now so engrained in the success of an organisation that achieving a well-rounded approach also enables new opportunities for businesses to grow.

"It gives you many ways to drive disruption and achieve even greater heights, while at the same time defending against breaches and keeping data private," says Mr Grandpre. "We can help customers deliver a bright digital transformation for their future without worrying about incurring greater risk.

"Over the last 40 years, Micro Focus has proudly built this very successful business from taking a lot of amazing technology, some more mature and some new, and making it work for where our customers are going. We have some of the best, innovative technology in the marketplace, spanning not just security, but many other parts of the enterprise."

For further information please visit www.microfocus.com/srgtimes

Or alternatively, email Nick Nikols at nick.nikols@microfocus.com or Travis Grandpre at travis.grandpre@microfocus.com

MICRO FOCUS

Q&A

Culture eats strategy for security

Nick Nikols, vice president of security strategy at Micro Focus, says building a risk culture is crucial to keeping secure in today's threat landscape

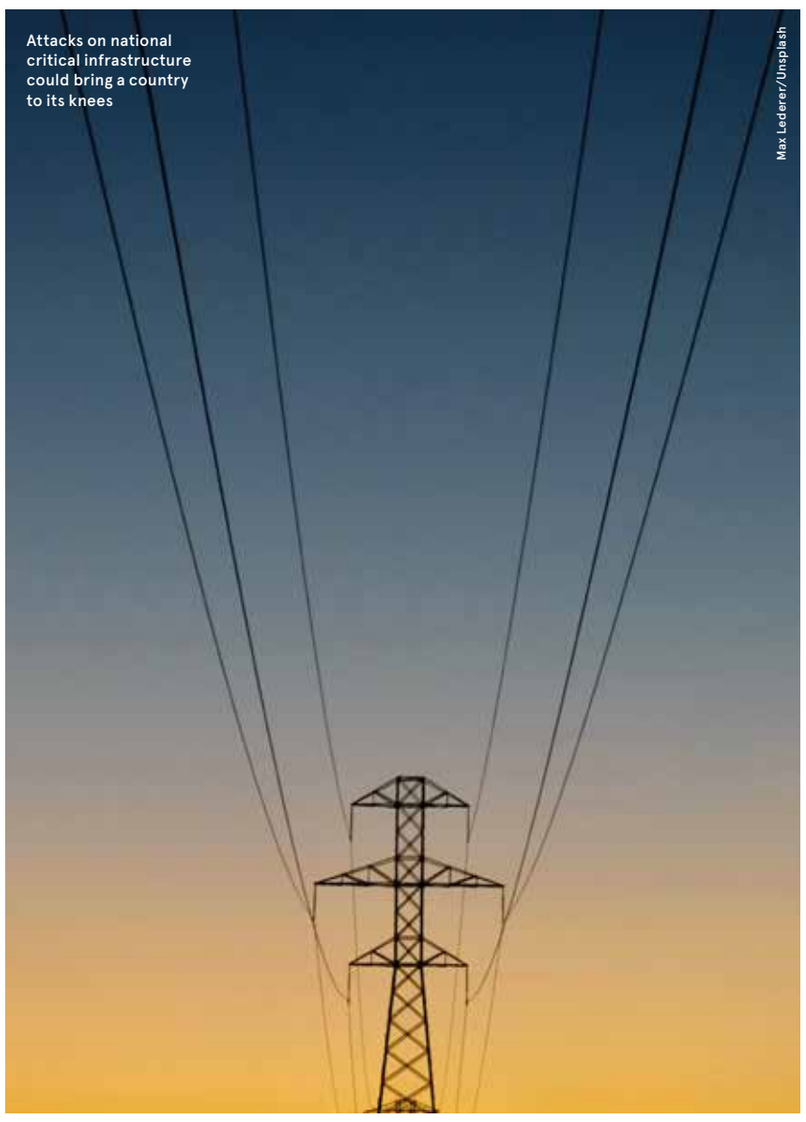
What is the danger of overlooking people and process when protecting an organisation from cyber-threats?
Technology is a tool the process uses, but it's people that make the decisions. You end up having multiple levels you're dealing with, from those running the business to the employees operating all of the necessary functions within the organisation and the customers being interacted with. Understanding that relationship relative to the processes and how the technology can facilitate their interactions is critical. You can't separate the three; they're integral to any successful deployment.

What's your advice for building a culture where technology, people and process interlink most effectively?
You need to have a certain level of transparency as to what's going on within the business. When you're dealing with technology, or even when you're dealing with processes, that visibility into the current state of play elevates the understanding of the overall risks. Having the right kind of analytics facilitates this because additional insights and awareness help change behaviour and impact the efficiency of how people interact. The culture builds a much more productive environment because everybody has a clearer picture of the risk of their individual activities and it becomes more natural to do the right things.

How can organisations ensure their people aren't their biggest vulnerability?
We've seen the biggest success when companies place more emphasis on career growth and fostering people to develop and stay within the organisation. By treating them as a long-term asset, they can keep growth going as far as addressing security and risk, and the things around culture that can be really impacted. Having said this, I don't know if it's ever possible for a company to be so risk focused that everybody watches everything they access and share, so technology plays a big part too. You can look at privileges and monitor access, keeping a much more granular look and avoiding a situation where no one really understands what's going on.

NETWORK INFRASTRUCTURE

National security models still not up to scratch



Attacks on national critical infrastructure could bring a country to its knees

Max Lederer/Unsplash

With cyberattacks rising in both volume and complexity, and critical network infrastructure now a vulnerable target, filling the gaps in government cyberdefence has never been more important

Matthew Staff

Here's a warning: "The world is still not prepared for cyberattacks on critical infrastructure. Governments are not ready, law enforcement isn't ready, the facilities themselves are not ready, and the people who design, build and operate them are often the least ready of all. Unfortunately, the cybercriminals are very ready indeed."

So says David Emm, principal security researcher at global cybersecurity provider Kaspersky Lab, who is not alone in his assessment of the current readiness among governments to protect critical network infrastructure and the public institutions that exist under its umbrella.

While private sector operators take responsibility for their own digital safeguarding, such are the financial dangers associated with not doing so, Mr Emm asks: "Who will take responsibility for protecting our utilities, our rail lines or our healthcare system?"

In the UK, the government holds information on individuals' health records, residency, bank details and numerous other pieces of private data. By inadequately protecting such personal information against potential breaches, the ramifications could be disastrous.

Mr Emm continues: "The difference between an attack on a single organisation and an attack on critical national infrastructure is there could be a real-world effect across an entire country. In 2015, Ukraine had a taste of this, when hackers took control of its power grid, plunging thousands of homes and establishments into darkness for hours."

Despite a growing awareness of the cyberthreat, many IT security models are still lagging behind, embedded in the hope that "security by obscurity" is enough. The challenge arises from the sheer volume of sensitive data that the public sector has to handle, against this entrenched slowness to adopt modern digital standards in the era of Industry 4.0.

"Yes, data dumps of printed Excel files are still a thing," says Alex de Carvalho, chief information officer and co-founder of PUBLIC, which helps tech startups solve prevalent public sector challenges and pitfalls.

"Many departments and local authorities have a pressing challenge to apply high standards of protection and oversight over a very disparate and digitally uneven network, and that's where we have been working to try and find startups that can help public sector security teams tackle the cybersecurity challenge."

Mr Emm and Mr de Carvalho agree that to implement reliable protection against all hazards, a multi-layered, highly configurable defence is required to extinguish more traditional threats, such as phishing emails, unsecure links and human error, and then dig deeper to ensure greater clarification of best-practice technology standards are in place for the companies or institutions themselves, their own internal arms, and their business partners and supply chain.

"Attacks on industrial systems are on the rise and it's clear that for businesses operating industrial or critical infrastructure systems, the risks have never been greater," says Mr Emm. "In 2017, TRITON, a malicious malware, took control of Triconex safety instrumented system controllers, giving attackers the ability to interfere with the plant's processes or to cause an emergency shutdown, halting operations at a critical infrastructure organisation."

Closer to home, it's more evocative to resonate with the notion of a similar event happening within the NHS, a fact that hasn't been lost on Barney Gilbert, co-founder and co-chief executive of Forward Health, a company offering secure messaging, compliant with the General Data Protection Regulation, for doctors and nurses as an alternative to open, prohibited portals such as WhatsApp.

"The NHS is a huge operation run by myriad staff, with varying levels of security clearance, most of whom engage with a unique combination of systems on a daily basis and the majority of which are processing highly personal data. It's a minefield," says Dr Gilbert.

> **The difference between an attack on a single organisation and an attack on critical national infrastructure is there could be a real-world effect across an entire country**

"This hasn't been helped by the piecemeal approach to IT upgrades that the NHS has spent several decades grappling with. It's made for a set of weak systems that are perfect for low-cost, high-impact asymmetric cyberattacks or other security breaches, which could easily see our personal health data becoming a cyberwarfare bargaining chip.

"We had a taste of what the impact of an NHS cyberattack looks like with the WannaCry incident in 2017. The impact was immediate and widespread, highlighting how vulnerable our most critical information systems can be."

Dr Gilbert says there shouldn't be a difference in how critical network infrastructure or physical infrastructure is protected, adding that governments need to make systems too "costly and ultimately counter-productive" to be attacked.

Mr Emm says: "Fast-changing threats have made it impossible to secure critical national infrastructure networks and systems completely, but a wait-and-see attitude should not be adopted. In fact, it should serve as the latest warning that hackers can severely affect, or even take offline, critical public infrastructure.

"Updating plans for improving defences and reducing the impact of attacks must become the new normal if the government and operators are to be agile in responding to this changing environment."

There is an overwhelming consensus that a reactionary approach to the current situation is not enough. To get ahead of the curve, a mixture of holistic system protection, on the surface, and improved networking, education and training, behind the scenes, is vital.

"Essentially, every industrial customer and process is unique, and it is important to deploy a solution made up of a portfolio of technologies and services that can adapt to different sectors, whether that's oil and gas, water, power grids, manufacturing and so on," says Mr Emm.

Mr de Carvalho believes inroads are being made in the UK through not just workshops and classes, but physical tools that are able to "quickly and effectively notify individuals and management of potentially unsecure actions".

By following a comprehensive, process-oriented approach, critical network infrastructure will be better guarded against sophisticated, targeted attacks, veering away from an inefficient, reactionary seek-and-destroy approach to an embedded culture of front-line public protection. ●

WANNACRY'S IMPACT ON THE NHS

Although not specifically targeted at the NHS, WannaCry was still the largest cyberattack to hit the health service in history. Launched on May 12, 2017, the ransomware disrupted NHS trusts and GP practices across the country, leading to thousands of cancelled appointments and operations

34% of NHS trusts in England were disrupted in the attack

6.9k appointments were cancelled in the space of six days

19k appointments would have been cancelled in total, based on the normal rate of follow-up appointments to first appointments

National Audit Office 2017

Last year's WannaCry cyberattack showed just how vulnerable the NHS is to ransomware and other threats

John Gomez/Shutterstock


RishabhWarshney/Unsplash

CYBER-STRATEGY

Building a cyber-resilient business from the ground up

As the number of cyberattacks surge, firms must ensure they have a resilient-by-design business model

Kate O'Flaherty

There is a well-known saying in cybersecurity: it's not a matter of if you are attacked, but when. And a growing number of big firms are starting to discover how true this is. The last year has seen successful cyberassaults hit the likes of British Airways, Marriott Hotel Group and Facebook.

As the frequency of attacks surges, cybersecurity is increasingly being viewed as a business problem. This is further fuelled by the growing cost of breaches. According to Accenture, companies globally could incur £4.1 trillion in additional costs and lost revenue over the next five years due to cyberattacks, as dependency on complex internet-enabled business models outpaces the ability to introduce adequate safeguards to protect critical assets.

At a time when business competition is fierce and the European Union General Data Protection Regulation (GDPR) mandates that firms report breaches of personal data, customer trust now depends on a business' ability to prove it is secure. This is putting a focus on resilience, a firm's capacity to protect itself from breaches, and respond quickly and appropriately when an attack does inevitably happen.

Yet cyber-resilience is not as straightforward as it seems. In the past, security was based on building a better "wall" around business data. But this approach no longer works in today's perimeter-free world of multiple devices and cloud, says Chris Moses, senior operations manager at Blackstone Consultancy.

Instead, a multi-faceted strategy can help create a resilient-by-design company. First, an organisation needs to understand fully its business model including its most valuable assets, says Jamal Elmellas, chief technology officer at Auriga Consulting. "Firms need to know which of their applications is most important to the day-to-day running of the company, and ensure this is resilient and can get back up and running should an incident happen."

87% of organisations do not yet have sufficient budget to provide the levels of cybersecurity and resilience they want

18% say that IT security fully influences business strategy plans on a regular basis

EY 2018

At the same time, it's important that infrastructure is robust, says Dr Sandra Bell, head of resilience consulting at Sungard AS. "The more robust your IT is, the more options an organisation has," she says.

When protecting infrastructure, perimeter walls should be strong enough to make it difficult for attackers to get in. "But if they do breach the perimeter, network segmentation will help to prevent an attacker from accessing business data," says Elliot Rose, head of cybersecurity at PA Consulting.

Firms also need to ensure their data storage methods meet legal requirements. "It is all too easy to get caught up in digital silos that ignore the bigger picture and the need to be holistic where prevention is concerned," says Helen Davenport, director and cybersecurity expert at Gowling WLG.

Understanding risk is a key part of building resilience. Indeed, GDPR calls for firms to think about how they protect sensitive information. The regulation also encourages businesses to consider the risk added by third-party contractors, which might not be secure and could lead to a breach of a company's data.

In some cases, an organisation's process for procuring services will need to be rewritten, says Mr Elmellas. "Cybersecurity needs to be written into your procurement, even as part of the vetting process."

There is no doubt that cyberattacks will continue to hit business, but technology can help to detect threats. For example, many firms are already using techniques that take advantage of artificial intelligence and machine-learning. Tools based on these technologies can monitor employees' behavioural patterns and pick up abnormalities, such as a change in the time they log into systems, to alert firms that they may be under attack.

And, of course, employees are an integral part of a cyber resilient-by-design business. "The foundation of a security culture must be rooted in a sense of shared responsibility," says Cath Goulding, head of cybersecurity at Nominet. "This means every person within the business, from the front desk, to customer service reps, all the way up to the board, must play their part. CEOs who feel security policies don't apply to them are mistaken; if anything, they are far more likely to be targeted due to their profile and stature within the business."

Nick Taylor, UK and Ireland security lead at Accenture, says "brilliant basics", including training employees to spot and report suspicious activity, are the foundation of resilience.

Dr Bell agrees. "We often hear they are the weakest link, but the users of the information system are the first line of defence," she says. "They need to be aware of procedures and processes, and what part they play. The system will be vulnerable and threat actors will try to manipulate employees, so give them coping mechanisms."

> **Every person within the business, from the front desk, to customer service reps, all the way up to the board, must play their part**

HOW CONFIDENT COMPANIES ARE IN SECURING EMERGING TECHNOLOGY

Percentage of leaders who said the following are critical to at least some of their business, and the percentage who said they had sufficient digital trust controls in place*

*Digital trust is defined as the level of confidence in people, processes, and technology to build a secure digital world

PwC 2018

Commercial feature

Re-establishing trust in an ultra-connected world

As cyberthreats continue to evolve at pace and nation state protectionism risks giving an advantage to hackers, Kaspersky Lab is pioneering a new set of standards and principles that champion trust, transparency and co-operation in the fight against criminals

The cyberthreat landscape has evolved at a rapid pace over the last decade as the digitisation of business and society has created a myriad of new opportunities for hackers. The rise of online shopping, artificial intelligence and the internet of things may have provided enormous value, but they've also made security far more complicated and challenging.

As one of the leading and oldest players in the cybersecurity market, Kaspersky Lab has ridden these waves for more than 20 years, and now tracks over 360,000 new malicious files every day in its mission to help organisations and consumers protect their data and devices. Its Global Research and Analysis Team (GReAT), made up of an elite group of security experts, has discovered and thwarted a long line of threats, including the likes of ProjectSauron, ShadowPad and 2017's notorious Android spyware Skygofree.

"The reality today is not if businesses are going to be attacked, but when," says Andrew Winton, vice president of global marketing at Kaspersky Lab, which counts more than 400 million users on its network across five continents. "We're constantly in a cat-and-mouse game to stay one step ahead of cybercriminals. Given that an average breach costs a large enterprise up to £1 million, it can have a significant impact on businesses."

> **Cyberthreats don't see boundaries that nations put up and to counter that from a security perspective we need to be able to operate without borders too**

One of the biggest emerging threats is the Balkanisation of the internet by nation states, driven by a geopolitical climate increasingly defined by protectionism. In their attempts to obstruct cyber-espionage and apply digital borders, governments are enforcing embargoes that ban or restrict trade with suppliers from certain countries. In the long term, this could result in more damage to national security, not less.

"If people weren't hearing from foreign cybersecurity firms as much as they do, and governments keep blocking such companies, we're actually likely to see more security problems for businesses and citizens," says Mr Winton. "The global political landscape that has led to successful campaigns for some countries and Brexit has created a more siloed world, which doesn't help anybody apart from the cybercriminals because the digital age does not work in silos, it's joined up, connected and doesn't have borders.

"Cyberthreats don't see, let alone respect, boundaries that nations put up and to counter that from a security perspective we need to be able to operate without borders too. Competition powers innovation and evidence shows that most companies benefit significantly when there are others around them doing the same thing, only better. In cybersecurity, this translates into better protection for everybody involved."

Kaspersky Lab is leading the cybersecurity industry's charge to counter internet Balkanisation, and re-establish trust and co-operation between nation states, businesses and citizens. Its Global Transparency Initiative (GTI), launched in October 2017, is a unique programme that has seen the company open itself up to third-party audit and review in unprecedented ways, pioneering a new set of standards for organisations to abide by.

Last year, Kaspersky Lab began redesigning its infrastructure and moving elements of its data processing to Switzerland, a nation known for its political independence and strong data security and management. It welcomes audits of its engineering practice there and is planning to open three further transparency centres globally, where its partners and customers can access its documentation and source code, which will also be verified and audited by a leading management consulting firm this year.

Kaspersky Lab now encourages other vendors to follow suit. Becoming so transparent is not risk free for a cybersecurity firm, Mr Winton concedes. Exposing the company's code, even in such a highly controlled environment, can open it up for attack. However, Kaspersky Lab believes this is a risk worth taking to fly the flag for trust in the digital world and to put customers at ease.

"We're evolving our strategy into one that strives for complete immunity," says Mr Winton. "In doing so, we think we're taking another step closer to saving the world. This is an ambitious claim, but we fundamentally believe the work we're doing, the products we offer and the movement of our business from a product set to a service solution, underpinned with the transparency we're offering, puts us in a really strong place to help protect consumers and businesses around the world."

For more information please visit kaspersky.com/transparency

KASPERSKY lab

OPINION

'Traditional corporate governance principles on their own are inadequate in the face of digital transformation'

The business environment can be exciting and unpredictable in equal measure. Opportunities for innovators who find openings that others fail to spot are unprecedented. At the same time, they face and cause risks that we did not even know about a few years ago; change can happen at break-neck speed. How we respond can be the difference between sustainable success and failure.

Against this background Airmic, which represents those who work in risk, commissioned a report from CASS Business School to examine the impact that the so-called fourth industrial revolution can be expected to have on the resilience of companies. Although *Roads to Revolution* is fundamentally positive, it warns that organisations cannot continue to manage risk as they have in the past and expect to remain successful.

This is an age when a teenage hacker working out of his bedroom can potentially cause as much economic damage as a tropical storm, when a systems failure or social media event that hits the unprepared business can leave a reputation in tatters. We must understand and deal with this kind of challenge.

"Board members need to understand that traditional resilience measures alone are insufficient in the digital age," our report says. Regular reviews of stakeholder purpose and continuous business model reinvention are necessary for the future success and sustainability of organisations.

The report underlines that good governance becomes even more important in the cyberage. But it goes further than that: traditional corporate governance principles on their own are inadequate in the face of digital transformation. In simple terms, there are a whole lot of emerging risks out there that could flatten a company unless they are identified, understood and overseen.

It has always been the case that firms must reconsider their purpose from time to time to stay successful. After all, the Shell oil company famously started out life, as the name suggests, importing and selling shells. The difference now is that things happen so fast that companies need to reinvent themselves almost all the time; to be alert, inquisitive, open to change and agile.

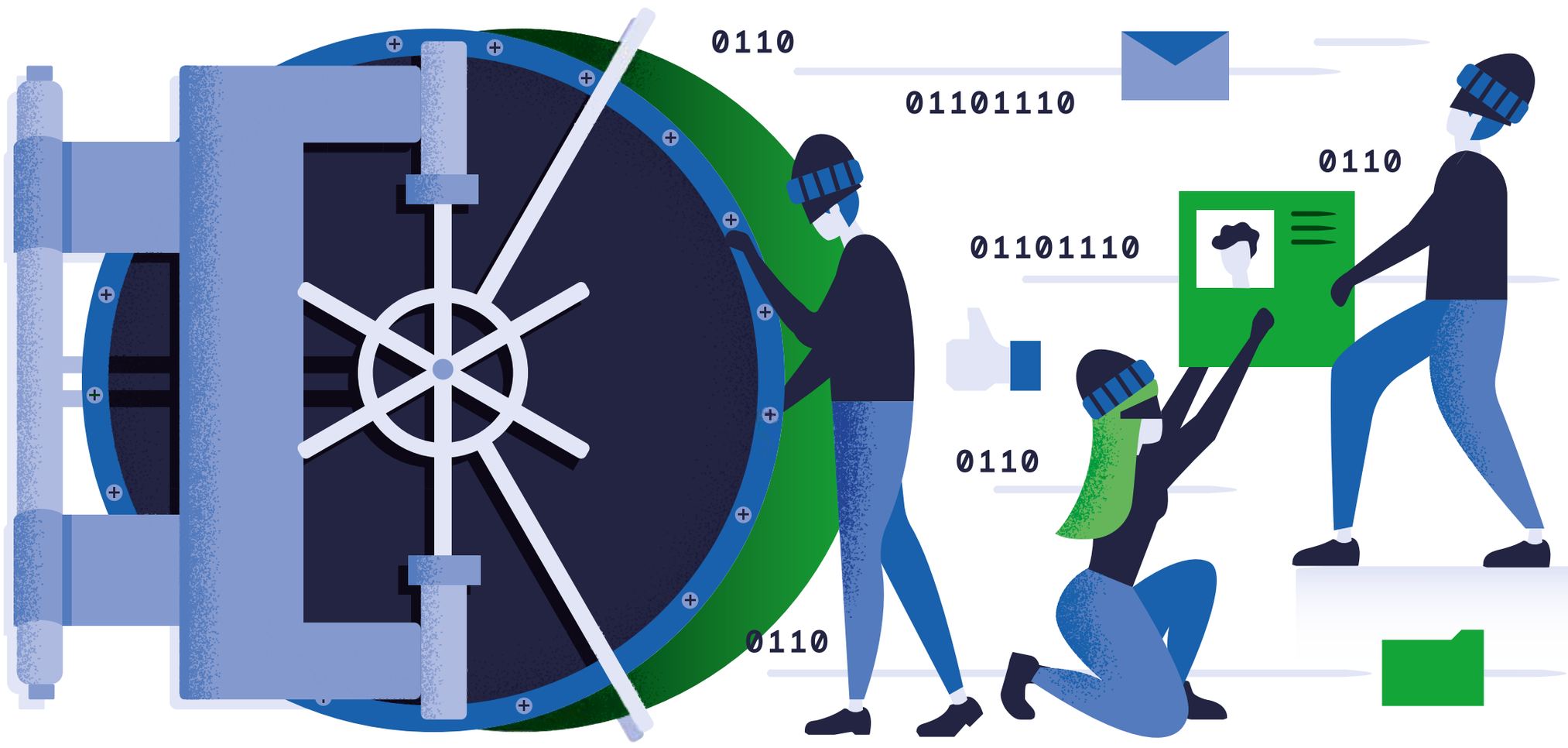
Cyber-related technology is, of course, at the heart of developments. It no longer merely helps us to carry out existing processes more efficiently. Digital transformation of business models is now core to how we add value, how we reinvent our purpose, organise our enterprises, our networks, supply chains, the products and services we offer, and how we relate to our customers and other stakeholders.

I have no doubt that an increasingly cyber-dominated business environment will continue to make the world more interesting and more prosperous. We need not fear innovations such as artificial intelligence, blockchain and quantum computing. But there will be losers as well as winners. The winners will be those organisations and individuals that acquire the necessary expertise, collaborate and embrace change. They will understand that positive risk management can make enterprises sustainable in these unpredictable times.

It is important to stress that good risk management is much more than a theoretical concept. Another CASS report, *Roads to Ruin*, commissioned by Airmic in 2011, featured 18 case studies of corporate catastrophes. It found that all could have been avoided had the board been better informed and more responsive.

Many board members do not understand what positive risk management can do for their businesses, while many risk managers do not understand and align to the business drivers sufficiently to wield strategic influence within their organisations. Changing this culture and putting risk at the heart of corporate thinking is a top priority with cyber at the centre of the discussion.

John Ludlow
Chief executive
Airmic



CYBERCRIME

Trillion-dollar industry hidden in the dark web

The low startup costs and huge profits associated with cybercrime have resulted in a thriving industry, and no companies – regardless of sector or size – are safe from its reach

Nafeez Ahmed

The internet of things (IoT) has been hailed as ushering in a technological revolution that will transform our lives for the better. With every conceivable tool and device we use seamlessly interconnected through the cloud, everything we do from work to leisure will be increasingly automated, efficient and easily configurable in ways that were previously unimaginable.

But even before the IoT revolution has fully arrived, associated costs are rising exponentially. A new Accenture report estimates that businesses could incur up to $5.2 trillion over the next five years in additional costs and lost revenue due to cybercrime "as dependency on complex internet-enabled business models outpaces the ability to introduce adequate safeguards that protect critical assets".

According to the report, some 80 per cent of business leaders admit having a hard time ensuring their companies are protected. And it's not just businesses. Government figures reveal that UK residents are more likely to be a victim of cybercrime or fraud than any other offence.

While the costs to legitimate businesses and consumers escalate, so do profits for cybercriminals. A 2018 University of Surrey study conservatively estimates that cybercrime carried out on well-known platforms such as Amazon, Facebook and Instagram rakes in a cool $1.5 trillion, equivalent to the GDP of Russia.

This is not even particularly sophisticated cybercrime. According to study author criminologist Dr Michael McGuire, these platforms are being used to evade tax, move money, trade illicit drugs and sell fake goods. As technology advances, the opportunities for such crime will transform.

"In a world where almost every instruction, process, transaction and secret is located in cyberspace, there could be a wealth of opportunities for criminals," warns an October 2018 report from the UK Ministry of Defence Global Strategic Trends programme. With relatively low startup costs and potentially huge profits, organised cybercrime has an obvious business appeal, the report says, especially for "people in countries with limited economic opportunities".

Most cyberattacks in the European Union, for instance, actually come from outside the region.

And like any other business, cybercriminals are rapidly investing in innovations and new techniques to improve their productivity. A report by the Tel Aviv-based global IT security firm Check Point Software Technologies highlights how cybercrime methods have become "democratised" and available to anyone willing to pay for them.

"Cybercriminals are successfully exploring stealthy new approaches and business models, such as malware affiliate programs, to maximise their illegal revenues while reducing their risk of detection," says Peter Alexander at Check Point.

Maya Horowitz, Check Point's director of threat intelligence and research, paints a picture of an increasingly corporatised approach to cybercrime. Attacks involve organised teams of programmers, corporate insiders, IT technicians and phishing experts. These teams even issue job ads for new roles for the next hack.

This sort of activity has been facilitated by the dark web, a hidden part of the internet where criminals can act undetected, using complex encryption and anonymisation tools.

The dark web first hit the headlines in 2013 when the FBI shut down the notorious Silk Road website, which ran on online black market in illicit drugs. The dark web thrives as a treasure trove of automated software applications which can be used to troll and attack vulnerable accounts automatically.

"A cybercriminal can simply purchase any number of password-cracking programs and can rent or purchase exploit kits which contain many attack tools," says Corey Milligan, one of the US Army's first cyber operations technicians and now a senior threat intelligence analyst at Armor Defense, a cloud security firm in Texas. "The kits are designed to make it quite trivial for an average computer user to successfully attack various vulnerabilities and then distribute malware or potentially wipe a victim's hard drive."

Cybercrime in the dark web is thriving, especially as people can be hired through third parties to conduct attacks. "The greatest impact they can have is when they are hired to do something for somebody else," adds Mr Milligan.

In effect, a whole new underground industry has emerged, dubbed "malware as a service". And as the IoT expands, so too will opportunities for commercial and criminal growth.

According to Intel, we are moving from a world of two billion smart, wirelessly connected objects in 2006, to a world of 200 billion by 2020. By 2021, half a billion of these will be wearable devices.

Dr Janusz Bryzek, a Silicon Valley guru who pioneered sensor technology, predicts that within 20 years there will be 45 trillion networked sensors, devices which detect and respond to physical environmental changes such as light, heat, sound, moisture and pressure.

Already, attacks on connected devices, including routers, cameras, thermostats, electronic appliances and alarm clocks, are among the top cybercrime targets. But companies are not doing enough to protect these devices, preferring to get them on the market without delay.

"The risk is global. Regardless of the size of your business, or what sector you're in, if you're connected to the internet, you're at risk, as anyone can find you and any of the assets you have connected," says Mr Milligan.

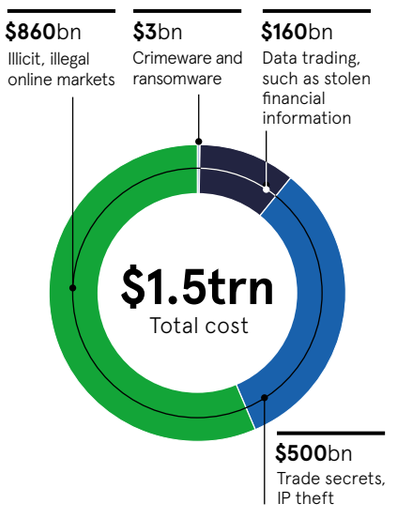
Most businesses remain dramatically behind the curve on safeguarding against these heightened risks. In 2018, the Ipsos MORI *Cyber Security Breaches Survey* found that four in ten businesses and a fifth of charities had experienced a cyberattack.

The findings led King's College London's Cyber Security Research Group this January to call on the UK government to name and shame companies whose cybersecurity measures fail to protect the data of consumers.

Complacency is not an option. In a taste of things to come, one of the largest electric power companies in America, Duke Energy, was hit with a $10-million regulatory fine in early-February for 130 violations of physical and cybersecurity standards. If companies fail to act now, governments will have little choice but to make them pay later.

ANNUAL REVENUES OF CYBERCRIME

Conservative estimates, based on data drawn from five of the highest profile and lucrative varieties of revenue-generating cybercrimes



Bromium 2018

COMPANY VALUE

Five ways cyberattacks can hit company value

The potential impact of cyberattacks on company value continues to be misunderstood by many business leaders and finance professionals. So while financial audits are regulated, why is cyber-risk still largely ignored and underplayed?

Tim Cooper

Business interruption

Serious business interruption after a breach has one of the largest effects on the value of companies because of its impact on cash flow, according to David Chinn, senior partner at McKinsey.

"Attackers are becoming more aggressive," he says. "Previously, they aimed to steal data. Now more interruption can come from ransomware or collateral damage from nation state attacks. For example, to cover their tracks, attackers are willing to damage companies' residual networks.

"In most cases, company share prices bounce back from business interruption. However, the stock market is particularly sensitive to the competence of the response. For example, being unclear, saying something that proved to be wrong, call centres that people can't get through to, websites that don't work; these can all be damaging."

According to the Ponemon Institute, disruptions that can affect corporate value include system downtime, increased communication including help desk activities, issuing new accounts, legal expenditure and identity protection.

Globally, companies that contained a breach in less than 30 days saved more than $1 million compared with those taking longer. However, containment is taking longer due to the increasing severity of attacks, says Ponemon.

Caleb Barlow, vice president of threat intelligence at IBM Security, says transport giant Maersk's response to the NotPetya attacks of 2017 was a great example of how to react. "They updated their website, telling people what was happening and restarted business operations in fewer than ten days, from scratch in some areas," he says. "Few companies could do that. We spend a lot of time training companies to make faster decisions in this kind of scenario."

Customer data

Loss of customer data is often a critical factor affecting share price after a data breach. For example, when credit information company Equifax lost more than a third of its value after reporting a data breach in 2017, it was largely due to hackers stealing personal customer information. This included addresses and social security, driver's licence and credit card numbers.

According to a study by the Ponemon Institute, the average cost per lost or stolen record in a breach is $148 and the more records the company loses, the higher the cost.

Ponemon says incident teams and better security such as encryption help mitigate these costs. It says organisations that fall victim to data breaches on average see their share price fall 5 per cent immediately after the disclosure of a breach. Falls range from 3 per cent for companies with good security to 7 per cent for companies with poor. Longer term, damage to corporate value can be even more, says Ponemon.

But having an incident response team saves $14 per record and the extensive use of encryption reduces cost by $13 per record.

Regulatory fines

Fines by regulators over data breaches do not always affect a company's share price at the time they are issued. By that time, the damage has often been done and the markets have factored in the impact already.

However, they can have an impact if the market is not expecting them or perhaps not expecting such severity. For example, when the Information Commissioner fined telecommunications company TalkTalk a record £400,000 in relation to a data breach, its share price, which had already plummeted after the attack, continued to fall after the announcement of the fine. The company's stock price has yet to recover.

The effect of regulation on corporate values could be set to rise dramatically now that the European Union's General Data Protection Regulation (GDPR), which allows for much higher fines, has come into effect. For example, millions of Facebook user accounts were exposed by a security breach in September 2018. Under GDPR, the company could be fined up to 4 per cent of its global annual revenue, which would be £1.3 billion.

Some experts have commented that TalkTalk was lucky in the sense that it was fined under more lenient rules before GDPR came in.

IBM Security's Mr Barlow says that, apart from the size of the new GDPR limits, the biggest issue with fines is that regulation can be quirky and misunderstood by many companies. "For example, they don't realise that the biggest regulatory impact is the speed of decision-making and process in responding to the breach," he says.

Intellectual property

As hackers become more sophisticated, there is greater risk of them obtaining sensitive commercial information such as intellectual property (IP) and using it.

Mr Barlow at IBM Security says: "If another country steals your IP, it has gone forever, you can't get it back and they will use it against you. So it is important to try and find out exactly what you have lost, who took the data and some idea of their motivation."

Mr Chinn of McKinsey says one way to guard against this is to ringfence the company's most valuable information. "If you can't keep attackers out completely, identify and protect the things that can impact most on corporate value," he says. "People are shifting from protecting the perimeter to differentiated protection according to the value of the asset."

Such information could take many forms. "For example, in a pharmaceutical company, clinical trial records are extremely valuable IP as they affect share price," says Mr Chinn. "In a manufacturing company, the systems that operate the factories are critical to corporate value. If you are in the middle of a big merger, the details of what you are willing to pay or the negotiation strategy are also incredibly valuable."

Reputation and trust

More organisations worldwide lost customers last year after data breaches, according to the Ponemon Institute. This could be due to increased awareness of breaches and expectations of what a company should do after one. According to a recent IBM Harris survey, 75 per cent of consumers said they would not buy from a company, no matter how good it was, if it was not protecting their data.

In the United States, losing customers after a breach cost companies $4.2 million on average, Ponemon says. Meanwhile 71 per cent of chief marketing officers believe the biggest cost of a security incident is loss of brand value.

McKinsey's Mr Chinn says: "When customer data is stolen, lost trust in management can impact corporate value and turnover significantly. Companies have been much quicker to report cyberattacks; however, there is a balance if they are trying to get the attacker out without them knowing and don't want to publicise the fact."

Peter Lefkowitz, chief digital risk officer at Citrix Systems, says media coverage has a major impact on share price. "The breaches that make front page news suffer the worst," he says. "Those cases usually involve something new and different or people hiding things. Often they have lots of problems happening at once, or the attack is by a nation state, or we learn more about [their governance] from the company's poor response."

Ponemon says organisations can reduce these losses if they have a leader, such as a chief information security officer, directing initiatives to improve customer trust in their guarding of personal information. Offering victims identity protection in the aftermath of a breach also helps.

Let the Red Team protect you from black hat hackers

The days of static, reactive approaches to cybersecurity are over

Businesses are becoming increasingly digital and agile to deliver products and services easily and conveniently to their consumers. However, these benefits come with a caveat. A recent study by IDG revealed that 78 per cent of consumers would stop engaging with a brand online if the brand experienced a data breach.

Protecting the brand and business in a digital world threatened by damaging cyberattacks is just as important as running that business in the first place. Cybersecurity has become an endeavour of building consumer trust.

Leading crowdsourced security-testing platform Synack has pioneered a model that combines the best of artificial intelligence (AI) and human intelligence to beat hackers at their own game and deliver not just security, but trust to their customers.

Synack was founded in 2013 when former US National Security Agency employees Jay Kaplan and Mark Kuhr recognised cyberattacks were evolving far more rapidly than organisations' defences could handle. The pair launched the industry's first solution to crowdsource hackers safely and effectively for vulnerability intelligence.

Six years later, the Silicon Valley-based pioneers have an expansive network of ethical hackers, the Synack Red Team (SRT), in more than 60 strategic locations around the world with the task of remaining a step ahead of their criminal counterparts, 24/7, 365 days of the year.

"By deploying a team of extensively vetted and superiorly skilled ethical hackers within the confines of an agile, continuous model, it gives our customers the ability to launch and sustain their own trusted applications and digital infrastructures," explains Synack's chief marketing officer Aisling Scallan MacRunnels.

SYNACK PROFILE

#1 choice of G2000 and security companies

Up to **200%** increase in Synack customers ARS over two years

Synack protects:

75% of top credit card companies

25% of top global banks

$110bn in digital payments revenue

"When we recruit and assess ethical hackers, we have the most stringent vetting model of any security company out there. It's not static either. It's a continuous process to ensure we always have the best and most trustworthy researchers in the world."

These researchers, or ethical hackers, are at the heart of the crowdsourcing business model first put forward by Synack in 2013. But the technology behind the crowd of hackers is just as important to ensure around-the-clock capabilities to stay on top of the most pertinent threats that organisations face.

According to Callum Carney, one of Synack's British Red Team hackers: "Every day, SRT members like myself work to protect a wide variety of Synack customers. Even though each customer has their own unique application stack, there will always be some SRT members on hand with the expertise and knowledge to find the critical vulnerabilities that customers are looking for.

> **Cybersecurity has become an endeavour of building consumer trust**

"To aid the SRT member in discovering these vulnerabilities, Synack created Hydra, a tool for categorising a company's digital assets. In my experience, Hydra massively decreases the amount of time required during the recon phase of working on a new engagement, allowing myself and other SRT members to begin locating vulnerabilities faster and more efficiently."

Ms MacRunnels continues: "Synack delivers integrated, continuous protection for organisations by seamlessly deploying their crowd with this AI-enabled technology that tracks all hacking activity for auditability and metrics, and even alerts the Synack Red Team of potential vulnerabilities to make them more efficient. Such diversity and scalability can only be realised via this optimal combination of human and machine intelligence that drives Synack's comprehensive crowdsourcing model."

Synack's platform produces valuable hacker-powered data and metrics that are accessible through the customer portal. "Our portal delivers powerful insight and intelligence to the customer. We can speed up or slow down this delivery of information to align with the customer's internal resource capabilities," says Ms MacRunnels.

"We're not an outsourced function or an afterthought brought in every now and then to monitor their security. We are entirely integrated into how these companies develop secure product, created with flexibility to fit each customer's needs, with complete transparency in terms of knowledge-sharing and education."

The data and metrics play a huge role in security that is practical and results-focused. Not only does the Synack Red Team uncover vulnerabilities and help customers fix them, but customers are getting a real-time score that tells them how resistant they are to attacks and how that score changes over time. Experience has proven that Synack customers increase their attacker resistance scores up to 200 per cent when they utilise Synack's crowdsourced security platform consistently over the course of two years.

"We have swung the pendulum from traditional human-based models to an intelligent, diverse and flexible model, which ensures trust between researches and customers, trust between security and DevOps teams, trust between DevOps teams and C-Level executives, and trust with their own end-customers," Ms MacRunnels concludes. "All of that comes from trust delivered by Synack."

For further information please visit www.synack.com

Synack

HACKERS

Should you employ a former black hat hacker?

In hacking, as in life, it is not just good and bad, black and white: there is a grey area. Converted black hat hackers have amassed the experience needed to test cybersecurity systems properly and many organisations are providing them with a clean slate to bolster defences. However, recent evidence indicates that more white hat hackers are being tempted to commit cybercrime. So although ex-criminals looking to redeem their past sins are likely to have the nous and skill to protect a company, can they be trusted? Ultimately, is it worth the risk?

Oliver Pickup

For

David Warburton, senior threat evangelist at application services organisation F5 Networks, believes the knowledge amassed by cybercriminals is invaluable for businesses trying to shore up their defences. "When we employ contractors to work on our homes, we tend to look for someone with strong hands-on experience," he says. "So while it may sound counter-intuitive to make use of ex-criminals to help plan and test our cyberdefences, the one thing they have in abundance is hands-on experience.

"Security architects have a wealth of knowledge on industry best practice, but what is often lacking is first-hand experience of how attackers perform reconnaissance, chain together multiple attacks and gain access to corporate networks. Application defenders need to consider every single possible angle of attack. With technology and vulnerabilities constantly evolving, it is a never-ending mission with no tangible finish line. Cybercriminals, by contrast, only need to find one area of weakness to get in and claim victory."

Ben Sadeghipour, hacker operations lead at HackerOne, a growing platform that is accessed by approximately 300,000 white hat hackers, looking to gain bug bounties, agrees. "It can be hard to work with ex-cybercriminals because of the 'baggage' they come with," he says, adding that it is still worth it. "The best part about working with hackers with a cybercriminal background is that, in some cases, possibly most, they understand how to demonstrate a real-world scenario in which a malicious actor could abuse a certain vulnerability or functionality."

Luke Vile, cybersecurity expert at PA Consulting, continues this theme. "Many large organisations understand there is sometimes a great deal of value in understanding how cybercriminals think and operate in the real world," he says. "Plus, there is a huge difference between paying individuals known to be involved in criminal work and using the specialist skills of people who have actively chosen to use their talents for the good of security."

Steps to ward off would-be black hat hackers from the dark side are being taken. Mr Vile's employers, in collaboration with the National Crime Agency and Cyber Security Challenge UK, recently ran an Intervention Day workshop that showed young IT enthusiasts the rewards of using their cyber-skills ethically and legally. He continues: "The programme introduces the Computer Misuse Act 1990, and combines technical exercises with industry insights and careers advice."

> **In our system of law, we must believe in rehabilitation and be open to it, otherwise it just doesn't work**

Furthermore, redemption should be encouraged, says Sam Curry, chief security officer at Cybereason. "For years, I believed that those who had transgressed should not be rewarded or hired at all," he says. "They couldn't be trusted and, most importantly, their former dark work was too often being glorified or used for gain by hirers. However, I have changed my mind in my old age.

"I'm glad I did because some of my best colleagues now used to be my adversaries, and I apologise to those I didn't try harder to help 20 years ago and blocked from hiring in my companies because of their black hat, for-profit endeavours. Over the last 30 years, many famous, infamous and not-so-well-known black hat hackers have shown genuine remorse and contributed to the public good.

"Every hacker is a unique case and generalisation is dangerous. What matters most, though, is that people with skills to harm learn the moral and ethical lessons of their errant ways and work towards the public good. Given time, many reform and utilising their skills is a tremendous benefit to the industry."

If ex-black hats are employed, more-than-adequate checks have to be in place, at least to begin with, urges Naaman Hart, cloud services security architect at Digital Guardian. "Initially, I can understand the need for some controls, but there should be an obvious expectation on both sides that trust is being built up with regular opportunities to prove that trust," he says. "Lasting stigma over being an ex-criminal is proven to be more likely to lead to reoffending as a form of spite. In our system of law, we must believe in rehabilitation and be open to it, otherwise it just doesn't work."

Against

Five years ago everyone knew about the much-lamented paucity of skilled cybersecurity professionals. That lack of talent is no longer a problem, though, and there still is no need to employ ex-black hat hackers as penetration testers. So says Ian Glover, president of Crest, the international not-for-profit accreditation and certification body that represents and supports the technical information security market.

"The UK cybersecurity services market is one of the most mature in the world," he says. "We have benefited from the development of a higher education system that generates significant numbers of cybersecurity professionals, a mature training market that allows people to cross-train into the industry and well-structured career pathways to promote professional practices, underpinned by codes of conduct and ethics that are both meaningful and enforceable.

"Therefore, the need to look at using cybercriminals to support the industry is not appropriate and is not necessary. This practice of using ex-offenders is not used in other professions, so if we want and need the industry to be viewed as a profession, this should not be encouraged."

> **Talent and skills are hard to find, but employing an ex-black hat requires a level of trust that cannot afford to be abused**

Lisa Forte, formerly of Red Goat Cyber Security, contends: "The reality is that very few organisations use ex-black hats at all. There is a multitude of reasons for this. Firstly, a common concern is that if it all goes wrong and they decide to attack you, it would be a PR disaster for the company.

"Secondly, the skillsets required don't quite match up. A lot of the black hats I've encountered seem to work almost entirely as lone wolves. Working for the cybersecurity team of a big company requires a high degree of teamwork and collaboration."

Steven Furnell, senior member of the Institute of Electrical and Electronics Engineers and professor of security at the University of Plymouth, has a similar view. "Being an ex-criminal is not a direct indication of capability; it simply means that they were breaking the law and were caught doing so," he says.

"While the idea of poacher turned gamekeeper has some credibility if you are looking for someone to think like an attacker, it doesn't necessarily mean they have the knowledge or skills to introduce the necessary protection."

Besides, in this digital age when attack vectors are multiplying, if you are encouraged not to trust anyone in your organisation, why take a risk on ex-criminals? "We are seeing more instances of the malicious insider causing damage to company productivity, revenue, intellectual property and reputation," says Marcin Kleczynski, chief executive and founder of anti-malware software organisation Malwarebytes.

"We must up-level the need for proper security financing to the executive and board level. This also means updating endpoint security solutions, and hiring and rewarding the best and brightest security professionals who manage endpoint protection, detection and remediation solutions."

However, given that Malwarebytes' recent research indicates cybersecurity professionals in the UK admit to participating in criminal activity almost twice as much as the global average, engaging canny, ex-convicts might not be smart.

Indeed, the August 2018 research identified the emergence of the "grey hat" hacker, those overlapping the realms of the good (white hat) and bad (black hat) hackers. The key findings include one in thirteen security professionals in the UK owned up to grey hat activity, compared with one in twenty two globally, and 46 per cent of respondents said it is straightforward to commit cybercrime without being caught. Moreover, the main driver for black hat transgression is the opportunity to earn more money than security professionals, according to 54 per cent of those surveyed.

Warren Mercer, technical lead at threat intelligence group Cisco Talos, says: "It's a tricky situation. Ex-black hats are likely to have unique insights and skills which can help identify and fix specific vulnerabilities, but these people are criminals.

"The industry has typically relied on individuals having a certain level of integrity, especially given that they could be granted access to a myriad of information, whether that's bank details, healthcare details, important conversations with loved ones or private pictures. Talent and skills are hard to find, but employing an ex-black hat requires a level of trust that cannot afford to be abused."

C-SUITE

Poor communication remains the weak link in cybersecurity

Language is key to successful collaboration between the chief information security officer (CISO) and other executives


hxdbzxy/Shutterstock

Davey Winder

Capgemini's *The Modern Connected CISO* report revealed 60 per cent of organisations have their CISO at key board meetings, but only half of business executives think the role has a high level of influence on management decisions. This could be because less than a quarter of executives thought information security was a proactive enabler of digital transformation. But just as easily it could be that C-suite and cybersecurity experts don't talk the same language.

Without a more cohesive working relationship between the CISO and chief executive, chief financial officer and chief operating officer, the organisation will never move at the speed of trust that is required by current agile business demands.

"Business leaders often choose to take risks while cybersecurity teams are trained to mitigate risk, which means priorities are at odds," says Greg Day, chief security officer, Europe, Middle East and Africa (EMEA), at Palo Alto Networks. Fixing this disconnect between the CISO and the rest of the C-suite is therefore key to building cyber-resilience through an informed risk management strategy.

So where are the most common disconnects to be found? That many CISOs find being heard at the top table still a work in progress, rather than a done deal, is part of the problem.

"CISOs, though growing in prominence, still struggle to wield influence at board level," says Keiron Shepherd, senior security systems engineer at F5 Networks. F5 research from last year showed 19 per cent of CISOs reported all data breaches to their board of directors, and 46 per cent admitted chief executive and board-level communications only happen in the event of material data breaches and cyberattacks. "This is a serious strategic disconnect," says Mr Shepherd.

Or how about the responsibility for day-to-day security which, for many businesses, doesn't fall squarely on any one person's shoulders?

"The narrow gap between the roles of chief information officer, chief executive and CISO shows that no one executive function is stepping up to the plate," says Azeem Aleem, vice president of consulting at NTT Security. "Given escalating threat levels and increasingly acute regulatory challenges, there's an urgent need for clear reporting lines and a foreground role for the CISO."

Ian Bancroft, general manager, EMEA, at Secureworks, agrees that all too often it takes a breach before the CISO is asked to present to the chief executive and board. "Developing the right communications flow is the key to ensuring that business leaders appreciate the risks and mitigation strategies," he says.

The commonplace situation of the CISO presenting an annual risk report to the board, with everything else across the year being made by their boss, usually the chief information officer or finance chief, can mean security status reporting often takes on the bias of whoever that happens to be.

The CISO undoubtedly needs to be able to communicate effectively with the senior leadership team. They need to be able to grasp complex issues relating to risk and get these across in a way that secures the buy-in needed.

"Yet many CISOs will have had no prior leadership experience," argues Chris Underwood, managing director at Adastrum Consulting. "As such, they will have limited knowledge of how to operate at executive level and speak 'executive' language." Which brings us to the biggest problem for cybersecurity: lack of alignment with the business.

"CISOs have traditionally been seen as running business prevention units," says Institute of Information Security Professionals chief executive Amanda Finch, who explains they are often thought of as "prophets of doom, scaremongers and a drain on the business". Clearly, CISOs must demonstrate they are on the same side. "They need to speak to chief executives and chief financial officers in language they understand to provide a common understanding of the real risks that an organisation can face," Ms Finch concludes.

Being able to articulate risk in a business context, alongside realistic and cost-aware solutions, is central to this relationship-building exercise. "This is easier said than done though," warns Sam Curry, chief security officer at Cybereason. "It requires soft skills, patience, gravitas, and sincere enthusiasm and participation in the business."

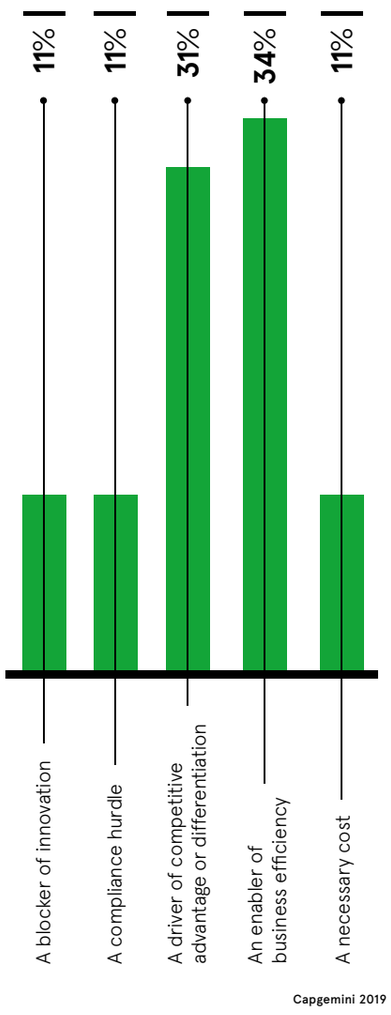
Which, according to Mr Curry, involves the use of just six key terms: revenue, cost, risk (this is the big one), customer satisfaction, employee efficiency and company strategy.

Simon Roe, product manager at Outpost24, says: "Each C-suite member needs to have an understanding of the business risks associated with a major breach." Whether that's costs associated with running a cybersecurity programme, reputational impact or financial penalties associated with an unreported breach, it's all part of a security culture.

Eoin Keary, chief executive of edgescan, sums it up: "There should be a conscious effort with one side committing to learning about cybersecurity and the other to make cybersecurity understandable to a layperson who has a different area of expertise."

PERCEPTIONS OF INFORMATION SECURITY IN THE BUSINESS

Survey of global chief information security officers



Capgemini 2019

> **Given escalating threat levels and increasingly acute regulatory challenges, there's an urgent need for clear reporting lines**


Towfiqu Photography/Getty Images

Communications failure + ignored risk = $100-million loss

"We undertook a cybersecurity assessment of a financial services business and it became clear there was a significant risk to that organisation from a specific piece of software essential to the operation of the business," Vince Warrington, chief executive at Protective Intelligence recounts. "We submitted a report to the client's technical security team highlighting the risk to the business."

When his team was called back in following a serious security incident, investigations traced it back to that vulnerable software. "The suspect functionality was still enabled, no monitoring had taken place and a criminal gang gained a foothold within the corporate network," Mr Warrington explains.

"In-house security had asked the C-suite for funding, but failed to impress upon them the significant risk it posed, talking in technical terms rather than framing it as a business risk. When the notoriously difficult chief financial officer asked why he needed to spend so much defending against kids in bedrooms messing about, they couldn't give a clearly defined business reason."

Both business and security team forgot about the vulnerability, and the finance chief was pleased he didn't need to spend any money. "Until the day nearly $100 million disappeared from their corporate bank account," Mr Warrington concludes.

Recording data for cyberdefence

By harvesting data from all over the digital landscape, an innovative company is providing firms with the intelligence to counter cybercrime

Deliver threat intelligence that's meaningful and accessible for all security professionals. Remove the barriers to adoption. Integrate threat intelligence into existing cybersecurity workflows. Cultivate the company's ecosystem of partners.

These are the tenets Recorded Future holds front and centre as it stares down the industry's biggest challenge: to help organisations reduce risk in the face of a vastly expanding attack surface.

On February 6, Recorded Future documented the latest in a long line of success stories, having helped a Norwegian company analyse a cyber-intrusion by a nation-state actor. The issue had resulted from a simple mislaid password and the resultant use of a third party to transfer private data out of the company.

Recorded Future's chief technology officer and co-founder Staffan Truvé deduces that this is yet another example of how an increasingly interconnected world is making us more vulnerable and increasingly exposed. It's a notion the company has been looking to remedy since its inception in 2009.

"When the company was founded, I was operating a research institute in Sweden, looking into the application of artificial intelligence techniques in various sectors," Mr Truvé recalls. "I could see how algorithms could help guide us in the future, while my business partner and Recorded Future chief executive Christopher Ahlberg was curious about ways we could use everything that was being published on the internet for more meaningful purposes.

"We brought those ideas together to create a business model that revolved around harvesting everything that people put on the web. First, we developed natural language processing to turn unstructured text into structured data. Once the structure was added, we were able to do all kinds of analytics on it."

Nine years on and with many success stories such as its Norwegian client in tow, Recorded Future continues to harvest data from sources all over the digital landscape, from RSS (rich site summary) feeds, big media, social media and even deeper down into the hackers' playground via forums. Ultimately, the company aims to deliver relevant, real-time threat intelligence powered by machine-learning to manage risk and empower security teams to make fast, confident decisions.

"It's such a broad spectrum we monitor and analyse," says Mr Truvé, "but over the past couple of years, we have looked to complement this text data with more technical sources too. For example, we are now harvesting all new registered domains around the world, as well as other technical information about how networks are being used, and even doing our own analysis of malware to see what's hidden inside them."

As Recorded Future's remit has expanded, and the general population's awareness of cyberthreats has increased, the company's demographic has broadened simultaneously.

"We are very industry agnostic in the present day, thanks to the breadth of data we collect," says Mr Truvé. "It's a tremendous spread of customers across numerous segments of industry ranging from finance, to manufacturing, to food and drink, and even transport. For each we have essentially geared our machinery in recent years towards the cyberthreat landscape.

"The core technologies are the same as what we started off with, but we have diversified in terms of the sources we collect from and the kinds of events we gear our algorithms towards detecting."

The model in 2019 acknowledges the different disciplines and requirements facing security teams, and Recorded Future helps to amplify the impact security teams can have across all internal, discrete functionalities.

The company has also greatly expanded its partner ecosystem, integrating with vulnerability management, security operations, incident response and SOAR solutions, as well as deepening its ties with top global resellers and managed security service providers.

"We add context that allows security professionals to take proactive steps, no matter which discipline a security professional is working in," says Mr Truvé. "At heart, we are a data company that provides intelligence for our customers' security teams to make decisions with information pertinent to their business."

As companies augment their digital capabilities, they are concurrently connecting their own systems to numerous others, both internally and externally across the supply chain and customer base. With every new interconnection, however, vulnerabilities are exacerbated and Recorded Future has looked to reduce the risk associated with this broadened network.

"Data is just data until you make it meaningful and actionable to the participant, and by doing broader and deeper collection of data than anyone else out there, and subsequently aggregating that information to bring a numeric value to certain risks, that's what we're able to provide customers."

The introduction of its third-party risk product further empowers customers to evaluate and assess proposed suppliers or partners prior to connecting digitally with them. Mr Truvé emphasises that this extent of risk management can only be achieved by operating outside company walls.

> **At heart, we are a data company that provides intelligence for our customers' security teams to make decisions with information pertinent to their business**

"We've conducted thorough mapping of more than 100,000 companies from this external vantage point," he says. "Web services, domains, IP address ranges, historical problems with data leakages; we can collate all this data and put a numerical score to it, so a human customer can assess and evaluate what's best for their company from a digital perspective before connecting their systems with another company's.

"I like to say that we're trying to build 'cybersecurity centaurs', to take the term from chess. The best chess player over the years hasn't been a human or a computer, but the combination of the two. It's the same at Recorded Future, we build machines and a portfolio of data that empower human analysts."

In the future, the business is turning its attention from descriptive analytics, where aggregated information on events that have already occurred are analysed and documented, to predictive analytics, where risk scores won't only be produced via historic data, but through predicting future trends based on the information being analysed and the threats being thwarted.

Mr Truvé concludes: "We can apply this predictive approach to domains, IP addresses and even industry sectors, and from there the obvious step is to move towards automation as well, not only predicting risks, but prescribing a course of action for companies to combat these foreseen threats.

"In doing so, we're edging closer to realising our goal of not just solving one security problem at a time, but allowing you to attack many of your security problems, faster and more confidently, with data that is impactful for your organisation."

IT WOULD TAKE

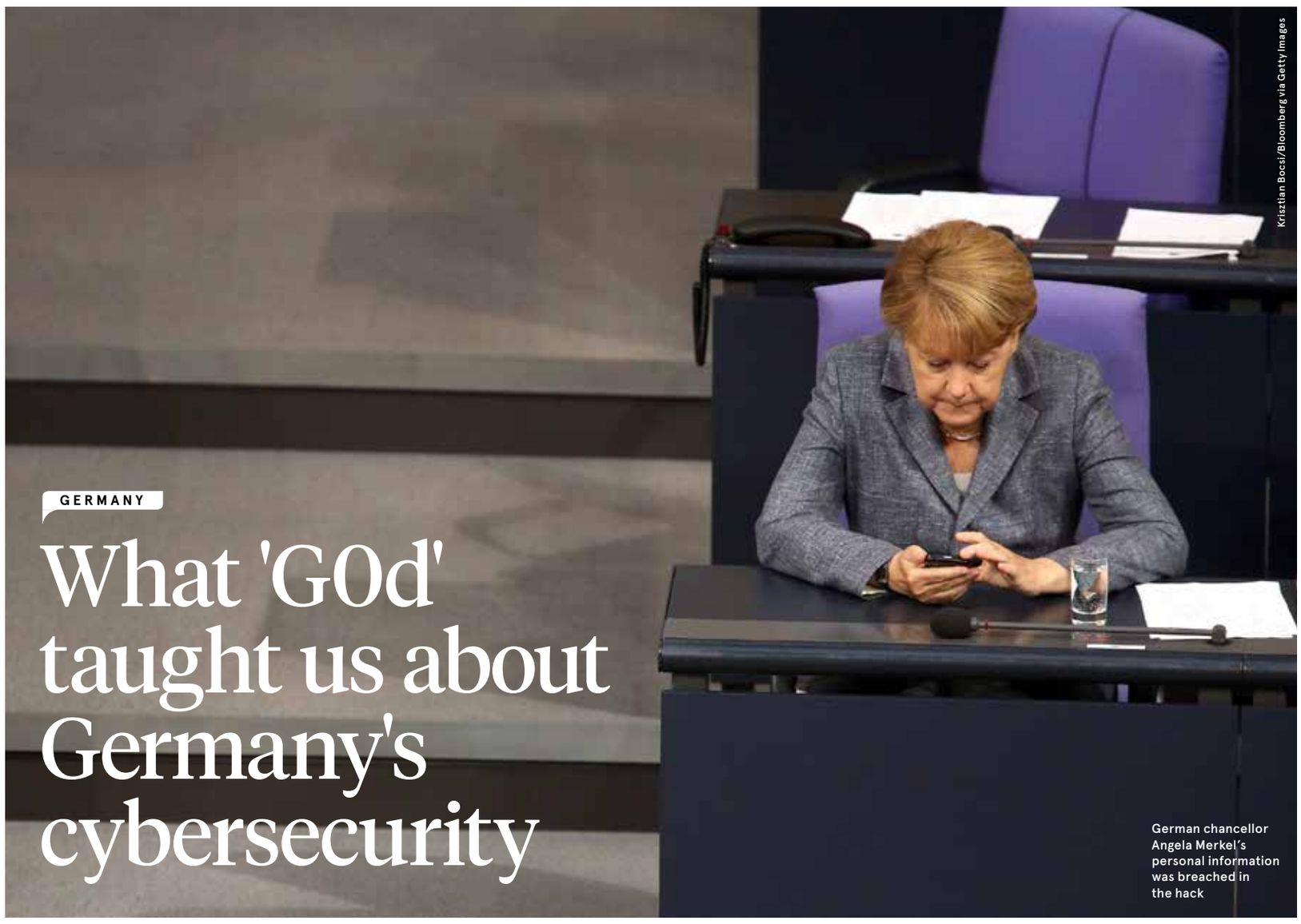
8,774
data analysts

8-hour
shifts, five days a week

52 weeks
to process the same amount of security event data machine analytics can process each year

For further information please visit www.recordedfuture.com

Recorded Future



Krisztian Bocsi/Bloomberg via Getty Images

German chancellor Angela Merkel's personal information was breached in the hack

Partially blurred tweets by Twitter account @_0rbit, which calls itself G0d, that released an 'advent calendar' of daily links to personal data and documents of German politicians and public figures in December 2018

Rawpixel.com/FreePik/AFP/Getty Images

GERMANY

What 'G0d' taught us about Germany's cybersecurity

An advent calendar of cyberattacks revealing the confidential data of thousands of German public figures revealed just how far behind the country is when it comes to its cyberdefences

James Gordon

The cyberattacks began in Germany last December. At first nobody paid much attention. But then the attacks started to become more frequent and more ambitious. Over the following few weeks, personal data relating to thousands of Germany's most influential people was published on social media by a hacker called 'G0d'. Links to confidential information, photographs and credit-card details were released daily in an advent calendar of attacks during the festive season. Panic ensued. Was this the work of a rogue nation state? Who would be next? But most troubling of all was how the security services seemed powerless to stop it.

When the authorities finally made an arrest in early-January, fear gave way to embarrassment and later to anger. The attack, it turned out, hadn't been sponsored by a rogue state. Instead, the perpetrator was a 20 year old, who had been working alone and seemingly from a very low skills-base. A determined amateur, he'd found his way into people's private lives by simply guessing passwords.

This attack, and another one, in which servers belonging to the German federal parliament were broken into four years ago, underlines just how far Germany is behind its European neighbours in cybersecurity. But it is not just politicians who have been affected. A recent report by German digital industry association Bitkom says cyberattacks have affected 47 per cent of Germany's manufacturing companies. And a study by insurance company Hiscox reveals the highest cost for a single incident amounted to a whopping €5 million.

But why is Europe's richest nation so cyber-unaware? Matthias Schulze, at the German Institute for International and Security Affairs, explains: "When it comes to the manufacturing sector, Germany is very different to the United States or UK. Its businesses are very hierarchical and steeped in tradition. This means many of them have until recently been sceptical towards digital innovation.

"It's also very difficult to integrate cybersecurity awareness and training in this rigid structure, and therefore the German manufacturing sector, which includes many small and medium-sized businesses (SMEs), is exceptionally vulnerable to attack by opportunist cybercriminals."

Curiously, UK SMEs – according to the Federation of Small Businesses there are 5.6 million operating at present – seem to be less vulnerable to cyberattacks than similar-sized companies in Germany. So why is this? Is it due to better preparedness?

Alan Woodward, a leading academic at the Surrey Centre for Cyber Security and an adviser to Europol, thinks so. He puts it down to the UK "creating a joined-up and agile network of organisations" which he says "form a powerful barrier helping the UK to fight cybercrime on many different levels".

> **Businesses are very hierarchical and steeped in tradition... many have until recently been sceptical towards digital innovation**

"It's important to understand that cybercrime can manifest itself in many different ways," says Professor Woodward. "It can be state sponsored, perpetrated by sophisticated cybercriminals, or in less serious cases, it can be carried out by so-called 'hacktivists'. Britain was quick to realise the nuanced nature of the global cyberthreat and, unlike Germany, it created the National Cyber Security Centre (NCSC).

"The NCSC, while part of GCHQ [Government Communications Headquarters], was established to stymie the threat to British industry through initiatives like the Cyber Security Information Sharing Partnership, which any business, big or small, can access to protect themselves from cybercrime. This light-touch approach, which seeks to educate, to influence businesses, rather than strong-arming them into complying, has been remarkably effective."

But with cyberattacks carried out by rogue states on the rise, it's clear that Germany, which is ranked below the United States, UK and Australia in The Economist Cyber Power Index, is playing catch-up. Its politicians believe that legislation is the answer and they are due to bring in new cybersecurity regulation during the first quarter.

Dr Schulze thinks legislation, while not an absolute panacea, can help Germany combat larger threats from rogue states.

But Professor Woodward disagrees. "The theory that passing more stringent legislation somehow makes a country safer, does not add up in my view. Why? Because cybercriminals, whether they're state sponsored or working for themselves, don't have any respect for the rule of law.

"Secondly, regulation, no matter how robust, is not fluid enough to keep pace with the digital world. Take password security for example. Five years ago people were advised to change a login password regularly. Now, however, the latest research recommends the exact opposite as the more a person changes a password, the weaker it becomes. Now imagine if password protection had been somehow enshrined in law. It would be difficult to amend and easy for hackers to exploit.

"A much better approach would be to promote more information-sharing with other EU states through institutions such as the European Cybercrime Centre and actively champion cyber-awareness best practice."

However, with more household devices such as toasters and televisions utilising the internet of things (IoT), both Dr Schulze and Professor Woodward believe protecting homes from cyberattacks is a challenge that few countries are suitably prepared for. So how would such an attack manifest itself and what is the worst-case scenario?

Dr Schulze says: "The big worry for Germany and most other states is that a rogue actor tries to take down a country's national gird by hacking into its smart meters and other strategic locations."

Professor Woodward thinks the IoT opens up a myriad of opportunities for hackers to exploit. "It doesn't have to be the grid that they try to compromise. Attacks seeking to penetrate the IoT will be much more subtle than that. In theory, if a nation state intent on cyberwarfare were to find a weakness in a smart TV, it could hack into it and create a YouTube video which would then instruct Alexa to order goods on Amazon.

"If the hackers could infiltrate enough households that have both devices, a hit like this could severely disrupt a nation's supply chain. And given that most countries rely on international supply chains, this could be damaging for a number of states."

But while America and the UK have embraced these smart devices, take-up in Germany has been slow, says Dr Schulze. This may be one cyberthreat that Germans don't have to worry about, at least for now anyway.