CYBER-RISK & RESILIENCE

02 **THWARTING THE TRICKSTERS OUT TO GET YOUR MONEY**
Phishing emails remain the main weapon used by hackers hiding in cyberspace

04 **HACKERS ARE AFTER PROCESSING POWER**
Cybercrooks are stealing computer space to "mine" for valuable bitcoins

05 **GHOSTS IN THE MACHINE KNOW WHO WE ARE**
Will our behaviour online become the only security password we need?

07 **QUANTUM COMPUTING AND CYBERSECURITY**
A new generation of quantum computing has the potential to transform security online

FAKE NEWS AND ENTERPRISE

Lies and chatbots are undermining commerce

Fake news is a disturbing problem that destabilises democracy, social cohesion, public trust and the value of truth

SHARON THIRUCHELVAM

Commercial enterprises have a vested interest to protect the value of veracity and maintain consensus around truth. Yet, far from abating, most people in mature economies will consume more fake news than truth through to 2022, according to research by technology consultancy Gartner.

The rise of truth as a binding force in scientific, legal, political and commercial practice was a gradual and hard-won achievement, argues the journalist Matthew d'Ancona in his book *Post-Truth: The New War on Truth and How to Fight Back*. "Those who blithely assume that its threatened collapse in the political world will have no ramifications in the rest of civic society are in for a shock," Mr d'Ancona warns.

Information plays such a huge part in the effective functioning of markets that they are particularly vulnerable to the manipulation of truth for commercial gain. Gartner predicts that within the next two years a major financial fraud will be caused by the spreading of highly believable falsehoods through financial markets.

"Trading on the stock market relies heavily on the automatic and high-speed consumption of content, parsing of sentiment in news stories, and application of algorithms," explains Magnus Revang, co-author of the Gartner report.

As companies increasingly demonstrate their civic values, they are vulnerable to politically motivated attacks. In August, Starbucks was the subject of a high-profile hoax dubbed Dreamer Day. Originating from the recesses of the far-right bulletin board *4chan*, the hoax was intended to troll Starbucks' chief executive, the left-leaning Howard Schultz.

A fake campaign spread through social media saying that Starbucks would offer a free or heavily discounted iced coffee to all undocumented immigrants in the US on August 11, 2017. All they had to do was line up at branches of Starbucks, where the pranksters hoped they would be met by US immigration officers.

In volatile and unstable markets fake news has the greatest potential to wreak havoc. In June, a fabricated news story, also traceable to users of *4chan*, claimed that Vitalik Buterin, co-creator of cryptocurrency ethereum, had been killed in a car crash. Mr Buterin eventually posted a selfie of himself to disprove the rumours, but by that point 20 per cent of ethereum's $4-billion market value had been wiped out.

There is more potential than ever for companies to become implicated in the fake news cycle, both as its victim and as its colluder. Indeed, fake news is a thriving industry dancing on the edges of the so-called dark arts.

With relative ease, and without having to visit the dark web, a company can employ a marketing agency to set up anonymous chatbots that will chirp endorsements of their brand through fake accounts on Twitter and YouTube. These services can cost as little as $7.

> Fake news is a thriving industry dancing on the edges of the so-called dark arts

Similarly, a recent investigation by online magazine *The Outline* has found companies secretly paying journalists to write favourable articles about their brands on mainstream news websites such as *Forbes*, *Fast Company* and *HuffPost*, without the platforms' knowledge and without declaring the content as sponsored.

Companies that advertise on discredited news sites not only fund the devaluation of legitimate news outlets, but they also undermine their own brands. According to a poll by Thomson Reuters, 87 per cent of consumers agree it is damaging for a brand to advertise on a news site associated with a fake news story, while 57 per cent, rising to 60 per cent at director level, say advertising on a trusted news site confers a more favourable impression.

Mr Revang is pessimistic about the potential for artificial intelligence (AI) to eradicate the fake news problem. The more we employ increasingly sophisticated algorithms to identify fake news, the more this will inadvertently lead to the creation of evermore sophisticated forms of fake news. He says: "We are also not only training the AI to detect fake news, but also training people to create more believable fake news."

Most fake news is made by individuals, with AI functioning as a content distributor, not as a creator. This won't last long. According to Gartner, as early as 2020, AI will be able to generate sophisticated fake news that will outpace the ability of AI to detect it, driving an arms race in the weaponisation of information.

Gartner predicts that the AI-driven creation of a "counterfeit reality" will foment further digital distrust. This will include not only words and pictures, but also video. In July, computer scientists at the University of Washington, using a form of AI called adversarial generative networks, proved they were able to manipulate and create video footage, and perfectly match it to any audio recording.

As fake news grows more pervasive and sophisticated, companies might be tempted to test the limits of truth. Indeed, simple economics dictate that it is a lot easier to make things up than it is undertake reliable research, and it is a lot cheaper to produce fake news stories than it is to detect and repudiate them.

But short-term gains will only be followed by long-term reputational costs. Instead, Gartner says, companies have a pressing responsibility to draw up a suitable code of digital ethics for their industry that should inform their public relations, marketing, product development and sales practices. At the same time, it would be in companies' best interests to train employees to ensure they are inclined and skilled to discern the truth.

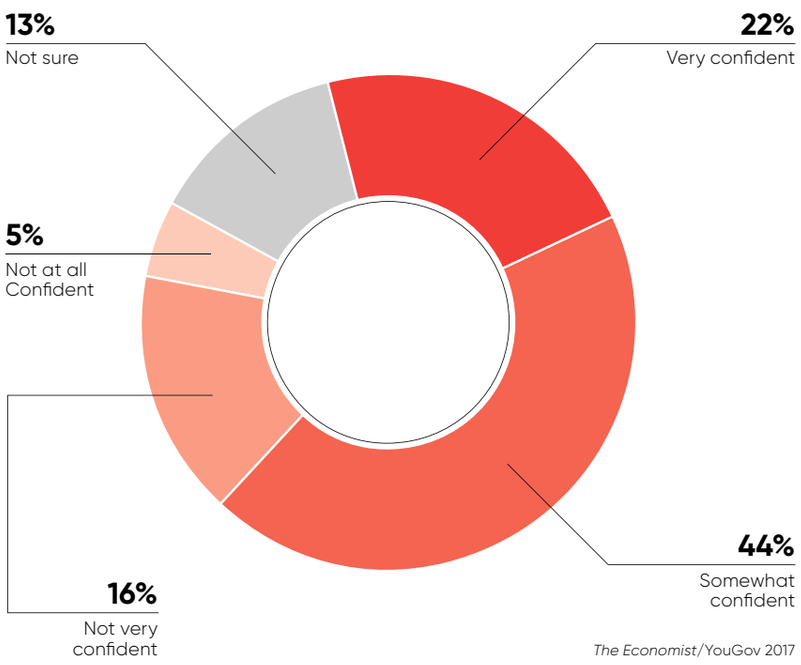
Commercial enterprise should also collaborate to quash the economic incentives that underpin the fake news market. Towards this end, social media sites and technology platforms such as Google, where fake news flourishes, could do more to pull their weight.

The information company LexisNexis relies on data from multiple news sources to provide its business-to-business customers with reliable data for legal, regulatory, research and reputation management purposes.

Pim Stouten, director of strategy at LexisNexis Business Insight Solutions, explains that social media remains an opaque category. "Most social platforms know their data is quite the gold mine, so they are reluctant to give you access to the full dataset. You have to rely on them that you are getting a complete subset relevant to the research or analysis you are doing," he says.

IDENTIFYING FAKE NEWS

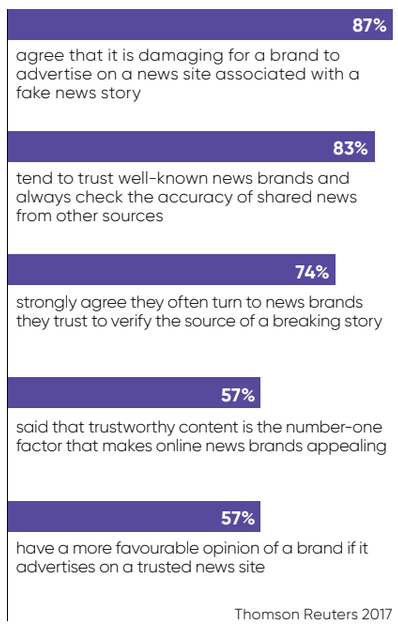
US ADULTS WERE ASKED HOW CONFIDENT THEY ARE IN IDENTIFYING REAL NEWS FROM FAKE NEWS



The Economist/YouGov 2017

AWARENESS OF FAKE NEWS

REUTERS.COM USERS WERE POLLED ABOUT FAKE NEWS AND ITS IMPACT ON ADVERTISING ONLINE



Thomson Reuters 2017

DISTRIBUTED IN
THE SUNDAY TIMES

RACONTEUR

PUBLISHING MANAGER
Jack Pepperell

PRODUCTION EDITOR
Benjamin Chiou

MANAGING EDITOR
Peter Archer

DIGITAL CONTENT EXECUTIVE
Elise Ngobi

DESIGN
Samuele Motta
Grant Chapman
Kellie Jerrard

CONTRIBUTORS

ADRIAN BRIDGWATER
Specialist author on software engineering and application development, he is a regular contributor to *Dr. Dobb's Journal* and *Computer Weekly*.

PÁDRAIG FLOYD
Former editor in chief of the UK pensions and investment group at the *Financial Times*, and ex-editor of *Pensions Management*, he is now a freelance business writer.

DAVE HOWELL
Freelance journalist, writer and micro-publisher, he specialises in business and technology, and has written for a range of publications and websites.

SHARON THIRUCHELVAM
Writer specialising in culture and innovation, she has contributed to *The Independent*, *i-D*, *Vice* and *Forbes*.

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

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

@raconteur
/raconteur.net
@raconteur_london

RACONTEUR.net /cyber-risk-resilience-2017

COMMERCIAL FEATURE

Time to grow up: why cybersecurity maturity is crucial for organisations

A true analysis of cybersecurity can show organisations where they are at risk and measure the return on investment of cybersecurity spending

IMPORTANCE OF CYBERSECURITY MATURITY

Achieving cybersecurity maturity (CSM) enables the IT security team within an organisation to report on the status of their organisation's security posture with confidence. Through consistent monitoring and risk analysis, a clear perspective can be provided to the board. A high level of CSM is also proven to reduce overall cybersecurity spend over a three-year period.

CNS Group, an independent cybersecurity consultancy, has developed Aegis, a comprehensive CSM service. The service provides organisations with a concise and contextual reporting mechanism for cybersecurity to the board and other stakeholders. By expediting CSM and visibility, organisations of all sizes can show return on investment from cybersecurity spend, and eradicate unpredictable and ineffective spending.

WHAT IS CYBERSECURITY MATURITY?

CSM is the effectiveness of an organisation to make cybersecurity decisions in a way that considers all relevant factors on a changing technology and threat landscape; the ability to improve defences continuously while the business operates and transforms. Organisations that invest in creating a concise and accurate view of their cybersecurity state and can communicate this clearly with the rest of the business see the benefits in terms of confidence and more informed, collaborative decision-making around the value of cyber-investment.

CYBERSECURITY CHALLENGES

01 **Complexity of information for the client**

From threat intelligence, compliance and regulations to security-testing and audits, the amount of information that an organisation is required to digest and base investment decisions on is growing. Not only does this impact the level of resources and skills required from the internal IT team, but it is confusing for the extended team of stakeholders. The maze of information and limited visibility across the overall IT infrastructure can leave an organisation vulnerable.

02 **Unpredictable and ineffective spending**

With no clear reporting model, organisations are basing their investment decisions on the results of the latest penetration test, security audit or pressure from existing or new regulations in force. This never-ending project-based model doesn't allow for continuity and intelligent spend over time. The traditional cybersecurity spend becomes a pattern of testing, part-fixing, requesting more budget, spending budget, testing – and repeat.

03 **Confusing and growing compliance landscape**

From the European Union General Data Protection Regulation, PCI Security Standards Council compliance, Cyber Essentials to ISO standards, the compliance landscape is a minefield for any organisation. Although achieving compliance enables organisations to achieve a level of best practice and is a helpful negotiation tool for budget requests, it doesn't mean that an organisation is completely protected. The constant changes in regulations also require up-to-date knowledge and skills within the IT team.

MEASURING THE CURRENT STATE OF CYBERSECURITY MATURITY

There are a few variations and grading scales for measuring CSM with the most common being the COBIT maturity scale. Recent research using the COBIT scale found that only 22 per cent of IT security professionals surveyed believed their CSM level to be optimised. Almost 20 per cent stated their level of maturity as non-existent, ad-hoc or didn't know.

This growing lack of control and visibility directly impacts how informed and prepared an organisation is to deal with either attempted or successful attacks. If a chief information security officer (CISO) wants to have an informed business conversation with their executives about risk, they need the same level of confidence in their presentation of cyber-performance data and reporting as the finance director would have in the numbers they bring to the board.

AEGIS: A COMPREHENSIVE CYBERSECURITY MATURITY SERVICE

A change is required in the way we manage and report on cybersecurity and CSM offers the most effective way to manage that change. To simplify CSM for organisations and support a higher level of CSM, CNS Group developed Aegis.

Aegis is a CMS transformation programme incorporating a proprietary benchmarking tool, active dashboard and consultancy services. CNS Group specialists use the programme to support organisations in measuring and scoring their current CSM against five key domains and 73 sub-domains.

This intelligence then provides the contextual, prioritised transformation plan for the organisation to reach its cybersecurity goals. The Aegis CSM scale draws measurements from standards including: ISO 27001; Cyber Essentials (Plus); PCI DSS; SANS/CIS/CPNI – top 20 critical control set; Sarbanes Oxley; SEC OCIE; and NCSC HMG IA maturity model and risk management principles.

The CSM market remains immature. CSM dashboards often omit one of the critical components that CNS Group's Aegis platform measures or fail to provide automated, systemised reporting for elements such as penetration-testing outputs or threat intelligence. Many solutions have their own reporting function, which may or may not be reviewed regularly, their own vendor point of contact, owner, interface into the business and assigned budget. The result is impenetrable complexity with multiple vendor conversations, stressed management overhead, conflicting advice due to limited context, and an increasing number of gaps, crossover and duplication.

The Aegis programme enables organisations to standardise and automate as much data input as possible. It gives organisations a clearly defined dashboard of business metrics to articulate cyber-risk and benchmark cyber-technology, resources and investment. This form of analysis and reporting drives better, more informed cyber-conversations with every stakeholder in the business, especially at board level.

Organisations that invest in CSM can all confidently answer these questions: Compliance and accreditation: are we meeting all mandatory regimes and standards? Technical compliance: where are the vulnerabilities and poor controls in our infrastructure, and what are we doing about them? Transformation and maturity: what's our current status across all projects? Events, alerts and threats: how good is our internal and external threat intelligence? Governance and policy: how robust is our policy compliance; where are the exceptions and who owns what?

Using an agreed benchmarking process allows CISOs, IT security managers and chief information officers to create a contextual plan of action, track and share improvements, and report concisely on the value and impact of every investment. At CNS Group, we have seen the positive impact of the transformation in CSM demonstrated through better targeted investment, more robust compliance and effective allocation of resources.

The graph demonstrates how an organisation can and should drive value from its cybersecurity spend. The Aegis programme is proved to reduce cybersecurity spend over a three-year period.

CNS Group's comprehensive CSM service enables organisations to transform the quality and value of short, medium and long-term planning and decision-making. The primary benefits of Aegis aim to provide a concise and contextual reporting mechanism for situational cybersecurity to the board and stakeholders; expedite a client's CSM and visibility; show return on investment for cybersecurity spend; organise and prioritise future cybersecurity spend for greatest risk reduction; highlight the greatest areas of cybersecurity weakness for immediate action; identify greatest threats to an organisation by type; and reduce a client's overall cybersecurity spend over three-year period.

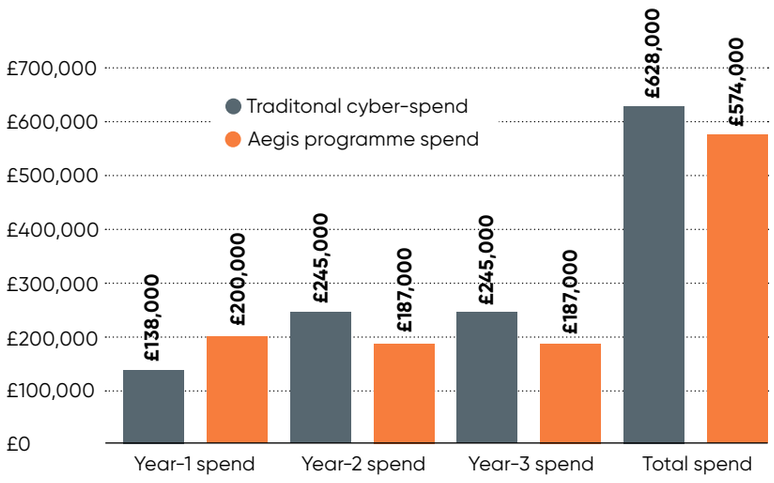
In addition, the CSM service allows organisations to identify the key and common criteria for successful cybersecurity by customer and by industry; ensure compliance to pertinent and mandatory regimes; reduce stress on inter-departmental management and overheads; improve cybersecurity awareness across an organisation; and promote a framework driven approach that ensures a complete picture of the cybersecurity state.

By improving the level of CSM through CNS Group's Aegis dashboard and consultancy services, IT security teams can finally have the confidence deserved in today's complex threat landscape.

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

TRADITIONAL CYBERSECURITY SPEND COMPARED WITH CYBERSECURITY SPEND ON AEGIS PROGRAMME

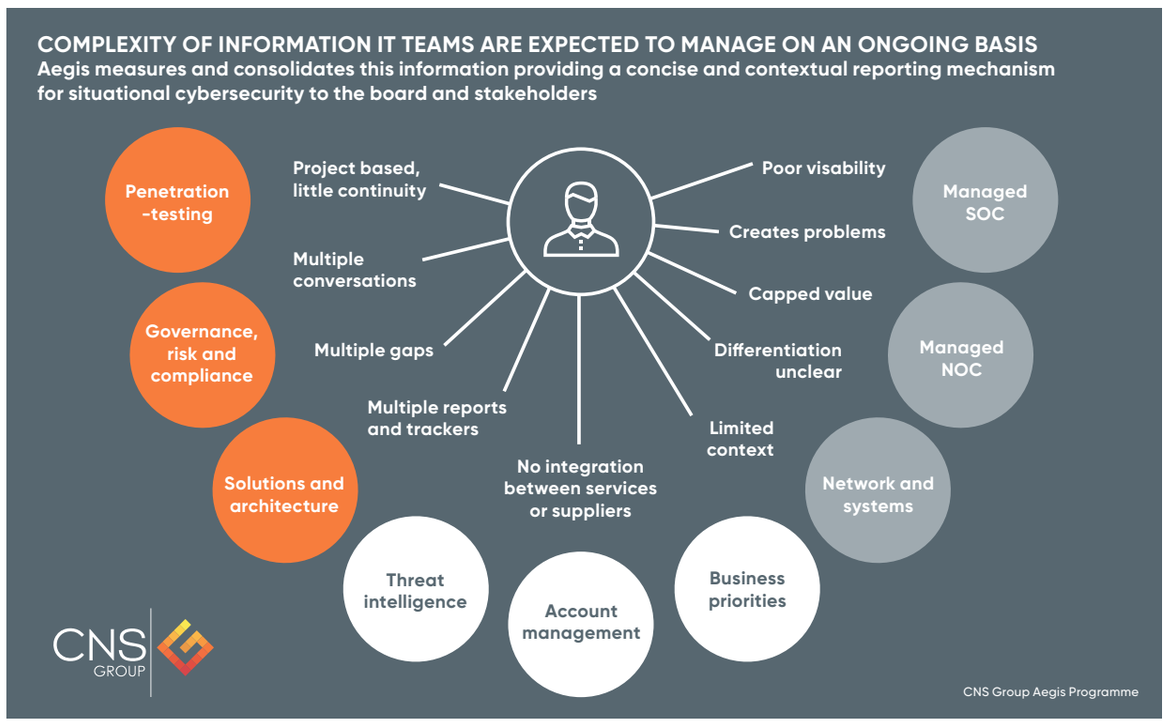
Overview of company's full cybersecurity posture from Aegis provides framework for future spend



CNS Group Aegis Programme

COMPLEXITY OF INFORMATION IT TEAMS ARE EXPECTED TO MANAGE ON AN ONGOING BASIS

Aegis measures and consolidates this information providing a concise and contextual reporting mechanism for situational cybersecurity to the board and stakeholders



CNS Group Aegis Programme

Research was carried out at Infosecurity Europe 2017. Total sample size was 172 IT security professionals. Fieldwork was undertaken June 6-8, 2017. The survey was carried out face to face.

SOCIAL ENGINEERING

Jason Hetherington/Getty Images

Thwarting the tricksters out to get your money

Phishing emails remain the main weapon used by hackers trying to steal valuable information and cash, but there are ways of protecting your business

DAVEY WINDER

Think of social engineering, in the context of information security, and you probably conjure up an image of Nigerian scammers promising millions in return for bank account details plus a small transaction fee. You probably don't think that it might involve the "virtual kidnap" of a loved one.

Michael Levin, formerly deputy director of the National Cybersecurity Division of the US Department of Homeland Security and now chief executive at the Center for Information Security Awareness, recounts how the threat works.

Making full use of intelligence from social networks, as well as the malware compromise of mobile devices, attackers stage a fake kidnapping. A call, possibly spoofed to look like it's coming from the victim's phone, informs you of the hostage-taking and ransom demand. You may hear what could be your partner sobbing or screaming in the background.

This is social engineering at its most evil; the devil literally being in the detail. By hacking into your computer, your phone and your social networks, they know enough to make the threat very convincing indeed. By compromising a smartphone and having access to the GPS location information, the cybercrooks can even convince the victim that they are watching them.

Panic is induced and ransoms are paid. Earlier this year, the FBI arrested one woman allegedly involved in such scams, involving $28,000 in ransoms.

More commonly criminal social engineers will look to employ such intelligence gathering exercises to gain access to corporate networks and the valuable data stored within. The *2017 Verizon Data Breach Investigations Report* shows one in every 14 phishing emails results in a malicious attachment or link being opened, and phishing is now present in one in five security incidents.

What's more, the latest *Enterprise Phishing Resiliency and Defence* report, from social engineering educators PhishMe, reveals such attacks are up 65 per cent from last year. That's worrying as phishing is the de facto tool of social engineering used by cybercriminals to hack humans and gain access to enterprise networks and the valuable data they contain. Some 15 per cent of these emails, according to the PhishMe report, will contain a malicious link and rely on entertainment, social media connections or reward as the emotional encouragement to click through.

So, how can the organisation best ensure that relevant employees are both aware of these threats and enabled to deal with them accordingly? To answer this, we first need to consider who those relevant employees are?

> Employees can become the first line of cyberdefence, able to spot a socially engineered phishing attempt a mile off

Graeme Park, senior consultant at Mason Advisory, says the simple answer is everyone. "It's usually easy enough to elevate a user account to an administrative account or take control of another computer once they have access to the company infrastructure," he says.

But some employees make more attractive targets, according to Mark Crosbie, head of trust and security at Dropbox, who warns that "those with strict business targets can be particularly at risk". Sales staff might be susceptible to being lured with the promise of a business lead, especially as, Mr Crosbie points out, "they often work with external organisations, so giving the attackers added scope to mimic trusted sources".

The C-suite should also look to itself as a potential target. The *iPass Mobile Security Report* suggests C-level executives, including the chief executive, are at the greatest risk of being hacked. This comes as no surprise to Alan Levine, cybersecurity adviser to Wombat Security, who points out that business leaders' digital identities "can be golden keys to valuable personal and professional data".

Stephen Burke, chief executive at Cyber Risk Aware, recalls one chief financial officer (CFO) receiving a fake email supposedly from the chief executive and instructing him to wire money into an account with an explanation promised on his return from a meeting.

"The result was the CFO wired the money and the success of this fraud was down to the fact that the criminals knew the CEO was out of office," says Mr Burke. How did they know? By simply calling the company, using publicly available information from social and corporate media, and establishing the chief executive's agenda for the day on some believable pretence.

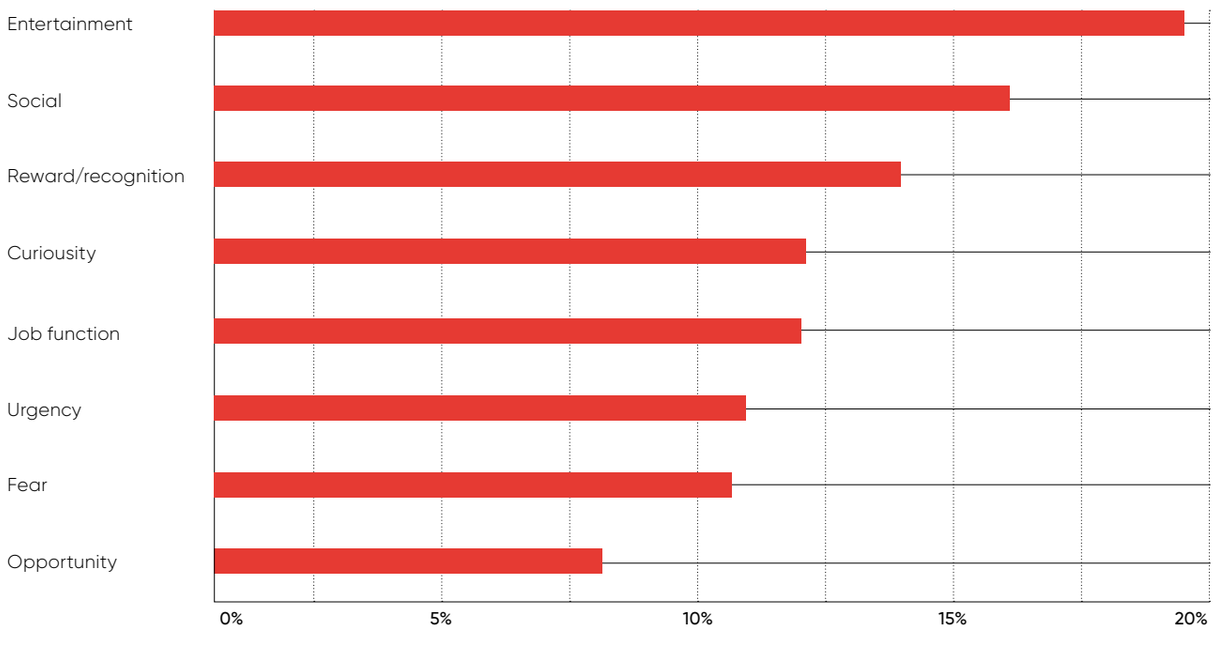
That's not to say that people should be considered the weakest link in security; quite the opposite. Aaron Higbee, co-founder at PhishMe, argues that with effective conditioning techniques in place "employees can become the first line of cyberdefence, able to spot a socially engineered phishing attempt a mile off".

So is awareness training the be all and end all of social engineering defence? "Advising people not to open suspicious emails, click on unexpected attachments or visit unvalidated websites only works if the attachment or email looks suspicious or the website is evidently a spoof," says Amanda Finch, general manager of the Institute of Information Security Professionals. The problem is that the threat actors are getting better at what they do and pulling the right triggers to offset suspicion.

Steven Furnell, professor of IT security at Plymouth University, recommends using the LIST acronym to emphasise core cyber-principles is the best method of achieving this. Legitimacy: should you be asked for this information and would you normally provide it this way? Importance: what is the value of this information and how might it be misused? Source: are you confident that the source of the request is genuine and can you check? Timing: do you have to respond immediately? If in doubt, take time to ask for help.

MOST SUCCESSFUL PHISHING CAMPAIGNS

AVERAGE RESPONSE RATE BY CATEGORY OF PHISHING CAMPAIGN



PhishMe 2017

WHY HACKERS HACK

MOTIVES BEHIND CYBERATTACKS

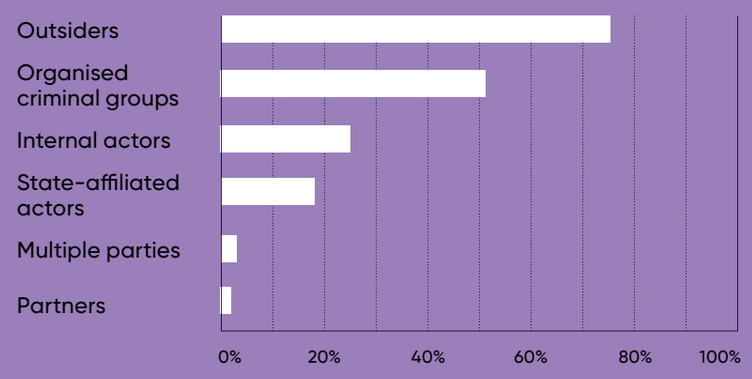
GLOBAL STUDY OF LARGE ORGANISATIONS THAT WERE VICTIMS TO A CYBERATTACK

41%	27%	26%	26%	24%	20%	11%
Ransom	Insider threat	Political	Competition	Cyberwar	Angry user	Motive unknown

Radware 2017

WHO'S BEHIND DATA BREACHES?

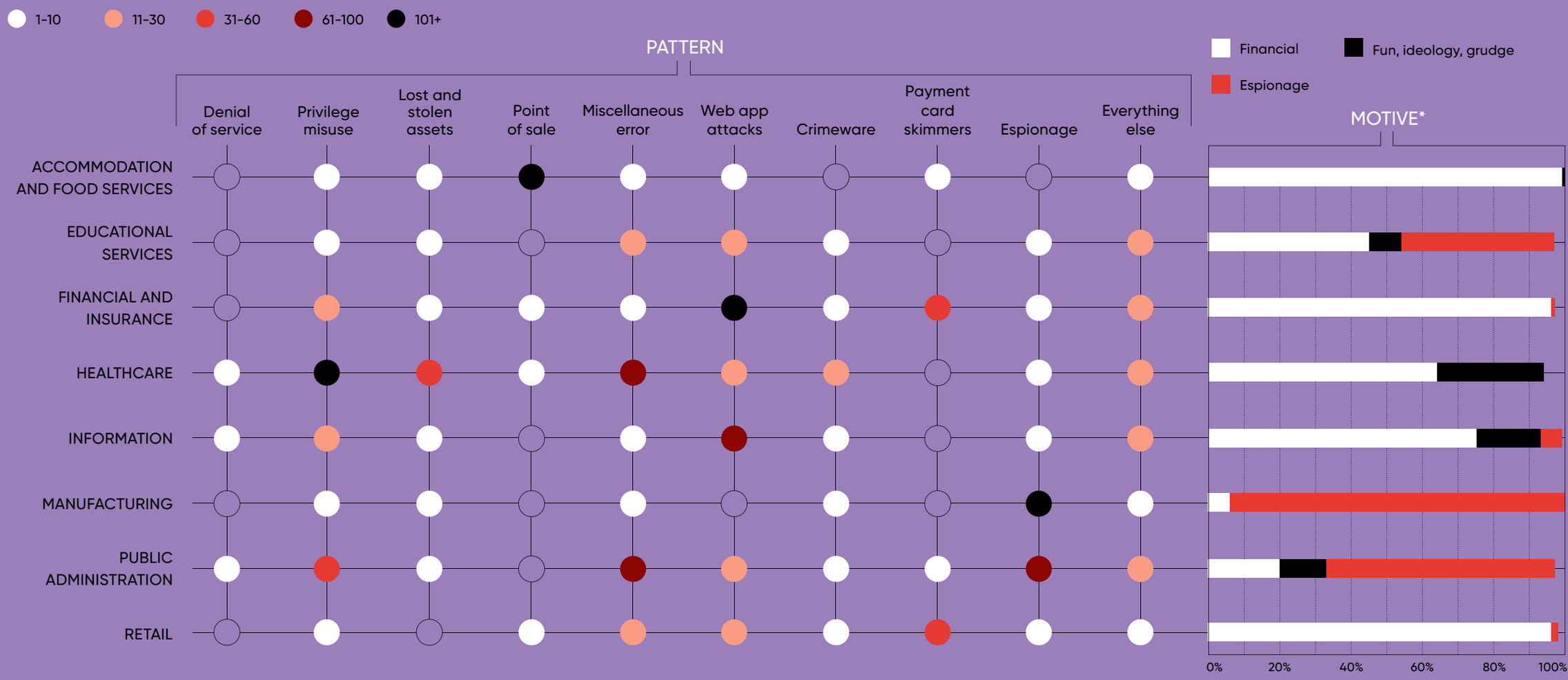
GLOBAL STUDY OF ALMOST 2,000 DATA BREACHES



Verizon 2017

DATA BREACHES, BY PATTERN AND MOTIVE

GLOBAL STUDY OF ALMOST 2,000 DATA BREACHES



*Some motives were unknown so not included in this data

Verizon 2017

OPINION COLUMN

'We want to give people more confidence in how their data is used'

KAREN BRADLEY
Secretary of State
Department for Digital, Culture, Media and Sport

Big data is often called the black gold of the 21st century and it is easy to see why: it is transforming consumer choice, helping improve healthcare and education, and revolutionising our homes.

Many businesses in our thriving digital economy rely on the collection and exchange of data, which is often personal and sensitive in nature. But research shows people are increasingly concerned about how their personal information is used. Some 80 per cent feel they don't have enough control of their own data. And that's bad news for everyone, ordinary people and businesses alike.

That is why we are revising data protection laws for the digital age through our Data Protection Bill, which is the first major review of the legislation since 1998.

This government's Industrial Strategy, published last month, set out our plans to build a Britain fit for the future, with increased productivity and better, higher-paid jobs in every part of the UK. Growing our data-driven economy is a central part of that plan.

And our Digital Strategy, published earlier this year, also made clear our commitment to unlocking the power of data in the UK economy.

We want to give people more confidence in how their data is used, so they can make the most of digital opportunities and so responsible businesses can use that data well, from major internationals to any small business with a customer database.

We will give people the right to be forgotten, beyond what is already offered by Google and other search engines, and to ask for their personal data to be erased. That includes the right to ask social media channels to delete information posted in childhood. And we are expanding the definition of personal data to include IP addresses, DNA and internet cookies.

We will also end the overuse of pre-selected "tick boxes". Many websites assume consent to their privacy policies unless individuals take steps to opt out, but we know people rarely read the small print. In future, explicit consent will be required before anyone's data can be used.

These plans are primarily designed to protect individuals' privacy, but that makes them good for business too. People are more likely to entrust their data where they know it will be handled carefully and safely.

The measures will be brought in through the Data Protection Bill and aligned with the General Data Protection Regulation, which comes into force in May 2018. After that the regulator for data protection, the Information Commissioner's Office (ICO), will be able to issue fines of up to £17 million for the most serious breaches of the rules and even pursue criminal prosecution. Any organisation whose data processing is considered high risk will be obliged to carry out impact assessments.

So every business and organisation which relies on the use of data will need to be ready. And we have made sure there is plenty of help available. The ICO is providing a range of dedicated products to help people prepare and its website is the place to visit to get the information you need.

This is a significant cultural shift in how data is handled. It puts the emphasis firmly on privacy without compromising the ability of business, the third sector or public services to function. The changes will require adjustments from those handling data, but it will free our data-driven economy to grow and create jobs as we build a country that's fit for the future.

COMMERCIAL FEATURE

Beware the insider threat in the war against cybercrime

Jon-Louis Heimerl, manager of the threat intelligence communication team at NTT Security, tells how to improve your defences against cybercriminals

The desire to bolster cybersecurity may be jumping up the list of priorities in boardrooms across the UK, given the uncomfortable rash of headline-making attacks in 2017. However, shoring up defences against external dangers is not enough on its own.

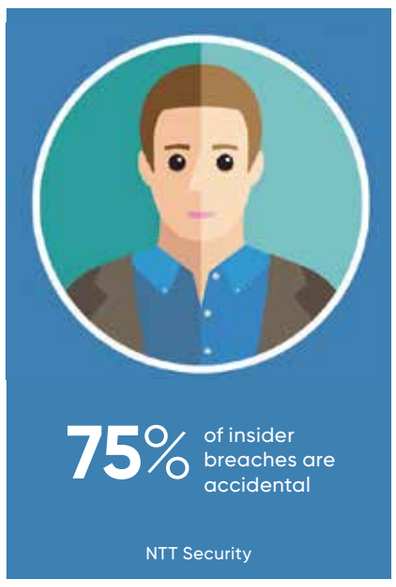
Few in the C-suite realise the potential risks of the so-called insider threat, not least because it is not always who you think it will be. The insider threat can be more lethal because once hackers have authorised access they can run riot.

NTT Security's latest *Threat Intelligence Report*, published in November, highlights that about 10 per cent of the incidents we have dealt with this year have been related to insider breaches. In truth, the percentage may be even higher; companies don't always know when they have been compromised, especially if the attack is triggered internally, whether intentional or not, and limited alarms are set off because the hacker often has authorised access.

Recently we had a new client who took two years to realise hackers had breached their system and the average detection time is thought to be around 190 days. While undetected, cybercriminals can access essential digital assets and sensitive data, such as payroll details, research-and-development plans and anything of value, if the right precautions have not been taken.

Since the beginning of 2016, only about 25 per cent of insider breaches with which NTT Security has been involved have been related to overtly hostile activity, specifically an inside attacker stealing corporate resources or information. The remaining 75 per cent of insider activity has been either accidental or negligent.

Unfortunately, accidents happen every day in the workplace. It can be something as seemingly trivial as mistakenly sending an email to someone thanks to a slip on the keyboard. Negligence mostly occurs when system administrators fail to back up properly, use patches or update applications as quickly as possible. Similarly, catching malicious insider threats is usually down to good management.



Consider that, on average, around 70 per cent of employees can access digital assets they shouldn't be allowed to. A majority of companies have not yet taken the steps to limit this exposure, though the introduction of the General Data Protection Regulation in May should encourage organisations to tighten their defences.

In your office you might have access to human resources records, payroll or other files you don't necessarily need. If you have highly sensitive information critical to your operation, and it is not segregated from other parts of the network, then that is problematic.

At NTT Security, we perform a variety of assessment services and you would be shocked at the number of times we are able to penetrate organisations with ease. Too often they have an internal structure which is completely flat; there is no segregation and only limited data protection.

To minimise the impact of insider threats, one of the most important things an organisation can do is segregate their information by using sub-networks in protected internal networks. This system can be simple for a chief information security officer to employ and cost effective. Crucially, it means that even if hackers come on to your network and gain a foothold, they will have to breach your internal subnets before they can succeed in exfiltrating valuable data.

Elevated security controls will help make sure users can't stroll from segment to segment. In addition, you need to establish a good authorisation password, and carefully and constantly monitor who should have control and access to a certain subnet. This is not necessarily a hard job, but it can take some time because you have to keep an eye on a lot of moving pieces. Anything we do to protect against the hacker at that level is also helping to limit an insider breach, whether it is accidental, caused by negligence or deliberate.

A final point to stress is that crisis planning is vital. If you are breached, from inside or out, you want to deal with it in the most efficient way, and that comes with practising and firming up necessary processes, including your incident-response handling. The longer it takes to deal with a cybersecurity issue, the more damaging it can be, especially when the GDPR comes into force, both financially and in terms of brand reputation. Ultimately, it is imperative not to make it easy for the criminals, from the inside out.

Download the NTT Security GTIC 2017 Q3 *Threat Intelligence Report*: www.nttsecurity.com/gtic-2017-q3

COMMERCIAL FEATURE

Predict and prevent cyberattacks with AI

Artificial intelligence and machine-learning can help predict and prevent cyberattacks before they have a chance to sink your business

At the end of a year pockmarked by an unprecedented number of cyberattacks, it is clear employees and users are often targeted by hackers to gain access into an organisation.

The evidence points to the reality that people are fallible. However, all is not lost, according to Dr Anton Grashion, Cylance's senior director of product and marketing for Europe, the Middle East and Africa. "As an industry we have failed to protect people from attackers and the onus is on us to prevent harm before it can even begin to have a negative effect on individuals or businesses," he says.

Dr Grashion, whose company vows "to protect every end-point under the sun", believes the solution to this mushrooming issue is to combine human effort with machine speed and accuracy. He says: "With artificial intelligence (AI) doing the bulk of the work of pinpointing suspicious malware or activity, humans can then focus on a smaller group of suspicious files or behaviour to determine what is potentially dangerous.

"This way people are no longer faced with an insurmountable amount of data that we can't process quickly enough to be effective. Ultimately, we want to give people time back to be more productive."

Recent technological advancements, specifically in AI, now enable us to prevent 99.8 per cent of attacks before they happen. Dr Grashion says: "Another benefit of utilising machine-learning and AI is that they allow us to remove clunky and intrusive security controls, and use more intelligent, lightweight and effective countermeasures against cybercriminals.

"We humans are hardwired to trust other people and that is precisely why social engineering works for hackers. That is not going to change any time soon, so to boost cyberdefences you have to help people make the right decisions or, even better, avoid having to make a decision, which is only possible if your systems are intelligent enough to support this approach.

"We don't depend on normal people, outside of your security and IT teams, to become cyberexperts. Frankly, it's unfair of us to ask it of them. The landscape is constantly changing and cyberattacks are evolving, so how do you keep pace?

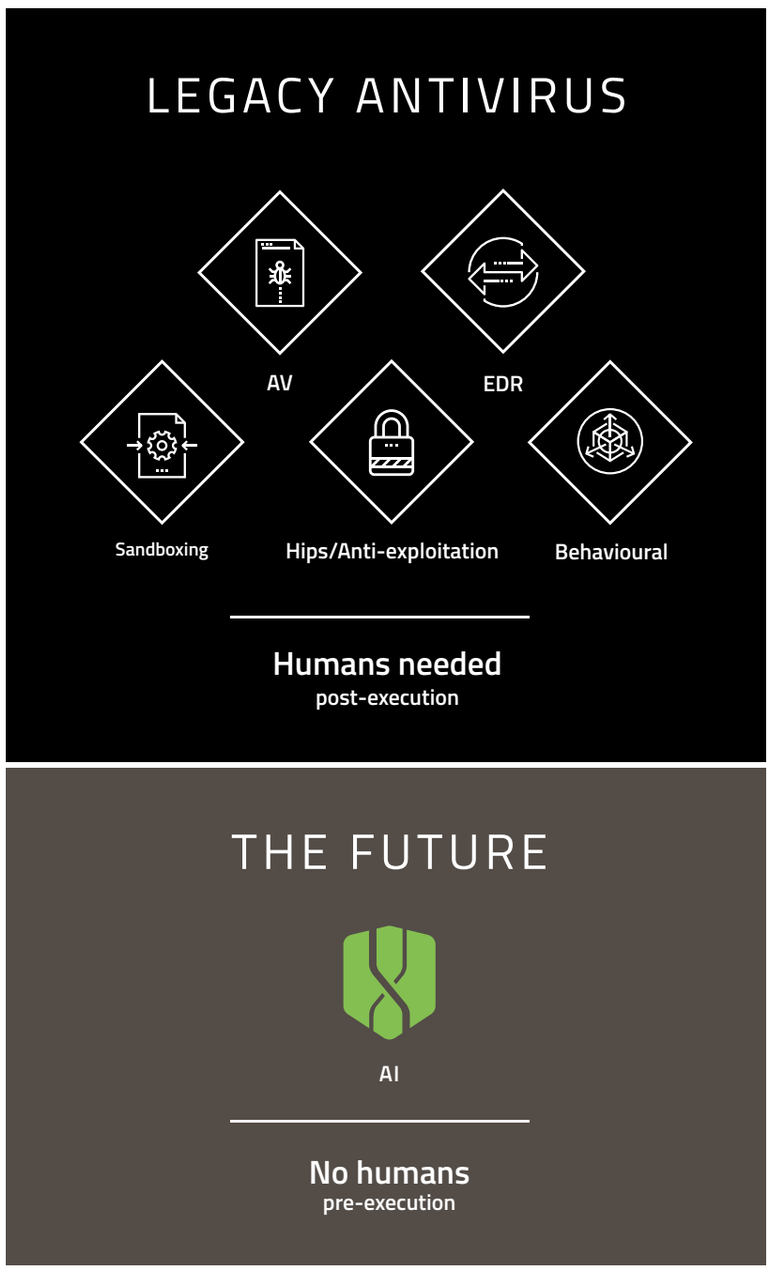
"Even old, known malware continues to cause brand damage, breaches and financial losses. How do you ensure you are covered from new or evolving attacks further down the line when we can't even seem to gain a handle on threats that were identified five years ago?"

To explain the current approach towards cybersecurity, Dr Grashion uses the analogy of a rowing boat with a large hole in the bottom, taking on water. "The first thing to do is reduce the flow of water into the boat," he says. "You don't want to have to get a bigger bucket to try and bail the water out, and that is where we are today.

"At present we are reactionary, springing to action only after the attacks have breached our systems and compromised the data we have tried to protect. Over the past five years, the balance from prevention to detection and response have been disproportionate. The prevailing thought has been that 100 per cent prevention is not possible, therefore you must invest more on detecting breaches and respond accordingly.

"But, returning to the boat analogy, with AI we can significantly reduce that hole so that there is just a tiny trickle of water. And at the risk of mixing my metaphors, the present detect-and-respond logic is faulty because it is as though you are choosing between who is the best undertaker in removing the victims.

"By improving your prevention stance there is no 'patient zero'. Organisations such as Cylance use AI and machine-learning to predict and prevent attacks before they have a chance to sink your boat. Therefore, I urge business leaders to rebalance their cybersecurity budget to reflect this change in improved defence, because it works. You still need to have detect and respond covered though; even with the AI, a minuscule amount of things still get through."



> The more advanced cyberattacks become, the more we will have to rely on AI – people alone don't stand a chance

The California-headquartered software engineers Cylance, established in 2012, spent two years working on a product that could prevent many of headline cyberattacks in 2017. "We took petabytes of data, both good and bad, and trained our AI model to differentiate between these categories of executables," explains Dr Grashion. "The power of this AI-based approach is that it doesn't have to have even seen the specific malware to predict and prevent it.

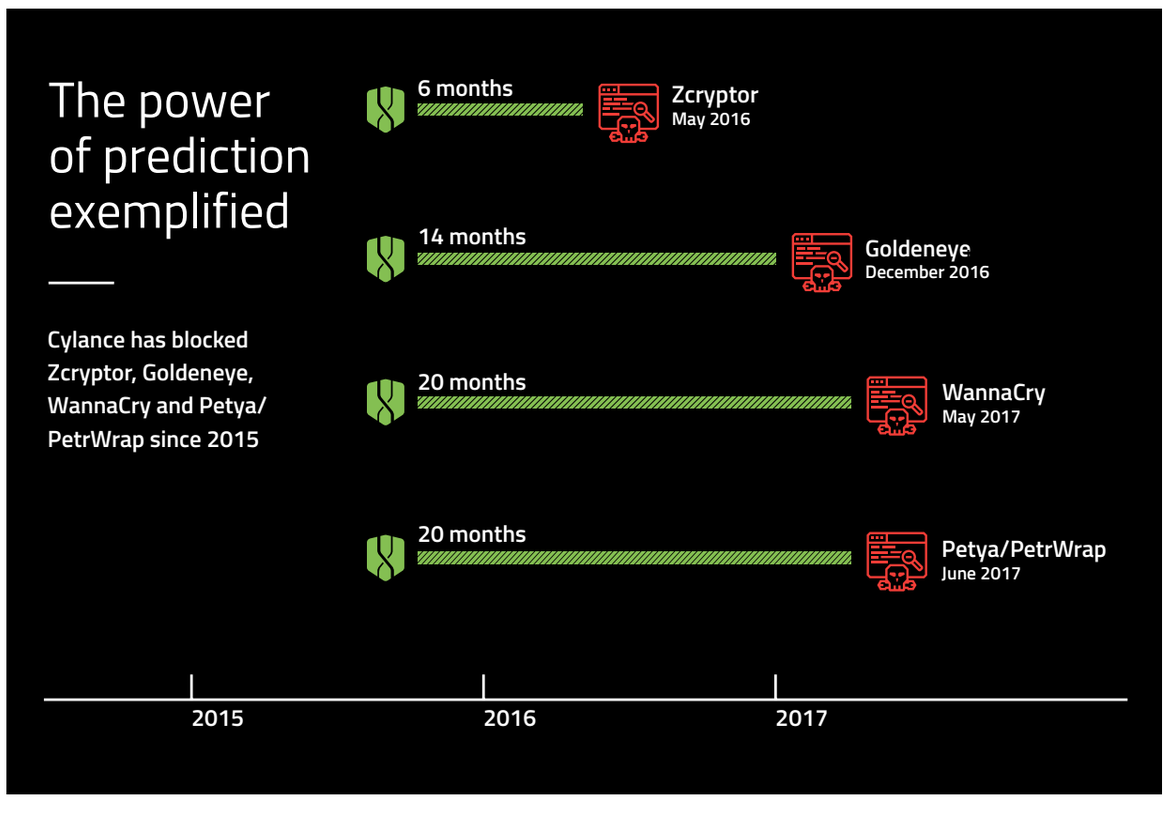
"We stopped a wholly quadrillion of ransomware – WannaCry, Petya, PetrWrap, Goldeneye and ZCryptor – with a mathematics-led AI model from 2015, long before they were in existence. The model could not have known about them in theory, but it worked because of the power of prediction the AI model delivers. In layman's terms, our model could predict these new, emerging threats based on factors and features they share with threats we already knew about. Those factors make these unknown files suspicious of being malware and stop them in their tracks."

To highlight how complex and robust the end-point-deployed Cylance AI model is, Dr Grashion reveals there are some two million features. "One of them is based on the entropy of a file. And if you were to only use that feature it would be fairly good at identifying malware; combine it with the other features and you can gain a good idea of where the prevention accuracy comes from. Further, you don't need to be connected to the internet for cloud lookups or to track behavioural changes; it still works perfectly if you are offline or on air-gapped critical infrastructure."

With the introduction of the General Data Protection Regulation (GDPR) looming, there has been much fretting by business leaders about cybersecurity, given the numerous breaches that have compromised industry-leading organisations. Dr Grashion posits that if organisations alter their thinking – from detect and respond to prevention, using AI – then GDPR need not be anywhere near as threatening, in terms of both finance and reputation, as many fear.

"There is a lot of nonsense talked about AI and people have conflicted views about it," he adds. "The likes of Elon Musk and Stephen Hawking might say that AI will lead to the end of the world, but what we are discussing in this instance is solely cybersecurity. And this application is quite simple: it determines whether or not an executable file is good or bad. The fact is the more advanced cyberattacks become, the more we will have to rely on AI – people alone don't stand a chance."

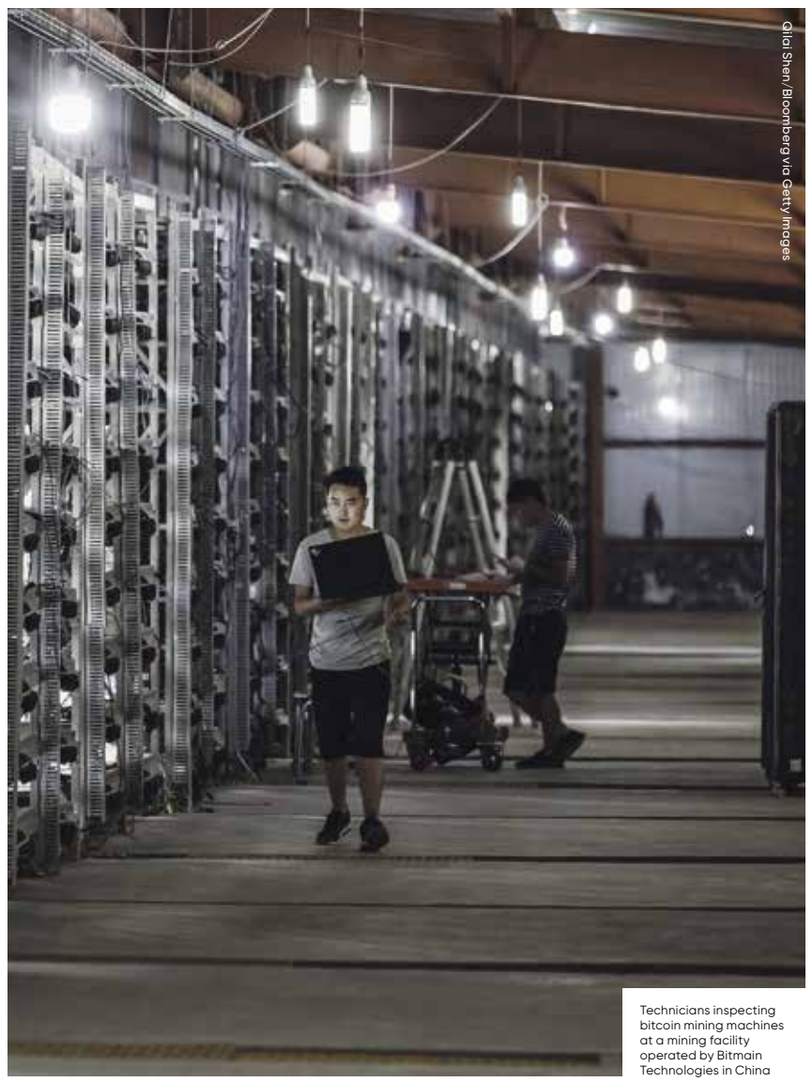
For more infomation please visit www.cylance.com



CRYPTO-JACKING

Hackers may be after processing power to get valuable bitcoins

Organisations with big computer processing power are now the target of cybercrooks with malware designed to "mine" for bitcoins


Qilai Shen /Bloomberg via Getty Images

Technicians inspecting bitcoin mining machines at a mining facility operated by Bitmain Technologies in China

PÁDRAIG FLOYD

Cyberattacks are no longer limited to the unlucky few, but have become worryingly common. And now, in addition to ransomware, the usual source of denial-of-service attacks, there is another, low-key form of criminal assault spreading in cyberspace.

Rather than locking down systems until their ransom terms are met, some hackers are prepared to play a longer game with a valuable prize in their sights – cryptocurrencies.

This is because cryptos have become so lucrative, with bitcoin increasing by more than 900 per cent and ethereum by more than 2,500 per cent so far in 2017.

The attack goes like this: hackers seek to infiltrate a company's systems and capture a small portion of its computer processing power to "mine" for coins, a process called crypto-jacking.

Mining cryptocurrencies is the backbone that enables cryptos to function. New coins are created as a reward for miners who secure and verify payments in the blockchain where cryptocurrency transactions are recorded.

This has become incredibly capital intensive in recent years, requiring huge amounts of processing power with a corresponding huge electricity bill. So there's ample reward for hackers to use other people's machines to mine coins.

To put this in perspective, Citibank has estimated that bitcoin will eventually consume as much electricity as the whole of Japan. Meanwhile, cryptocurrency analyst Alex de Vries has created an index which shows current bitcoin energy consumption as being equivalent to that of Serbia or almost 10 per cent of UK usage, which means the power used for each transaction could power a home in the United States for a week.

As the price of cryptocurrencies has shot up, so has the use of mining malware. Russian internet security firm Kapersky Lab says it has detected 1.65 million incidents of malware mining so far in 2017 on top of 1.8 million in 2016.

> New coins are created as a reward for miners who secure and verify payments in the blockchain where cryptocurrency transactions are recorded

"Over the last few years we have seen a large increase in availability of complex malware which has fuelled the number of cyber-incidents in general," says Devina Patel, an account executive in the cyber and technology, media and telecommunications division at Willis Towers Watson.

Though the most likely to be attacked, larger firms are also best prepared and there are others who should take note of the threat.

"Companies that should be wary of this risk are the small to mid-sized businesses that have often been targeted with the knowledge their defences won't be state of the art," warns Ms Patel.

The education sector, particularly universities with research facilities that use powerful supercomputers, should be mindful of the risks as they may be unattended during certain times of the year.

That doesn't mean large organisations don't need to increase their vigilance. Both Equifax and Uber have recently announced major breaches and they won't be the only ones. Utilities have considerable computing power, but on ageing systems, while local authorities, hard pressed to cut costs, may have compromised their IT security.

However, even financial services organisations can find mining malware on their systems, says Martijn Verbree, a partner in KPMG's cybersecurity team.

"It is not necessarily on a machine that is directly connected to the internet, but a network server that was used for Christmas party photos from years ago and has been forgotten about," he says.

Disrupting mining malware is not difficult, says Mr Verbree, as it can often be stopped with the use of an ad-blocker. Discovering that you have it is another matter because it's designed to be unobtrusive, so you need to be watching all the time.

"You have to get back to basics and understand what is in your network, what is hanging off your network, and you need to scan these boxes for nasty surprises," he says. Ensuring software is up to date, patches are in place and passwords being used are neither the default nor too simple is half the job done.

The *Cyber Security Breaches Survey 2017* shows that despite security being considered a high priority (93 per cent) among senior management, the government's recommended ten steps for cybersecurity are being applied in a piecemeal fashion.

While 92 per cent of businesses update software when it is available, 90 per cent maintain up-to-date malware protection and 89 per cent maintain firewalls with appropriate protection, only 30 per cent offer training to their staff and 11 per cent have a formal incident plan in place should there be a catastrophic breach.

Access is the name of the game and "whitelisting" sites considered safe, limiting media content and blocking JavaScripts all help to prevent web browser-based attacks, says Ms Patel. In addition to regular updates, companies should monitor computer central processing unit performance for any spikes and start off with a baseline of what "normal" looks like.

"If companies are able, they should be using intrusion detection and prevention systems that look at the number of connections being made, where they are going to and come from, and the amount of bandwidth each connection is using," she says. "This way anomalies can be detected and analysed in much more depth."

Not every business needs 24/7 cyber-watchdogs patrolling their networks. Each business should balance the risk against its resources and determine an appropriate response.

However, employees – the most important element of cybersecurity breaches – are all too often overlooked, and worryingly few businesses focus on user education and awareness of the risks.

"It needs to be ingrained in the workforce that they all play a part in cybersecurity," says Ms Patel. "Employees need to be thinking carefully before clicking on unknown links or allowing any downloads on to their systems."

That needs to include mobile devices and where they are used, she says, yet only 23 per cent of businesses have a policy on mobile working and 22 per cent on what may be stored on removable devices.

Businesses may find their cyber-risk insurance will cover losses, but the insurance industry is keeping an eye on its development.

"We see a lot of breach cases where the hackers are not interested in data, but want access to hardware," says Neil Gurnhill, chief executive of specialist cyber-risk insurer Node International.

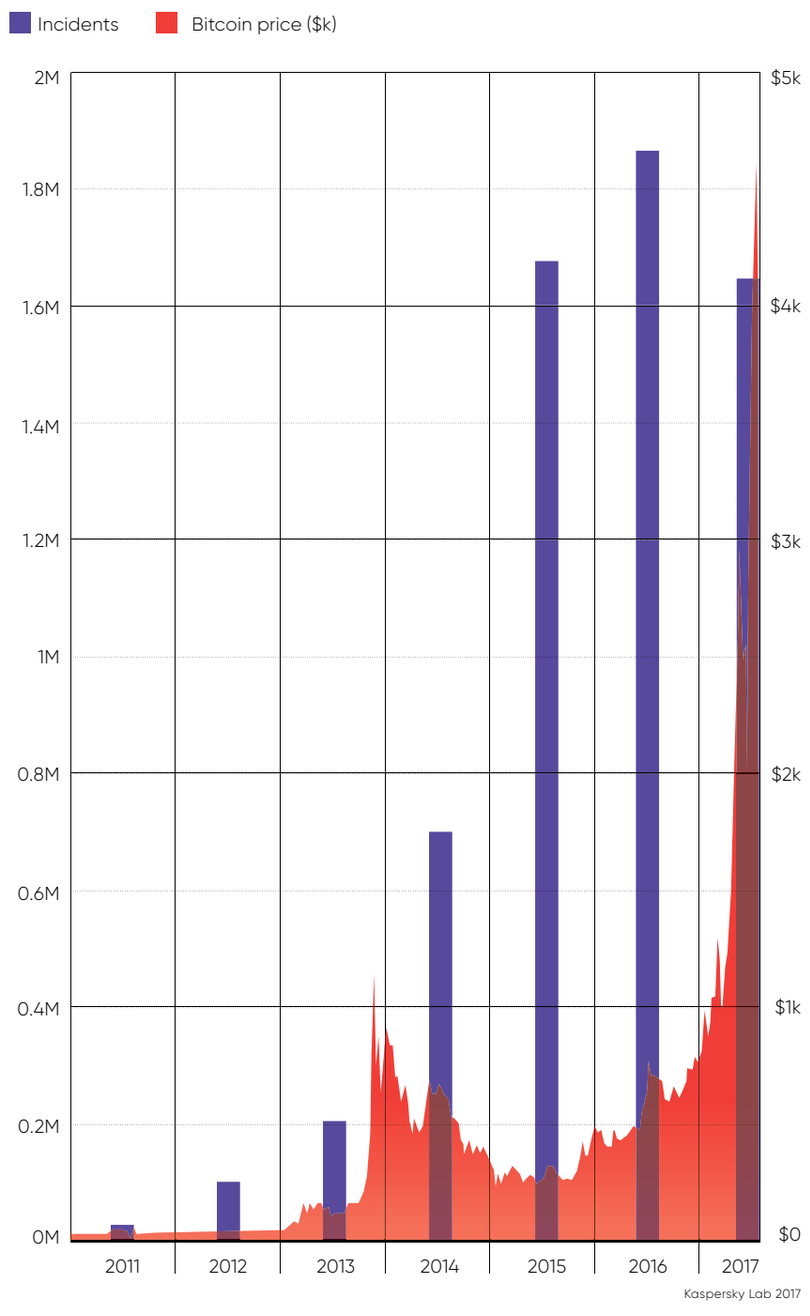
"Like most evolving risks, we don't identify mining malware specifically, but I imagine we will."

The current treatment for mining malware is straightforward for those maintaining basic IT hygiene. However, the growth of cryptocurrencies threatens further development of more sophisticated attacks, which may not bring down the company, but leave a door open for those who would choose to do so.

Businesses must be prepared, and be seen to be prepared, to be mitigating these risks vigorously.

NUMBER OF INCIDENTS OF CRYPTOCURRENCY MINING

ANNUAL DETECTIONS BY KASPERSKY LAB; 2017 FIGURES AS OF SEPTEMBER 12



Kaspersky Lab 2017

DIGITAL IDENTITY

BEST-BACKGROUNDS via Shutterstock

Ghosts in the machine that know who we are

Are we entering a new age of behavioural tracking with the emergence of artificial intelligence and machine-learning, will this offer new levels of personal data security and will our behaviour online become the only password we need?

DAVE HOWELL

A proactive and dynamic response to digital identity security is now critical. Latest figures from fraud prevention organisation Cifas show there has been a sharp rise in identity fraudsters applying for loans, online retail, telecoms and insurance products.

Simon Dukes, chief executive of Cifas, says: "We have seen identity fraud attempts increase year-on-year, now reaching epidemic levels, with identities being stolen at a rate of almost 500 a day."

Proving your identity has always been essential, but none more so than across the digital landscape. It's not surprising that artificial intelligence (AI) and machine-learning are being rapidly developed as an aid to identity authentication.

The risk of chargebacks, botnet attacks or identity theft is leading enterprises to deploy intelligent systems that are not simply looking at publicly available data to identify a person. Earlier this year, for instance, Sift Science announced its Account Takeover Prevention that can detect and block illegitimate login attempts.

The *Cyber Security Breaches Survey 2017* revealed that just under half (46 per cent) of all UK businesses identified at least one cybersecurity breach or attack in the last 12 months. This rises to two thirds among medium-sized firms (66 per cent) and large firms (68 per cent). Protecting the personal data of their customers is now a commercial imperative.

> We have seen identity fraud attempts increase year-on-year, now reaching epidemic levels

Using traditional data, such as name, address, email, date of birth, IP address and biometrics such as voice, fingerprint and iris scan, are being joined by behavioural characteristics that are unique to the individual. This is necessary as much of the traditional personal data is available via public record or can be purchased on the dark web. However, behaviour isn't a tangible piece of data that can be purchased, which makes this form of security highly attractive for enterprises and organisations.

The issue has been analysing the masses of data a consumer's digital footprint could contain. This is the province of AI and machine-learning that can see patterns in the data collected and accurately assign this to an individual as their digital ID. Just checking information on credit agencies, for instance, is no longer robust enough in the face of cybercriminals who can create synthetic personas.

To combat spoofing attacks, AI and machine-learning are being used widely in a variety of security applications. One of the most recent comes from

Onfido that has developed its Facial Check with Video that prompts users to film themselves performing randomised movements. Using machine-learning, the short video is then checked for similarity against the image of a face extracted from the user's identity document.

For all enterprises and organisations, the authorisation of payments is vital. Johan Gerber, executive vice president of security and decision products at Mastercard, explains their approach: "Artificial intelligence and machine-learning are crucial security capabilities to interpret the complexity and scale of data available in today's digitally connected world."

How you behave online will become a critical component of your identity. However, AI and machine-learning systems will need to be sophisticated enough to understand when someone changes their behaviour, without it being malicious. For instance, when you are on holiday, your digital footprint changes. AIs would need access to your travel arrangements to ensure your credit card isn't declined because of anomalous behaviour. These systems are coming from a new breed of security startups, including Checkr, Onfido and Trooly, that understand cyberthreat.

It is also becoming clear that those businesses that use more sophisticated security and identity verification systems lessen their instances of cyberattack. The *Fraud and Risk Report 2017* from Callcredit illustrates this as only 5 per cent of businesses that have been victims of fraud this year have used any sort of behavioural data for fraud insights. Essentially, businesses that aren't getting hit by fraudsters are using more sophisticated techniques.

Last year 63 per cent of cyberattacks involved stolen credentials, according to *Verizon's Data Breach Investigations Report*. "By monitoring to ensure that all systems and data are behaving normally instead, enterprises can allow people to get on with their work and only intervene when someone is trying to access areas they shouldn't," says Piers Wilson, head of product management at Huntsman Security.

The current level of development with AI and machine-learning has already delivered new security systems that are in use today. Mastercard's Decision Intelligence is a good example. However, AI and machine-learning are far from autonomous and still require high levels of supervision. They can clearly search vast quantities of data to respond to a specific question or task, such as authenticating the identity of a shopper. AIs can identify a change in behaviour and highlight an anomaly, but is this behaviour a threat?

Greg Day, vice president and chief security officer at Palo Alto Networks, concludes: "There is a bigger impact that machine-learning will have on the cybersecurity industry and that has to do with the collection and aggregation of threat intelligence. When cybercriminals ply their trade, they leave behind digital breadcrumbs known as 'indicators of compromise'.

"When collected and studied by machines, these can provide tremendous insight into the tools, resources and motivations that these modern criminals have. As such, access to rich threat intelligence data and the ability to 'learn' from that data will ultimately empower organisations to stay one step ahead of cybercrime."

As we all tend to fall into habits, including how we access digital services, our purchasing decisions, what devices we typically use, for how long and from which locations, these behaviours can all be used by AIs to build a profile of an individual.

If this behaviour is deviated from, the AI can easily spot this change of pattern within the data that defines who we all are. This "contextual intelligence" is the basis for rapidly developing security systems that could not function without advanced AI and machine-learning.

AWARENESS OF MACHINE-LEARNING IN CYBERSECURITY

SURVEY OF CYBERSECURITY PROFESSIONALS

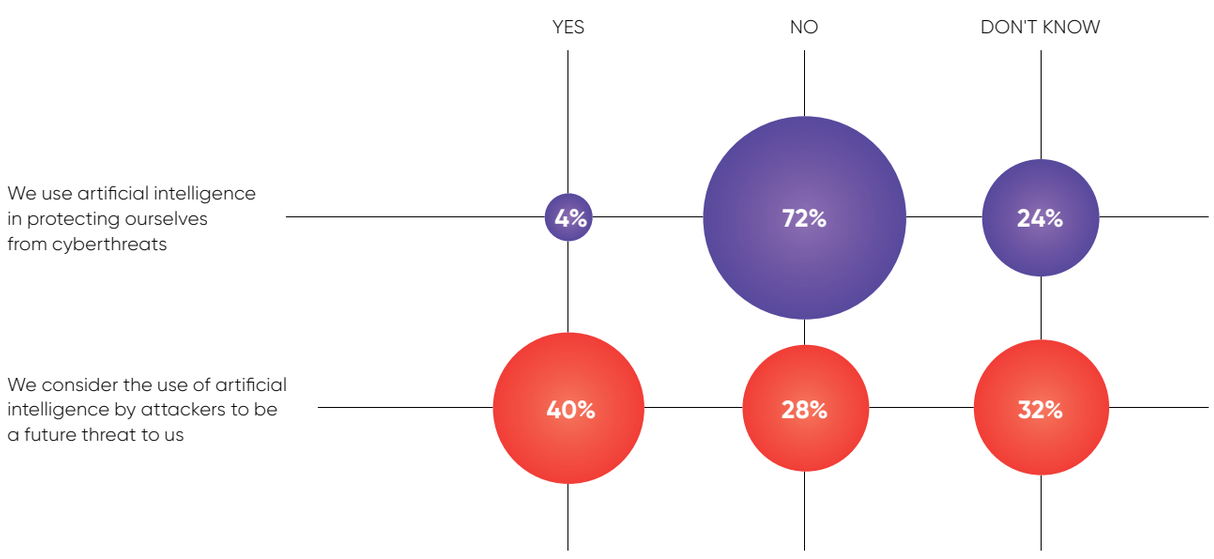
30% claim to be very knowledgeable about machine-learning/artificial intelligence (AI) in relation to cybersecurity analytics and operations

12% have deployed/are planning to deploy machine-learning/AI technologies for cybersecurity analytics and operations

Enterprise Strategy Group 2017

ARTIFICIAL INTELLIGENCE: DEFENCE AND ATTACK

SURVEY OF CYBERSECURITY PROFESSIONALS



KPMG 2017

COMMERCIAL FEATURE

Social media: giving you a head start in a crisis

Social media has transformed the reporting of serious incidents – now companies are using it to get a head start in crisis management

AnotherDay
Dataminr

From terrorist attacks to major cyberbreaches, the world suddenly seems to be more dangerous and unpredictable than it has been in the last half century. These alarming events come against a background of political and economic instability.

On top of concerns about the security of employees, IT systems and supply chains comes pressure from investors, clients and regulators to ensure organisations are ready to act quickly to pre-empt or at least mitigate problems caused by these events.

"We find that organisations often create their own crises," says Jake Hernandez, global consulting director at AnotherDay, a fast-growing strategic security consulting firm that focuses on forethought and prevention to enable its clients to operate as safely as possible. "Either they haven't had the time to do any crisis planning or they've done too much and overcomplicated the process with vast documents and complex, unworkable procedures."

Adding to this challenge is the way in which news of an incident is reported. Social media supports the instantaneous spread of information and has made news dissemination faster than ever before. Whether it's a suspected terror attack, a natural disaster or a data breach, information about an event will travel around the world in seconds thanks to the rapid rise of the citizen reporter.

Quite understandably many organisations have considerable concerns about social media but, as well as simply spreading news about a crisis incident and adding to the threats faced by firms and others, social media often plays a constructive role. Facebook, for instance, recently launched Safety Check which, it says, is a way for members to "connect with friends and loved ones during a crisis, offer or find help for people in the affected area".

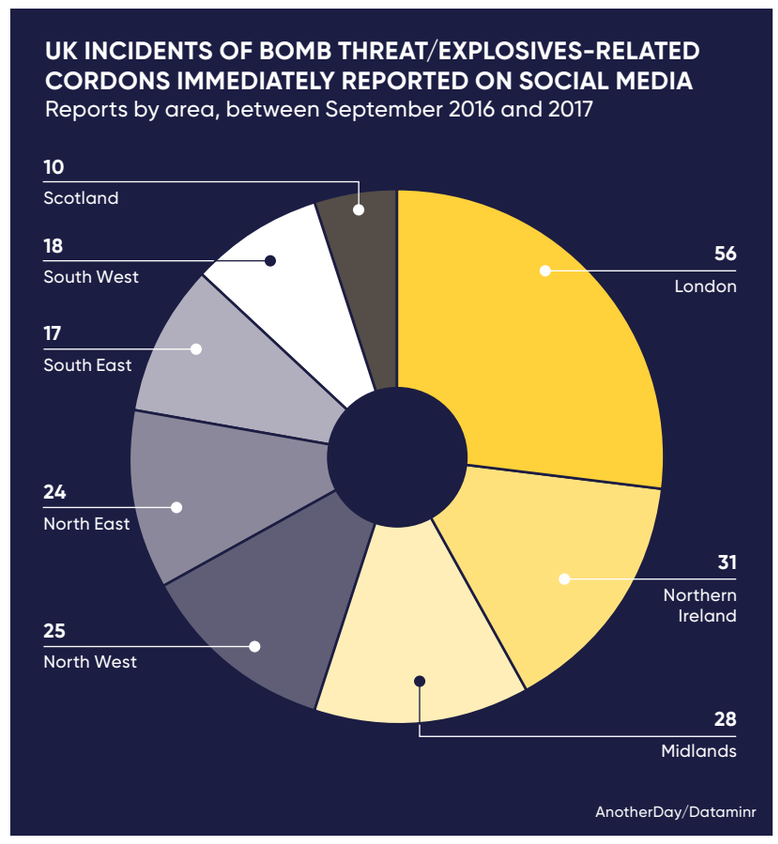
It was to harness the power of publicly available social media, starting with Twitter as the fastest purveyor of news wherever and whenever it might be breaking that Dataminr was founded in 2009.

Dataminr processes all publicly available tweets in real time and detects indications of breaking events. Using proprietary algorithms and machine-learning technology, Dataminr sends clients real-time alerts so security teams can quickly prepare the most effective response to unforeseen incidents.

Corporations depend on Dataminr to help keep their personnel, facilities, operations and interests safe around the world. Political and terror-related risks have always been around, but these days the key is the speed at which they're reported thanks mainly to social media, and the ability of organisations to react with equal alacrity and agility, as they begin to exploit the power of social media as a source of news.

"In this volatile atmosphere, what matters is the speed of the alert," says Tim Willis, director of Europe, Middle East and Africa corporate security at Dataminr. The company was able to inform its customers that last month's Oxford Circus incident, for instance, was not in fact a terrorist incident, before anyone else.

Following its first alert about the event at 4.46pm, by 5.11pm it was sending updates to inform clients that the incident appeared to be contained. As a result, crisis management teams were able to stand down their crisis procedures far earlier than if they had relied solely on traditional sources of information.



> We have the Dataminr app running constantly on our desktops at AnotherDay and our consultants have it on their smartphones wherever they are in the world

AnotherDay uses Dataminr's services to turn the ocean of public data provided into useful, actionable information that its clients can use in their crisis-response procedures.

"We have the Dataminr app running constantly on our desktops at AnotherDay and our consultants have it on their smartphones wherever they are in the world, so we can all receive alerts for terrorist incidents, cyberattacks or other threats," explains Mr Hernandez. "We can then use our understanding of our individual clients' operations to put these alerts into context. We can say to an insurer, for instance, 'This is what has just happened, this is what it means for you and this is what other companies like you have done in similar situations'."

Both Dataminr and AnotherDay are brought in by departments ranging from the communications team, corporate security, human resources and, increasingly, in these days of "just-in-time" delivery, those responsible for supply chain management.

One Dataminr client that transports refrigerated medicines across Turkey was able, following an alert about political instability in the country, to keep drugs in their refrigerated warehouses. Had they been transported, they would have deteriorated when road blocks delayed the lorries, impacting storage conditions and costing hundreds of thousands of pounds.

"Companies are realising that not only can they reduce their risk, but they can gain an advantage over their competitors that aren't managing such risks as well," says Mr Willis.

Not only is it imperative to respond quickly to risk when it arises, but also to plan for it. Mr Hernandez points out: "Organisations are suffering cyberattacks, for instance, all the time. But more and more are realising that they need to be proactive in handling these attacks. We're also seeing more companies address a greater range of risks at the C-suite level. This means that organisations can co-ordinate their efforts and take a more holistic approach. After all, prevention is better than cure."

For more inforamtion please visit
www.another-day.com
www.dataminr.com

WESTMINSTER TERROR ATTACK

On March 22, Khalid Masood, 52, drove a car into pedestrians on London's Westminster Bridge, then stabbed a policeman before being shot and killed near the Palace of Westminster. Within two minutes of this attack, at 2.41pm, Dataminr delivered a flash notification from an eyewitness at the scene to its clients around the globe, including AnotherDay.

"Gun shots outside Parliament now," the alert read. From the rapidly rising volume of tweets, Dataminr issued a second alert at 2.46pm, discovered from a Twitter user based in the Palace of Westminster with more information.

"This was an example of the kind of major incident that firms associate with the word 'crisis'," says Mr Hernandez. "We've normally worked with a client to develop their plans and train their team so that we can say, 'This is what we've planned and trained together for. Now that it's happening and, given how we understand you're likely to be exposed, here's what we think you should do'."

INTERVIEW


Mark Thompson/Getty Images

Felipe Massa of Williams Martini Racing on track during practice for the Abu Dhabi Grand Prix last month

Tech knows behaviour of Williams F1 team in race for chequered flag

Graeme Hackland, chief information officer of Williams Martini Racing, tells how user behaviour intelligence technology is helping to propel the team's Formula 1 car

FINBARR TOESLAND

The explosion in enterprise data, innovative mobility solutions and the move to cloud-based technologies have made safeguarding sensitive material an increasingly difficult task. Long gone are the days of the traditional security perimeter, where firewalls and intrusion detection systems were the key consideration for chief information officers (CIOs). These changes have expanded the scope of insider threats and turned many IT executives to user behaviour intelligence solutions to deal with one of the most complex challenges of enterprise security.

The importance of giving employees wide-ranging access to confidential data, while also ensuring they do not misuse it, cannot be overstated at Williams Martini Racing, a leading Formula 1 team. "Formula 1 is a known quantity for us; we have a new car every year and the data after three to four years is not that valuable anymore, but at Williams we also have our advanced engineering company," says the team's CIO Graeme Hackland.

"The projects that we're working on in advanced engineering and in electric vehicle technology, selling our expertise into some of the biggest OEMs [manufacturers], is where we're at the cutting edge. It's really valuable intellectual property from our perspective."

But it's also vital to ensure staff are not slowed down and are able to access the data they need, when they want it. "There are a number of people at Williams who have jobs that require them to copy and move around all types of data," says Mr Hackland. "For example, members of our marketing team will be using videos and photos from every race they are able to, which becomes their normal behaviour. If they suddenly copied a whole load of aerodynamics data that would raise a red flag," he says.

Soon after Mr Hackland joined Williams in 2014, the team partnered with user behaviour intelligence provider Dtex Systems to get a better grasp on intellectual property (IP) protection and immediately discovered two instances of data misuse, which they were able to address very quickly.

"After we sorted the initial issues out and fully deployed the tool across all Williams' machines, we informed our staff at a town hall meeting about this new capability and why we needed it," says Mr Hackland.

A total of 11 investigations have been completed around the misuse of data, with the information collected from these cases shared with every new Williams staff member to give them insight into the threats the team are facing and underline the importance of data protection.

"We spent a lot of time talking to staff and making sure they understand the implications if they breach policies, as we really don't want our people to do something to contravene our policies and then run the risk of losing them," he says.

Mr Hackland explains that most of the incidents discovered by user behaviour intelligence technology at Williams have been inadvertent. "There are times we have found people taking data outside their normal role, but they had a reason. They wanted to do something specific without understanding the risks they were putting themselves and the company at," he says.

It's not just their own proprietary data that Williams have to secure, as the business works with some of their customers' IP and also jointly develops IP. "We have a number of different challenges compared to a regular F1 team that might just have this year's and next year's F1 car data to protect. Part of our company is also listed on the Frankfurt Stock Exchange, so we have some reporting responsibilities that most, if not all, the other F1 teams don't have," he says.

User behaviour intelligence technologies work best when human expertise plays a key part in discovering insider threats, according to Mr Hackland, with Williams having established a baseline of normal user behaviour so the technology isn't returning false positives.

"We translated our policies to the user behaviour technology to categorise what is sensitive information for us and are only alerted when that is moved about. Context is added, asking questions such as 'was that data confidential?' This has all been fully defined," he adds.

> The Williams CIO is keen to ensure a balance is struck between security and allowing creativity in the team

Company culture is an important concern when trying to combat insider threats. Williams is a family business, with founder Sir Frank Williams leading the team as principal and his daughter, Claire Williams, supporting as deputy team principal. When Mr Hackland looked at user behaviour and the potential internal user threat, he came from a position of "trust but verify".

"It's the Williams team and there is a culture you have to take into account. We wouldn't be comfortable putting in intrusive technology that either stops people from doing their job or makes people feel like there's someone constantly sitting monitoring what they do," he says.

Williams is pushing forward with pioneering technologies, as many races often see winners and losers separated by split-seconds, and even a small competitive advantage can mean the difference between success and failure. From internet of things-enabled batteries that can transmit data about their level of charge and current state, to biometric data collected from the pit crew, all manner of artificial intelligence solutions are being applied at the 40-year-old team.

Although these initiatives may bring benefits to Williams, they also create new avenues for insider threats. "We've going to have to protect all this new data and make sure it can't be tampered with, especially as we're looking at how machine-learning and automation can be used in race engineering. For example, could we automate some of the decision-making that happens at the track or call a pit stop without human intervention. This can only be done if we're confident that the data is accurate and hasn't been tampered with at all," says Mr Hackland.

The F1 car has been a connected device since 1979 and the risks around insider threats are only set to grow as more advanced technologies are brought on to the racecourse, but the Williams CIO is keen to ensure a balance is struck between security and allowing creativity in the team.

"The idea of controlling everything a company does using IT is just not possible for CIOs anymore. I don't want to be the bottleneck that's holding up innovation in any part of my organisation. I'm here to help with the projects IT is best suited to, in everything from change management to risk analysis and reliability," he concludes.


Williams

Graeme Hackland

COMMERCIAL FEATURE

Turning cybersecurity inside out

A user behavioural intelligence system can protect an organisation from its biggest security threat – the unwitting activities of staff

Enterprises are boosting their spending on the latest security solutions to protect themselves and their customers from data breaches. Spending on cybersecurity is expected to top $1 trillion from 2017 to 2021, according to the *Cybersecurity Market Report*.

Yet companies still face crippling data losses as sensitive information leaks out of their systems or is stolen by hackers.

It would be easy to assume that cyberattacks are highly sophisticated operations targeting the perimeter of these organisations. But most of these breaches occur through the simplest of paths – a vulnerable employee. According to the *2015 Verizon Data Breach Investigation Report*, people are the root cause in 90 per cent of security incidents that result in data breaches.

This may be down to negligence where a member of staff has fallen for a phishing attack, opened a dodgy attachment or clicked on an infected file.

More worrying are malicious cases, where staff actively try to steal information from their companies. Staff may also fall foul of credentials thieves, bad actors either inside or outside the organisation trying to steal their identity. This allows data thieves to break into a network to steal information or intellectual property, or carry out acts of fraud in someone else's name.

Most data security products focus on protecting the perimeter and keeping intruders out, but pay little attention to insider risks.

By using a system known as "user behavioural intelligence", organisations can track the computer activities of their staff and use machine-learning algorithms to predict when they are likely to commit a data breach, innocently or intentionally. The system works by analysing the typical behaviour of users and looking for unusual activities or abnormal practices. The system predicts whether an abnormal activity is likely to lead to a data breach and informs the organisation.

If a user starts accessing a file or area of the network in contravention of the user policy, maybe at an unusually late hour or in a way is out of character for their natural behaviour, this will be quickly identified by the system. The organisation determines a scoring system for abnormal acts with the user behavioural intelligence provider and each unusual activity is scored as it happens. When the behaviour reaches a certain threshold, the system alerts the organisation that a potential data breach is likely. Remedial action can then be taken.

> The system acts as an early-warning system for breaches, identifying when an individual is behaving out of character in a way which could potentially lead to a data loss

The system acts as an early-warning system for breaches, identifying when an individual is behaving out of character in a way which could potentially lead to a data loss. This is an effective way of keeping track of the activities of individual members of staff without compromising their privacy.

Dtex, a Silicon Valley-based company which is growing fast in the UK, has developed a sophisticated user behavioural intelligence system. It is lightweight for the user and effective for the organisation.

"One of the most significant enterprise security challenges is getting the visibility needed to defend against the wide range of insider threats, says Mark Coates, vice president, Europe, the Middle East and Africa, at Dtex Systems. "Our top priority at Dtex is helping enterprises eliminate insider threats by delivering real-time visibility and intelligence with an approach that is agile, scalable and seamlessly integrates with today's modern security environments."

The Dtex system uses a library of thousands of bad behaviours that enables it to create a baseline of what is acceptable digital behaviour to identify suspicious activities quickly.

Dtex works with the Williams Formula 1 team. This is an organisation that needs carefully to guard its core intellectual property, the design of its car, as well as data shared with their technology partners. The challenge is that this is a very transient industry employing a revolving door of highly paid designers, developers and engineers.

The cybersecurity system needs to keep all the data inside the organisation, as well as stopping users from bringing outside information into their network. The last thing a Formula 1 team wants is for an employee to bring intellectual property into the network from another team as this could open them up to massive liabilities. Using the Dtex system, such dangers are forestalled and any potentially dangerous digital behaviour is quickly identified and prevented.

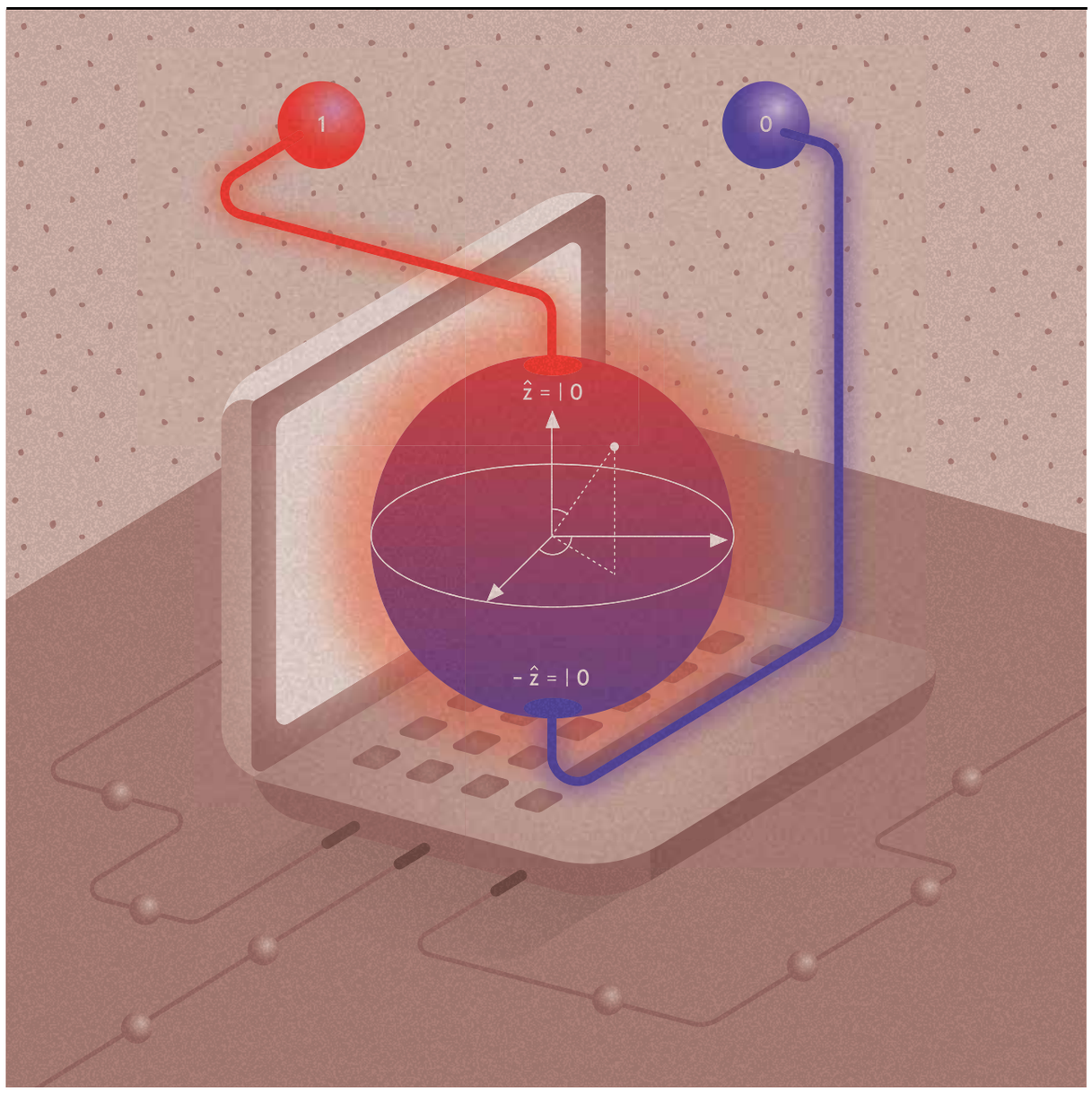
User behavioural intelligence is evolving fast. The systems are increasing their contextual analysis and understanding of users' intentions. Increasingly sophisticated machine-learning capabilities are allowing organisations to strike a better balance between privacy, productivity and their security.

The new generation of cybersecurity systems needs agile, lightweight tools. They must become increasingly accurate and focus on finding the right data rather than simply more data. They need to analyse staff both on and off the corporate network effectively, and they must be compliant with new privacy laws and the imminent European Union General Data Protection Regulation.

Dtex is developing fast and embedding new capabilities into its system. This offers organisations a rapid, agile and lightweight method of protecting data from the biggest threat – the unwitting activities of their own staff.

For more information please visit dtexsystems.com

QUANTUM COMPUTING



Five ways quantum computing will change cybersecurity forever

A new generation of quantum computing has the potential to transform cybersecurity. Still years away from the mainstream, quantum power is nevertheless a reality, a certainty and an inevitability

ADRIAN BRIDGWATER

Traditional old-fashioned digital computers run on data that is encoded according to the binary system. In binary, the state of any single bit can only be 0 or 1. The options are quite literally binary. Any single computing bit can only reside in one of two positions. Now emerging as the next generation of computing, quantum computers run on data that comes in the shape of qubits or quantum bits.

Quantum goes beyond binary by virtue of a qubit's ability to reside in more than one of two positions. A qubit can represent a quantum state made up of two or more values simultaneously, called a superposition. A qubit's superposition can also be differentiated depending upon the context in which it is viewed, so in basic terms we get more computing power in the same space.

But quantum states are fragile and quantum errors are notoriously difficult to measure, so we need to treat this new power with respect. How then could this new thrust of computing strength give us new tiers of power to analyse IT systems at a more granular level for security vulnerabilities and protect us through more complex layers of quantum cryptography?

1 SPEED

Quantum computing is a game-changing technology for cybersecurity due to the inherent speed boost it offers to solve complex mathematical problems. Vice president of security research at Trend Micro Rik Ferguson explains that traditional computing, when compared with quantum, is effectively "brute-forcing" mathematical problems until it arrives at a solution, thus the more complex the question, the slower the answer arrives.

"Traditional cryptography relies on the fact that factoring large prime numbers is mathematically complex and hackers attempting to brute-force an answer need a long time. For quantum computers, this kind of factorisation is where they excel, potentially reducing the time to solve problems from billions of years to a matter of seconds. We can now use that power to build more complex protection layers," says Mr Ferguson.

But could quantum computing also arm the hackers? "Obviously yes," he says. "What we need to remember is that the majority of attacks in today's threat landscape target the user in one way or another and social engineering plays as large a part, if not larger, than technical expertise. As long as a human can be persuaded to part with a secret in inappropriate circumstances, all the cryptography in the world will not help, quantum or not."

2 SECURITY

Perhaps the most compelling near-term impact of quantum is the role of security "distribution functions" that use quantum effects, providing us with a powerful mechanism for sharing cryptographic keys between remote parties with a high degree of implicit security.

According to IBM computer scientist Leigh Chase, we should also look more generally at the types of data transformation operations we can perform in quantum computers to exploit effects that are not present in the classical world of IT. Effects such as superposition and entanglement offer information-processing benefits, many of which can be meaningfully applied to cryptography, such as improved random number generation.

But while we attempt to build phrases like superposition entanglement randomness into the layperson's understanding of technology, do we throw out all our existing cryptosystems in favour of quantum now? IBM's position, for now, is that we should consider quantum-safe cryptography, only some of which requires or exploit quantum effects.

3 RESPONSIBILITY

Although the money is more generally on quantum power keeping us safer, we should constantly remind ourselves that the responsibility for safe use is by no means guaranteed. Senior threat analyst at FireEye Parnian Najafi agrees that quantum computers running what is known as Shor's algorithm pose some risks to current cryptography.

"Some encryption algorithms are thought to be unbreakable, except by brute-force attacks. Although brute-force attacks may be hard for classical computers, they would be easy for quantum computers making them susceptible to such attacks," says Ms Najafi.

But he agrees it is unlikely that hacktivists and cybercriminals could afford quantum computers in the foreseeable future. However, nation states do have the ability to afford and run them. "Current quantum computers require near absolute zero temperature to be isolated from interference like radio waves and noise, so qubits keep their quantum mechanical state. All these requirements make it difficult and expensive for non-nation state actors," she says.

4 SAFETY

So is a quantum apocalypse on the horizon and will cryptocurrencies be a key target? As a security company FireEye's research highlights there are several efforts currently underway to make cryptocurrency more secure, including the quantum-resistant ledger. It would appear then that as fast as we are building quantum power, we are also working to secure against its misuse.

Security strategist at Symantec Ramses Gallego agrees. He points out that a machine which could effectively and efficiently run Shor's algorithm – the most complex quantum algorithm known – could enable us to factorise large prime numbers and do things we cannot even imagine today.

"Such great computing power, however, will present a huge challenge for cryptography in the future as cybercriminals will be able to target organisations with highly complex quantum attacks. To pre-empt this, security specialists are currently developing quantum-resistant algorithms, but we are yet to see how quantum computing will really revolutionise cryptography in the future."

5 RESISTANCE

Human vulnerabilities notwithstanding, could we really use quantum computing to build an unbreakable computer truly resistant to hacking? Director of product strategy at Gemalto Joe Pindar is upbeat.

"What is special about random numbers from quantum computing, and why their early prototypes are being used by Swiss banks and governments, is they can be used to create a 'one time pad'. This is a special kind of encryption key that is essentially unbreakable. Interestingly, one time pads were first used in World War One and are made exceptionally secure by being used only once, for a single message, so codebreaking techniques simply don't work," he says.

Mr Pindar offers some reassurance on the potential misuse of quantum computing. He says that while it will change most of the encryption algorithms commonly used on the internet, it is not true that quantum will break all encryption. "The encryption systems that are used to secure data stored in database records and archives, such as legal documents, use a different technique which quantum computing has been unable to break, so far," he adds.

COMMERCIAL FEATURE

Buckle up for a bumpy 2018 as cyber-extortion hits new highs

What a 12 months we've had. The threat landscape has evolved again and again during 2017 to net cybercriminals billions and cause chaos, destruction and political turmoil in the process

Many IT and business leaders will be keen to know where the next big threat will come from in 2018, but unfortunately cybersecurity is not an exact science. What we can say, though, is that we've certainly not seen the last of digital extortion, business email compromise (BEC) and cyber-propaganda campaigns.

With cybercrime happening on an industrial scale, we must find innovative ways to combat an increasingly agile and resourceful enemy.

YEAR OF RANSOMWARE

Just how big is the scale of the cybersecurity challenge facing us? In the first half of 2017 alone, Trend Micro blocked more than 38 billion threats, including 82 million ransomware attacks. As predicted, ransomware was adapted in 2017 for maximum impact. We saw the result of these efforts in the catastrophic WannaCry and NotPetya campaigns, which caused firms such as global shipper Maersk, FedEx subsidiary TNT and Nurofen-maker Reckitt Benckiser hundreds of millions in losses.

WannaCry, in particular, caused chaos in the NHS, with an estimated 19,000 operations and appointments cancelled. Those behind NotPetya, meanwhile, showed an even more sophisticated approach, using ransomware to disguise what was in reality an attempt to destroy the systems of its initial Ukrainian targets.

The bad news is that the ransomware-as-a-service or RaaS model will continue to drive the growth of this cybercrime sector in 2018, enabling even non-technical hackers to generate profits by exploiting poorly secured organisations.

DIGITAL EXTORTION DEEPENS

However, online extortion will get even more insidious over the coming year as the bad guys go straight for the money. The old model of launching information-stealing malware to compromise customer personally identifiable information is still favoured, but it can leave cybercriminals hanging for months or even as long as a year before they can finally monetise their efforts. Even then, many may find that their return on investment (RoI) from such campaigns is disappointing. Contacting the victim organisation directly to extort funds is far quicker and arguably more likely to result in success.

Thus we'll see the hackers increasingly targeting those more likely to pay up, such as industrial operations run by utilities providers, where any ransomware-related outages could have a major impact on the populace. We may even see cybercriminals using the threat of General Data Protection Regulation fines to extort companies, potentially by stealing their customer data and then offering to delete it if a ransom is paid, as Uber did. Organisations should be aware that the headline fine of 4 per cent of global annual turnover or £17 million is not automatic and will only be levied in extreme circumstances if little effort has been made to secure systems.

However, by the same token, if attackers find a particularly poorly secured organisation, their extortion may well work. Some cursory intelligence gathering to establish the annual revenue of the company, and therefore how much in GDPR fines it may be facing, could further help them to tweak their ransom price.

38bn threats blocked by Trend Micro alone, which included...

82m ransomware attacks

$9bn estimated losses in 2018 in BEC scams

19k operations and appointments cancelled in the WannaCry attack in the NHS this year

$400k for a 12-month campaign to manipulate an election though fake news

BUGS ARE EVERYWHERE

Something else we learnt from the past year is that software vulnerabilities are increasingly the weakest link in the corporate security chain. Even flaws which had been patched by the manufacturer ended up being exploited to devastating effect months later. Just consider the Windows SMB vulnerability, which Microsoft issued a fix for in March, but enabled WannaCry to spread to hundreds of thousands of users around the globe within hours. Cybercriminals will see the impact these exploits had and will try their luck with many more known vulnerabilities in 2018, hoping that organisations will have failed to implement best-practice security.

> We'll see the hackers increasingly targeting those more likely to pay up, such as industrial operations run by utilities providers

A comprehensive patch management programme is essential to ensure all systems are protected as soon as an update is made available. Things get trickier in critical infrastructure where IT managers may not be able to patch because of legacy systems or else don't want to risk the downtime associated with testing. That's where virtual patching can come in handy, protecting systems until they're ready to be patched properly. Machine-learning can also help organisations spot threats early on, with more accuracy than traditional solutions.

EMAIL SCAMS HIT HOME

It's also fair to say that 2017 was the year of BEC scams and 2018 is likely to see total global losses hit a staggering $9 billion. It's proof again of cybercriminals going straight for the jugular with direct tactics designed to net them the biggest RoI possible. Many BEC attacks are made even harder for traditional security filters to spot because they typically don't involve the use of malware. Instead, a chief executive's email address is forged and a member of the finance team targeted with classic social engineering in a bid to trick them into transferring large sums of money outside the company.

Part of the answer lies in raising awareness among staff of such scams. Employees are your other major weak link in corporate security, so all staff including temps should be trained in a continuous year-round programme. Try to move away from theory and technical jargon, and towards exercises using real-world situations and everyday language.

POWER OF MACHINE-LEARNING

Machine-learning once again can be useful in helping to prevent BEC. Think of it as a kind of forerunner to full artificial intelligence. Its value lies in being able to analyse huge amounts of data to find the needle in the haystack that might indicate a major threat. But to be successful, any machine-learning-based security tool must be properly trained. You need good quality data, and lots of it, to help the system establish a baseline of "normal" behaviour so it can flag with a high degree of accuracy when something doesn't look right. That could be anything from a BEC email scam or a vulnerability exploit in a ransomware-laden email.

High-fidelity machine-learning should be a key component of your layered security response in 2018.

But be warned, while the white hats are increasingly promoting machine-learning as a way to combat advanced threats, the cybercrime community may also be tapping publicly available tools to find security gaps and zero-day exploits.

GET REAL ABOUT FAKE NEWS

As we've discussed, the success of staff security awareness programmes will have a major bearing on the threat landscape in 2018. But we also need to think about educating society as a whole, not just on cybersecurity, but on spotting fake news and cyber-propaganda. Earlier this year we uncovered for the first time the sheer size of this underground market, where a 12-month campaign to manipulate an election can cost as little as $400,000 (£315,000).

In many ways, the impact of fake news is the one cyber-related threat that really does have the potential to cause the most damage to our society and way of life. So as we go into 2018, with key mid-term elections coming up in the United States, it's never been more important to think before you click.

For more information please visit www.trendmicro.com

CYBERCRIMINAL ECONOMY

How organised is organised cybercrime?

Make no mistake, cybercrime is big business and run like an industry with levels of deceit shielding the masterminds from capture

DAVEY WINDER

Law enforcement, security vendors and white hat hackers all collaborate in the fight against cybercrime. It would be naive to imagine that cybercriminals are not meeting this challenge in kind. Yet far too many organisations seem to think that the dark side of the internet is still inhabited by teenagers in hoodies looking to make some beer money.

The truth is that your average cyberattacker will be part of an organisation that is far closer to a corporate enterprise in its structure. "Cybercrime units possess roles that we typically come across in any large legitimate business such as partner networks, associates, resellers and vendors," says Kevin Curran, professor of cybersecurity at Ulster University, "and they even have dedicated call centres which are typically used to help with requests from ransomware victims."

So who are the successful threat actors and how do these criminal groups organise themselves? The youths in hoodies certainly do exist but, as new entrants in the cybercrime fraternity, are usually "only capable of leveraging low-level hacking tools", says Travis Farral, director of security strategy at Anomali. "But they may eventually be writing their own tools or enhancing the capabilities of existing tools," he says.

Almost inevitably, as they mature they become part of sophisticated cybercrime groups. Interestingly though, Jim Walter who is senior research scientist at Cylance, says the more sophisticated a crime group is then the more isolated it becomes. "That's true for government or nation state-sponsored operations and criminal groups as well as those that straddle either side. Whereas mid-tier operations have more visible partners and will use any enabling resource you can imagine," he says.

These will include much the same open source and commercial tools that legitimate organisations rely on to do business. "Criminals will use common tools like WhatsApp, Slack and Google Groups to conduct their business in real time; tools that are available on both the regular internet and the onion-routed networks commonly referred to as the dark net," says Chris Day, chief cybersecurity officer at Cyxtera.

But Ed Williams, senior threat intelligence consultant at Context Information Security, doesn't believe it's always such a dark world. "Brazilian cybercriminals, trailblazers when it comes to financial cybercrime, are renowned for communicating and marketing their wares on social media," he says.

> They even have dedicated call centres which are typically used to help with requests from ransomware victims

HOW AN ORGANISED CRIMINAL GROUP IS SET UP

TEAM LEADER	Responsible for overall missions and communication with workers
CODER	Malware developers who focus on writing software which infects systems, spreads automatically and evades detection
NETWORK ADMINISTRATOR	Manages a large number of compromised systems used to spread malicious payloads, such as viruses, spam and denial-of-service attack packets
INTRUSION SPECIALIST	These concentrate on making sure any successfully installed malware persists allowing continuing compromise
DATA MINERS	Needed to make sense of the stolen data by organising and reformatting for ease of sale; here they make use of crowdsourcing
MONEY SPECIALIST	These identify ideal ways to make money from all their datasets

National Cyber Security Centre 2017

Morgan Gerhart, vice president at Imperva, argues that cryptocurrencies and dark webs have between them added liquidity to the broader cybercrime industry, and dramatically reduced transaction costs and counterparty risk. "With those market enablers in place," Mr Gerhart insists, "cybercriminals are able to leverage automation to drive down the unit cost of launching an attack."

51%

of data breaches analysed were perpetrated by organised criminal groups

Data Breach Investigations Report, Verizon 2017

Also driving down the cost are specialisation and compartmentalisation in the cybercriminal underworld. Tim Brown, vice president of security architecture at SolarWinds MSP, says there's a focus on "specific services and making sure that these work exactly as advertised".

Hardik Modi, senior director of the security engineering and response team at Arbor Networks, agrees. "Each of these components are routinely upgraded and customised for use in new campaigns, pointing to dedicated and separate teams of competent programmers," he says. Indeed, the cybercrime industry has become so robust that an attacker can hire out work for each link in the attack chain at an affordable rate. Each link remains anonymous to other threat actors in the chain, reducing their risk of being found out if one link gets busted.

"One group might develop the delivery system of an attack, switching out exploits when they're no longer viable," explains Marina Kidron, leader of the Skybox security research lab. "Another might handle the malicious payload that infects the machine and money collection outsourced to a mule."

And this last service might just be the Achilles' heel of cybercrime gangs. Ian Trump, chief technology officer at Octopi Research Lab, argues that "stolen money and fraudulent purchases have to be laundered" and, no matter how sophisticated the malware might be, "making money from cybercrime requires this service layer".

> Cybercriminals are able to leverage automation to drive down the unit cost of launching an attack

Indeed, the risk in the mule operation can be seen in the success of law enforcement across 26 countries during European Money Mule Action in November. According to Europol, in just one week a total of 766 mules were identified, 409 interviewed and 159 arrests made. Importantly, this operation also resulted in 59 mule recruiters being identified, useful information when profiling cybercrime organisations.

Law enforcement operations have also had considerable success in disrupting dark-web marketplaces of late. Earlier this year, both AlphaBay and Hansa Market were taken down, representing two of the biggest players in this underground cybercrime economy. Investigators had effectively been running the latter for at least a month and used it to collect information on criminals flocking to it after the former was shut down. Quite apart from anything else, this kind of disruption introduces an increased uncertainty of who cybercriminals can trust.