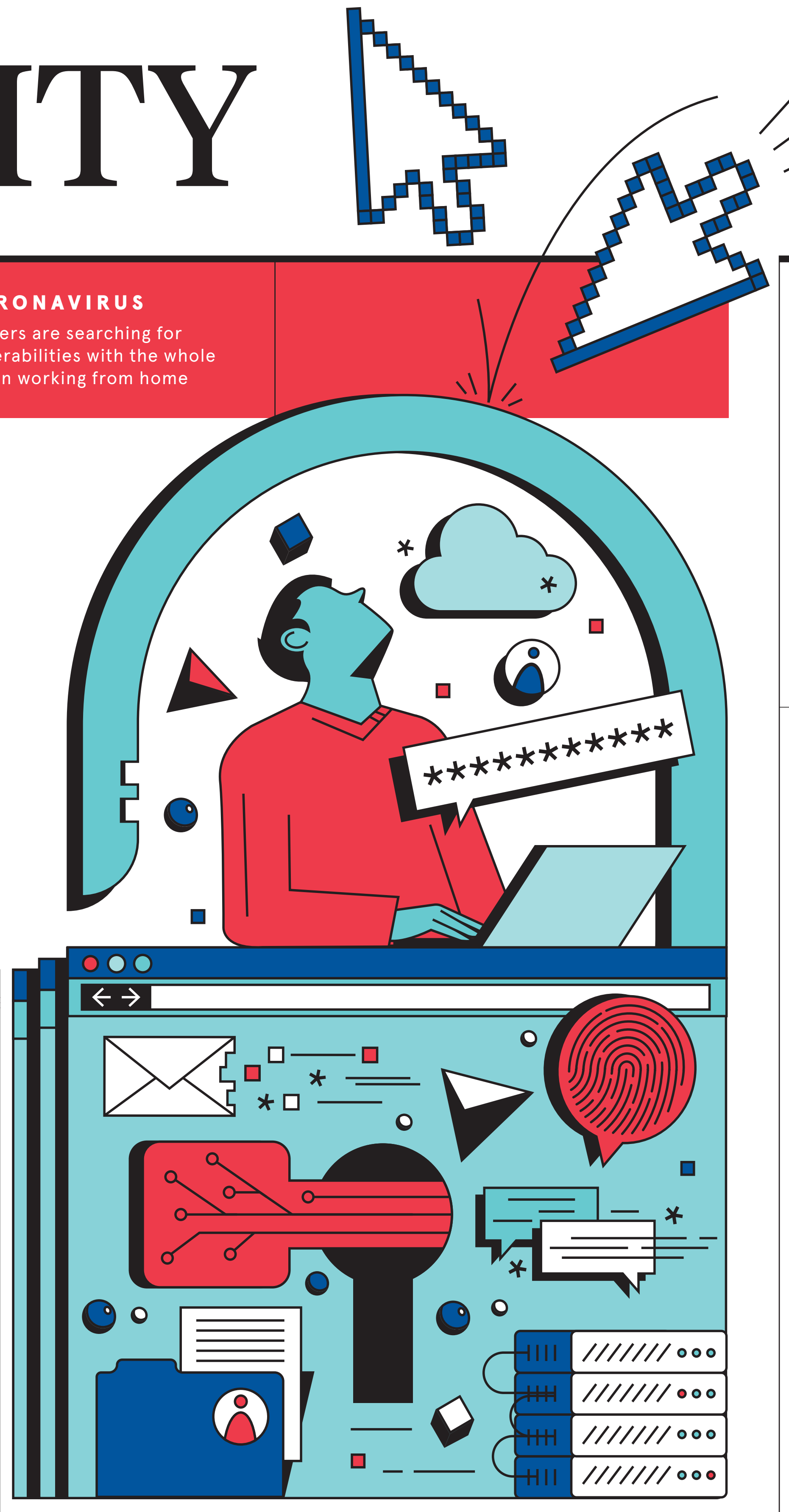
INDEPENDENT PUBLICATION BY

RACONTEUR

RACONTEUR.NET | #0656 | 22/03/2020

CYBERSECURITY



SECURITY BY DESIGN

Providing protection from the ground up

With reactive approaches to cyberthreats proving futile in preventing data breaches, companies are embedding design principles into the core of their systems and processes to give them the protection they require

Davey Winder

Digital transformation and connectivity have provided unprecedented opportunities for businesses and revolutionised industries as a result. But this has come at a price as organisations have now been opened up to a growing array of cyberthreats.

Companies are under near-constant attack and a traditionally reactive, sticking-plaster approach to dealing with the online assault has proved ineffective, making cybersecurity by design a growing and crucial feature of any organisational structure.

Introduction of the General Data Protection Regulation in 2018 has forced organisations to take a more proactive approach to cybersecurity. Previously, only strongly regulated companies in sectors such as insurance and banking were required to take strict measures to protect customer data. Now, facing hefty fines for non-compliance, companies in all industries are prioritising investment in cybersecurity.

However, there is still a long way to go. Most small companies are unable to hire security specialists because of the added cost and enterprise-level businesses are often hindered by legacy systems. The result is many organisations are unprepared for current cybersecurity threats and unable to take a proactive approach to protecting their business.

Cybersecurity-by-design frameworks advocate embedding a proactive stance against threats into business processes. The security team is involved in all development processes and use their expertise to review and provide advice on cybersecurity best practice before anything is rolled out. Implementing a security-savvy design process into all product development and implementation protects an organisation from the inside out.

> “It is only through an organisation-wide security culture and early involvement that risks can be successfully identified

“Security teams need to think of the worst possible situation and then work backwards to implement a cybersecurity-by-design process and measures that will either stop threats or reduce the damage,” says Dominik Malowiecki, chief information security officer (CISO) at smart home insurance provider Neos.

“Teams need to approach this from the perspective of an outsider and check all possible entries to customer data. Cybersecurity should always be an ongoing process.”

Introducing a cybersecurity-by-design framework means security becomes a proactive, end-to-end strategy and spans across the entire organisation and supply chain. Solutions are always tailored to the business, rather than a one-size-fits-all model.

Cybersecurity is a fundamental business practice that affects people, processes and technology, and a core principle of implementing design processes is integrating security at the beginning of the product development life cycle rather than just as a feature of a product. This enables organisations to model and fortify the ongoing cybersecurity posture and build resilience against threats and risks that are also continually evolving.

“This is an approach that should be adopted by all,” says Inga Schorno, head of information security at Tandem Bank. “As a bank built on open banking, we are a data-driven business and understand the benefits of efficiency and productivity, but acknowledge this must be balanced by identifying digital risks. It is only through an organisation-wide security culture and early involvement that those risks can be successfully identified and mitigated.

“Incorporating cybersecurity-by-design principles will help to adapt to the changing threat landscape by involving information security and risk teams at early stages of development. Failing to see it that way can leave you vulnerable to unexpected threats with a rigid framework unsuitable for fast response. Organisations must cultivate a wider cyber-resilient culture with ongoing training and adoption of the security framework.”

It is crucial that senior management are involved in the cybersecurity design process. This typically begins with due diligence whereby each company’s CISO or chief information officer is involved in agreeing the protection, access and permitted sharing of data. People are often the weakest link in security so it is important to ensure all employees are well trained on aspects such as cybersecurity best practice. System designers and developers should also be involved at the very least in the planning and implementing stages.

Before adopting any systems, design principles require the business to identify what they are for, what’s needed to operate them and what risks are acceptable, while ensuring there is no ambiguity about responsibilities. Organisations must make any compromise difficult by reducing the attack surface, designing for easy maintenance and making it easy for users to do the right thing. They should make disruption difficult by designing for scalability, identifying bottlenecks and testing for high load and denial-of-service conditions.

“Any compromises should be easier to detect through collecting all relevant security events and logs, making it difficult for attackers to detect security rules through external testing,” says Kevin Curran, senior member of the IEEE (Institute of Electrical and Electronics Engineers) and professor of cybersecurity at Ulster University. “Organisations should also remove unnecessary functionality, especially where unauthorised use would be damaging, anonymising data when it’s exported to reporting tools and avoiding unnecessary caches of data.”

As a company that specialises in digital due diligence, security is very important to Neotas and its clients. As such, a decision was made early on to keep everything in-house with a heavy emphasis on data encryption, Microsoft SharePoint and information resources management.

A cybersecurity-by-design framework has been key to achieving this. Neotas shares thousands of links around structures and has many restrictions on its libraries, so it requires a reactive security approach with an ability to see who has access to what and why.

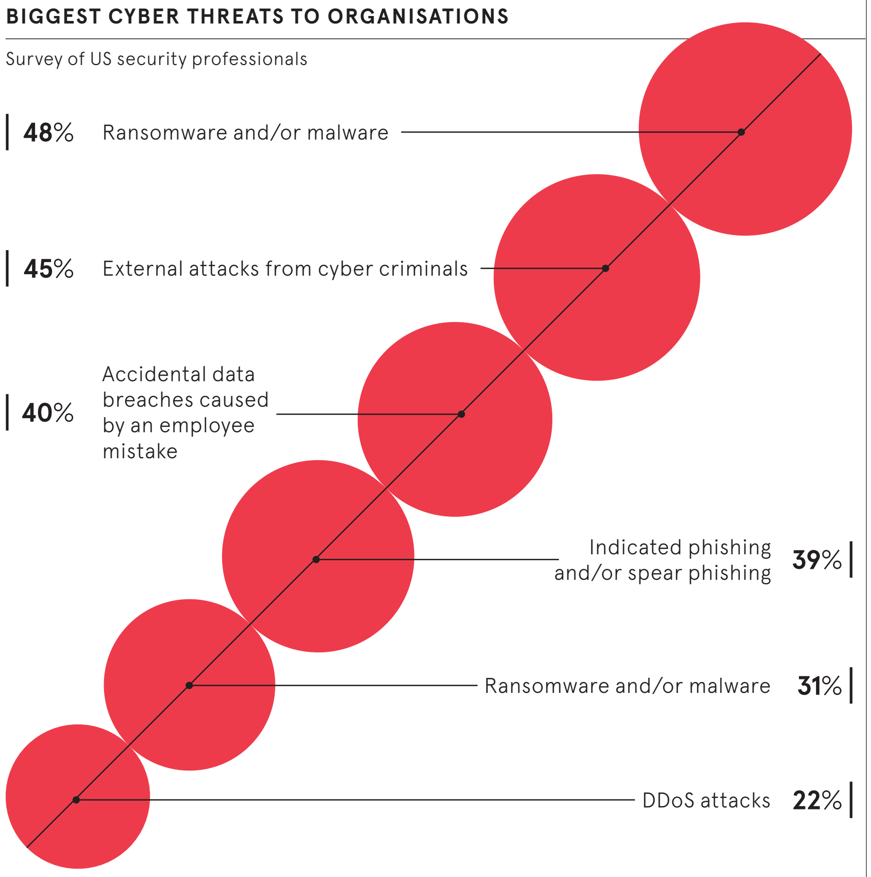
As part of ISO 27001 accreditation, Neotas needed a robust system to complement its cybersecurity-by-design framework and help mitigate risks. A system from Torsion provides peace of mind by enabling quick changes throughout its architecture and solving the problem of limited control or visibility over data access, which often leads to security and compliance issues.

“The reaction internally has been very positive,” says Patrick Reynolds, head of operations at Neotas. “Users are confident they are using a simple, secure information security system. We have seen bigger vendors with software that is bamboozling, but not as effective for what we require. It’s about finding a cybersecurity-by-design approach that works for your business.”

Introducing cybersecurity by design into an organisation provides a holistic set of pragmatic guidelines which can enable businesses to consider the full remit of protection. Companies that don’t put design processes in place to cope with the ever-present avalanche of cyberthreats will be more open to damaging vulnerabilities. ●

BIGGEST CYBER THREATS TO ORGANISATIONS

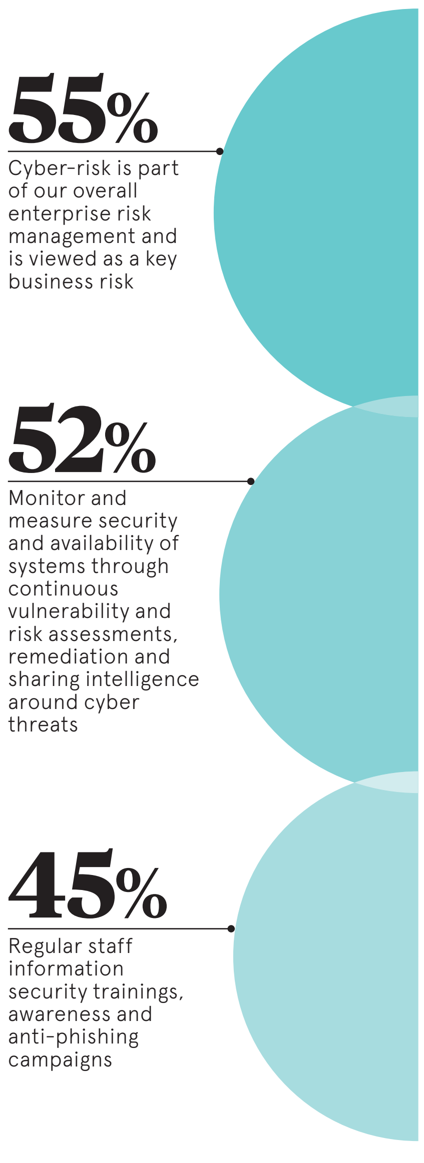
Survey of US security professionals



Egress 2019

TOP THREE APPROACHES TO MANAGING CYBER-RISK AND IMPROVING RESILIENCE

Global survey of risk professionals



Allianz 2020

Distributed in

THE SUNDAY TIMES

Published in association with

infosecurity® EUROPE

OMDIA

Contributors

Cath Everett
Journalist specialising in workplace, leadership and organisational culture, she also writes about the impact of technology on business and society.

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

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

raconteur reports

Publishing manager
Reuben Howard

Managing editor
Benjamin Chiou

Associate editor
Peter Archer

Deputy editor
Francesca Cassidy

Digital content executive
Taryn Brickner

Head of production
Justyna O'Connell

Design
Joanna Bird
Sara Gelfgren
Kellie Jerrard
Harry Lewis-Irlam
Celina Lucey
Colm McDermott
Samuele Motta
Jack Woolrich

Head of design
Tim Whitlock

Although this publication is funded through advertising and sponsorship, all editorial is without bias and sponsored features are clearly labelled. For an upcoming schedule, partnership inquiries or feedback, please call +44 (0)20 8616 7400 or e-mail info@raconteur.net. Raconteur is a leading publisher of special-interest content and research. Its publications and articles cover a wide range of topics, including business, finance, sustainability, healthcare, lifestyle and technology. Raconteur special reports are published exclusively in *The Times* and *The Sunday Times* as well as online at raconteur.net. The information contained in this publication has been obtained from sources the Proprietors believe to be correct. However, no legal liability can be accepted for any errors. No part of this publication may be reproduced without the prior consent of the Publisher.

/raconteur.net
@raconteur
@raconteur_london

raconteur.net /cybersecurity-2020

Commercial feature

Building a culture with security at the heart

With the security perimeter shifting from the office to the home, security leaders must speak the language of the business to build the culture needed to protect their company and overcome the perception they are blockers of innovation

As many employees are already, or soon will be, working remotely, organisations globally are implementing a variety of cloud-based solutions to support staff in adjusting to working from home. The primary goal is maintaining close to the same level of productivity as if they were in the office.

However, in a world of accelerated transformation and a shifting security perimeter, companies must ensure they have fit-for-purpose security solutions in place combined with an organisation-wide awareness programme.

Data breaches have become a lot more difficult to detect. Every opportunity is used by cybercriminals to gain entry, such as phishing emails that masquerade as important updates on topical and newsworthy items, including COVID-19. This means the focus now needs to be on employee awareness and behaviour. If employees aren't vigilant, this can easily create vulnerabilities regardless of how much has been spent on security solutions.

"Tried-and-trusted methods of cyberattack, such as phishing and social engineering, are still the best way of gaining access and compromising a business, and they're very much targeted at the individual and what that individual knows," says Barry McMahon, senior international manager at LastPass by LogMeIn.

"That's not to say the problem is between the seat and the keyboard as there is an onus on the business to make sure they put the right tools, processes and procedures in place. Unfortunately, that's where many companies stop. The real value is realised when an organisation-wide culture of awareness and appreciation for security is aligned to existing solutions and processes.

"To build a security culture, you need to communicate with employees in a language they understand which, for the most part, is a non-tech language. Try to make it relevant to their personal life and then, by association, address the relevance to the business.

"Companies need to shift from a few employees doing a lot, to a lot of employees doing a little, and then continually improving on that and measuring the improvement along the way. If you can't measure it, how can you demonstrate you are adding value by reducing the risk profile of the business?"

Whether an employee is working from the office or remotely, the best security approach is to manage their digital identity and access methods as they login to the resources they need. But this must be done in a frictionless way. User experience is crucial to building a security culture and, if it is poor, employees will quickly find ways to circumvent the security measures in place. If user experience is good, employees will barely even realise those measures are there.

Many security teams face the additional challenge of being sidelined. While cloud solutions offer enormous value, they also allow line-of-business and department heads to bypass security teams if they perceive they are blockers of innovation and productivity, and then deploy the solutions on their own. This means the security or IT department is no longer the automatic gatekeeper of any technology deployed, which can create vulnerabilities and security blind spots they're not even aware of.

Security teams therefore face the task of changing the perception not just of themselves, but of security as a whole within the business. This requires proactive communication and raising awareness of the value and credibility they add when they are involved. If they fail to change that perception, and line-of-business and department heads continue deploying technology in their own vacuum, it will be the security team's problem when something is compromised.

Similarly, in line-of-business projects, security leaders need to position themselves as the experts who can enable projects to be secure by design. By positioning the security team's involvement as a seal of approval, the line-of-business stakeholders can use this to demonstrate their project doesn't expose the business to any unnecessary risk.

"If security teams are out of the loop, then from a top-down perspective it's likely that senior leaders in the business just see them as a cost centre," says McMahon. "This not only increases the exposure of the business to vulnerabilities and threats, but could also lead to the company losing talent from its security team. With talent in the security sector a scarce resource right now, if security professionals don't feel valued, challenged and energised, they're likely to search for a company where they will add value."

Business leaders are unlikely to approve investment for something they can't comprehend, so security leaders that talk in a language they understand will fare much better. It's important to point out that the underlying security objective may not change, but how the organisation perceives the value security adds will rely heavily on how security leaders communicate its business value. By translating the value they are offering, from security language to business language, they can get the buy-in they need.

> "Security leaders need to seize this opportunity which will elevate their profile, change perceptions and bring them back to the decision-making table

"That's how they can start to change how they are perceived in the business and add more value, rather than being considered a blocker," says McMahon. "Employees are the single largest vulnerability to a business, but the flip side is they're also the single biggest security resource a company has. A security culture is achievable if employees are educated and made aware of why it's important.

"Security leaders need to seize this opportunity which will elevate their profile, change perceptions and bring them back to the decision-making table. At LastPass, we work with companies to achieve that culture and protect their business in a more sustainable and evolving way."

Organisations realise identity management is no longer their core competency given the variety of on-premise and cloud services employees and partners have and need access to. And with the high probability that the workforce will be based away from the office for the foreseeable future, on-premise identity management solutions are not reactive enough to scale to meet the needs of a dynamic business. They need to work with a company that has identity management as a core competency.

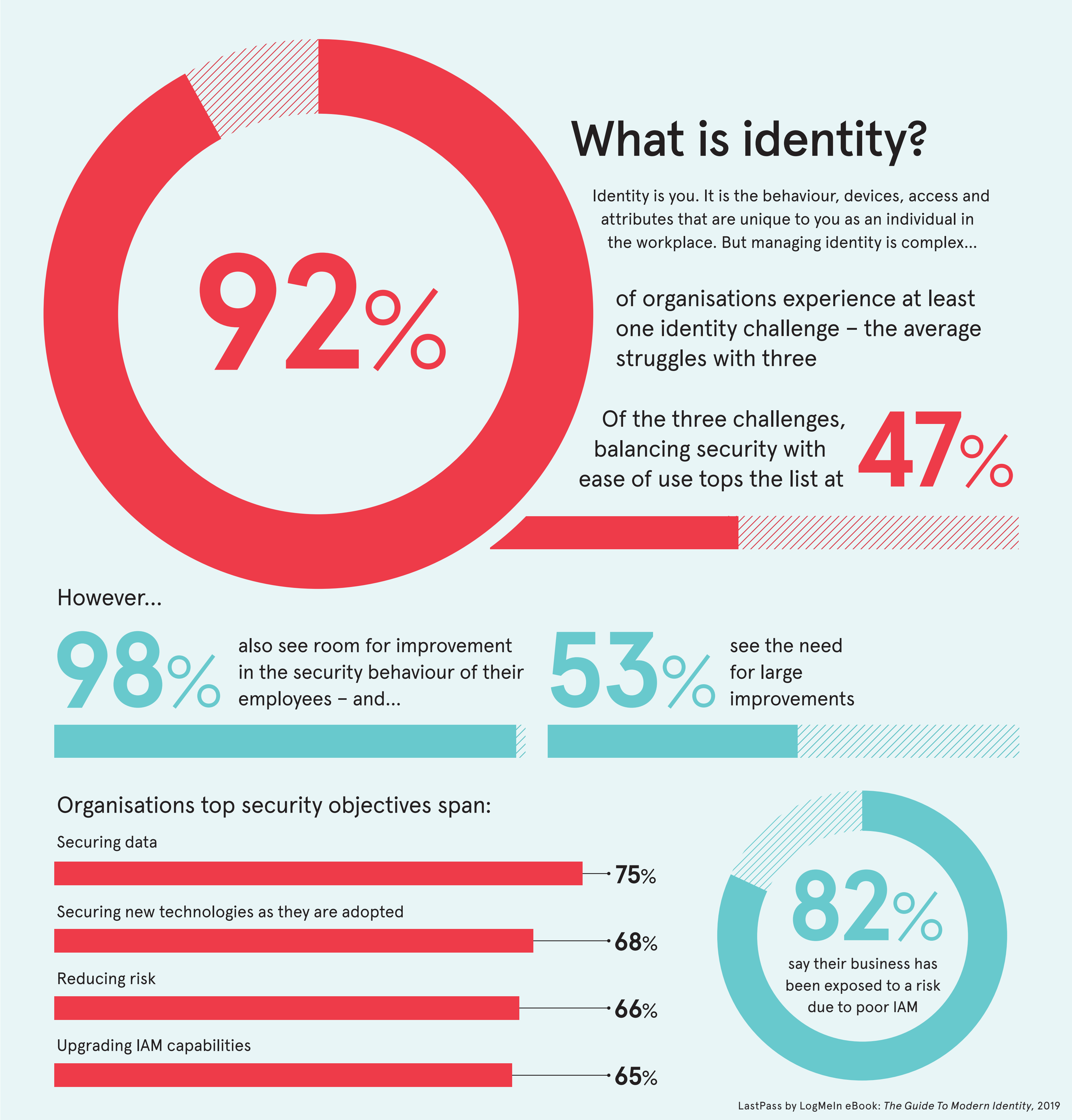
"Many people are familiar with LastPass from a personal user perspective," says McMahon. "In the corporate space, LastPass offers a compressive identity management solution combining enterprise password management (EPM), single sign-on (SSO) and multi-factor authentication (MFA).

"EPM goes a long way to eliminating password reuse, providing admins with detailed reports and policy controls, and employees with a secure vault accessible across all devices and browsers, which creates and stores strong, unique passwords for immediate use when required.

"For applications that are high use by a large portion of the organisation, leveraging SSO to put all the applications behind a single login window is best practice. And leveraging MFA adds an additional security layer that prompts users to validate they are who they claim to be. This can be done in a number of ways, such as via biometric request or other push notifications. This is all contained within one platform, so companies that come to LastPass can enjoy a complete identity as a service, or IDaaS, solution from one vendor."

For further information please visit www.lastpass.com/identity

LastPass ••• | by LogMeIn



What is identity?

Identity is you. It is the behaviour, devices, access and attributes that are unique to you as an individual in the workplace. But managing identity is complex...

92% of organisations experience at least one identity challenge – the average struggles with three

Of the three challenges, balancing security with ease of use tops the list at 47%

However...

98% also see room for improvement in the security behaviour of their employees – and...

53% see the need for large improvements

Organisations top security objectives span:

Securing data	75%
Securing new technologies as they are adopted	68%
Reducing risk	66%
Upgrading IAM capabilities	65%

82% say their business has been exposed to a risk due to poor IAM

LastPass by LogMeIn eBook: *The Guide To Modern Identity*, 2019

95%

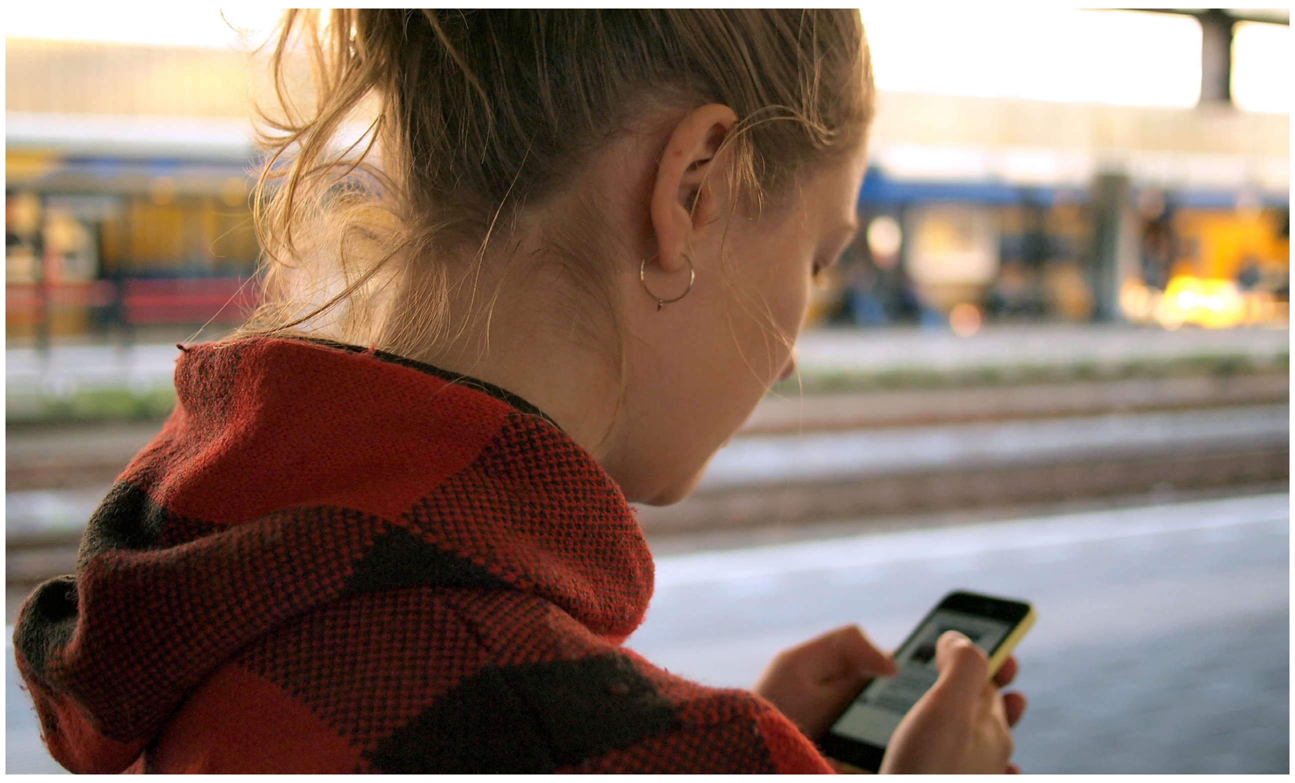
of organisations claim to have a good or complete understanding of authentication

59%

believe strengthening user authentication with MFA is crucial

93%

agree that bringing the various aspects of identity and access management under one solution would greatly benefit the overall security of the organisation



Changing hearts and minds

One of the greatest challenges enterprises face in safeguarding their business is encouraging the right behaviours among their employees

Pinsent Masons

International law firm Pinsent Masons has developed a human-centric approach to security to help protect the future of the organisation through education, transformation and trust.

Central to this approach has been an acceptance by the firm that people will typically be more interested in safeguarding their own digital lives than the company they work for. Rather than challenge this mindset, Pinsent Masons has sought to tap into it to develop behaviours that benefit the business as well as employees in their personal life.

An area where the mindset is most evident is passwords. Remembering numerous passwords, or having to change them frequently, can not only be frustrating to staff, but often counterintuitive to security if people write them down or only change them slightly each time.

Recognising this, Pinsent Masons turned to LastPass's enterprise password management (EPM) solution to ensure its employees had a secure way of storing their passwords in a vault that requires just one password to be accessed.

> "Our ultimate goal is to ensure our people are at their most secure wherever they are

To bolster Pinsent Masons' vision to enable staff to follow this way of working, LastPass has provided each employee with a personal LastPass Premium account for use in their personal lives alongside the enterprise installation. This is key to encouraging the right behaviours.

"Our ultimate goal is to ensure our people are at their most secure wherever they are," says Christian Toon, chief information security officer at Pinsent Masons. "With LastPass, we've been able to procure an enterprise password manager that has given a personal benefit to our employees as well as value to our firm. The onboarding LastPass provided has also been excellent.

"Password managers are still quite new to many organisations, so culture change is required to bring people on board. LastPass has been supportive in resource, but also in personnel and content to help us get those hearts and minds where they need to be."

Another major threat vector in the legal sector is phishing, which firms such as Pinsent Masons have historically tackled by measuring click rates on suspect emails. Pinsent Masons was seeing little results from the approach and the perception among employees that the security team is trying to catch them out can perpetuate a divide.

In 2017, as part of their efforts to build a human-centric security culture, Toon and his team decided to flip the approach by instead urging people to report suspicious emails and measuring based on that. To encourage employees to feel confident and comfortable in reporting such emails, they embraced gamification by producing league tables showing which departments were the most prolific.

"Our reporting has gone through the roof because people are now more aware," says Toon. "It's a great example of how changing our language and approach can have a huge benefit. The culture we've built means people feel safe and comfortable talking about security, escalating it and allowing us to deal with it.

"That's helped no end not just in terms of security, but also our reputation internally. We're no longer seen as blockers or the sales prevention team or the people who say no. We're an integral part of the firm's growth because the business can continue doing what's needed to support clients and we know they're doing it securely because we're involved in those conversations."

Human-centric security is the growing trend within many verticals. And while digital transformation brings new technology and greater productivity, some risks haven't changed, such as phishing and social engineering.

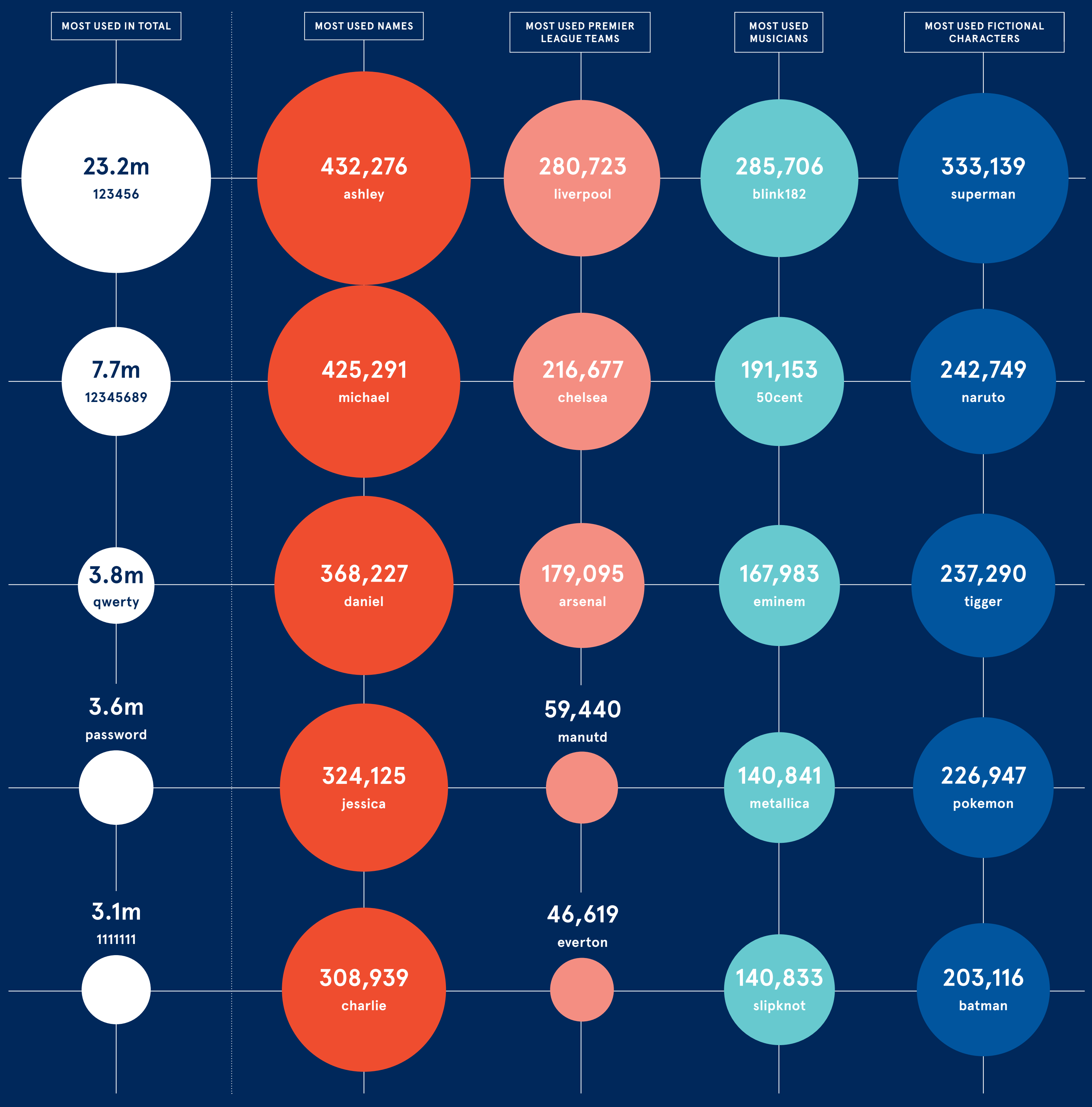
"Our human-centric security policies are all about making security work better with and for people," says Toon. "It's very much front and centre of our employees' lives when they're at work and when they're at home. Fostering the right behaviours and continuing on this human-centric journey with LastPass has reduced the risk to our business in a way that benefits everyone. It's a win-win."

PUBLIC PRIVACY & PROTECTION

Consumers are increasingly concerned about how their personal information is used by organisations, and what measures are in place to protect their data. But when it comes to their own cybersecurity, many still don't know how to protect themselves online, and are using unsophisticated passwords that won't prove much of a test for your average cybercriminal

MOST USED PASSWORDS

Analysis of breached accounts worldwide



MOST USED IN TOTAL	MOST USED NAMES	MOST USED PREMIER LEAGUE TEAMS	MOST USED MUSICIANS	MOST USED FICTIONAL CHARACTERS
23.2m 123456	432,276 ashley	280,723 liverpool	285,706 blink182	333,139 superman
7.7m 12345689	425,291 michael	216,677 chelsea	191,153 50cent	242,749 naruto
3.8m qwerty	368,227 daniel	179,095 arsenal	167,983 eminem	237,290 tigger
3.6m password	324,125 jessica	59,440 manutd	140,841 metallica	226,947 pokemon
3.1m 1111111	308,939 charlie	46,619 everton	140,833 slipknot	203,116 batman

National Cyber Security Centre 2019

63%

of global consumers say most companies aren't transparent about how their data is used

58%

say they are comfortable with relevant personal information being used in a transparent and beneficial manner

54%

say most companies don't use data in a way that benefits them

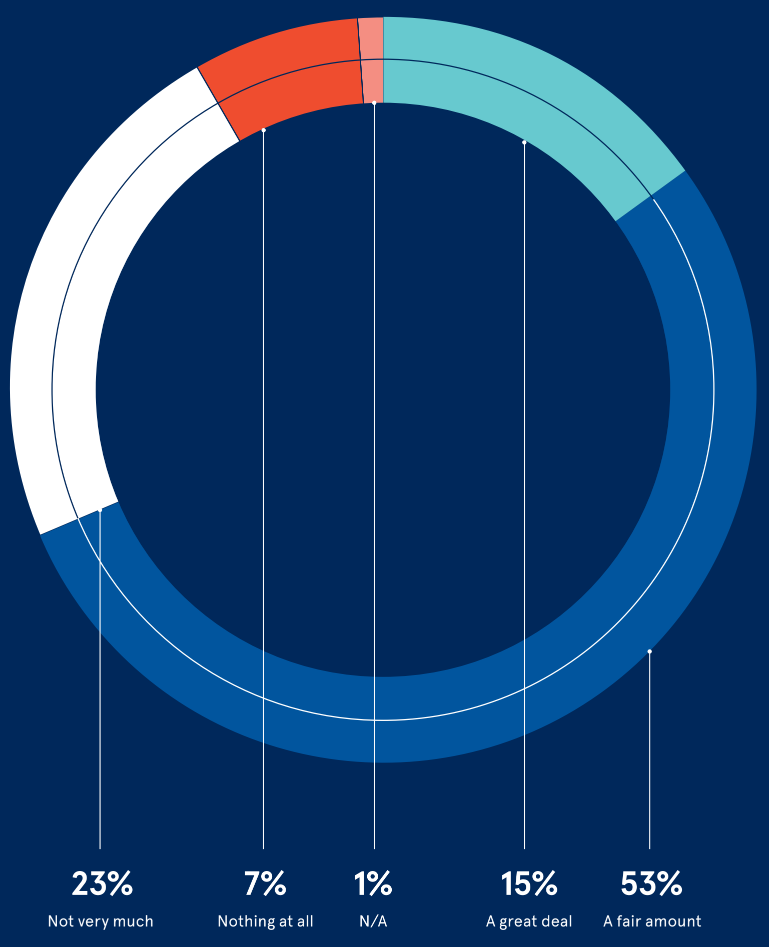
48%

have stopped buying from a company or using a service due to privacy concerns

Salesforce 2020

CYBER PROTECTION AWARENESS

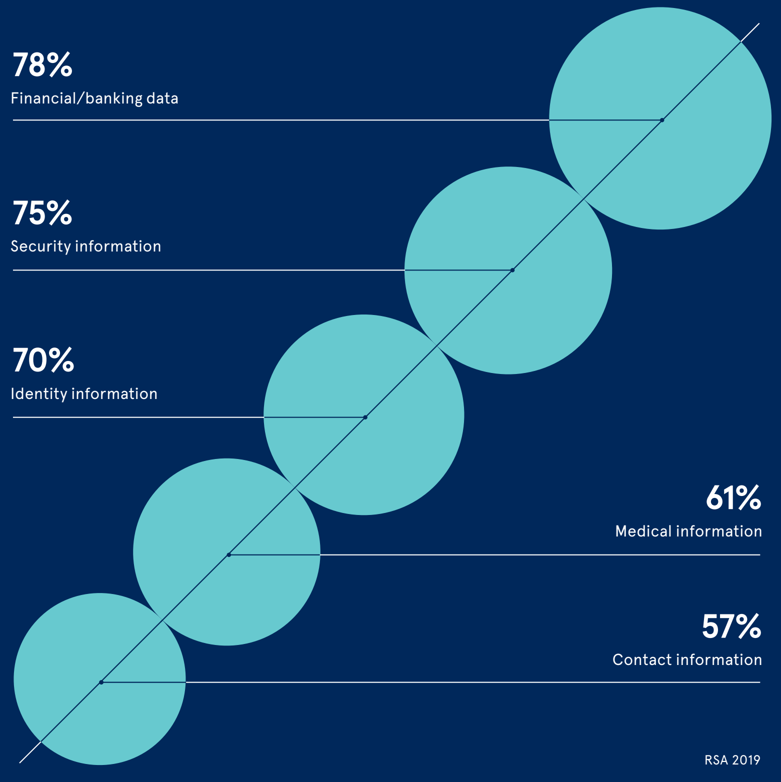
Whether UK consumers think they know how best to protect themselves from harmful cyber activity



National Cyber Security Centre 2019

PERSONAL INFORMATION CONSUMERS CARE ABOUT THE MOST

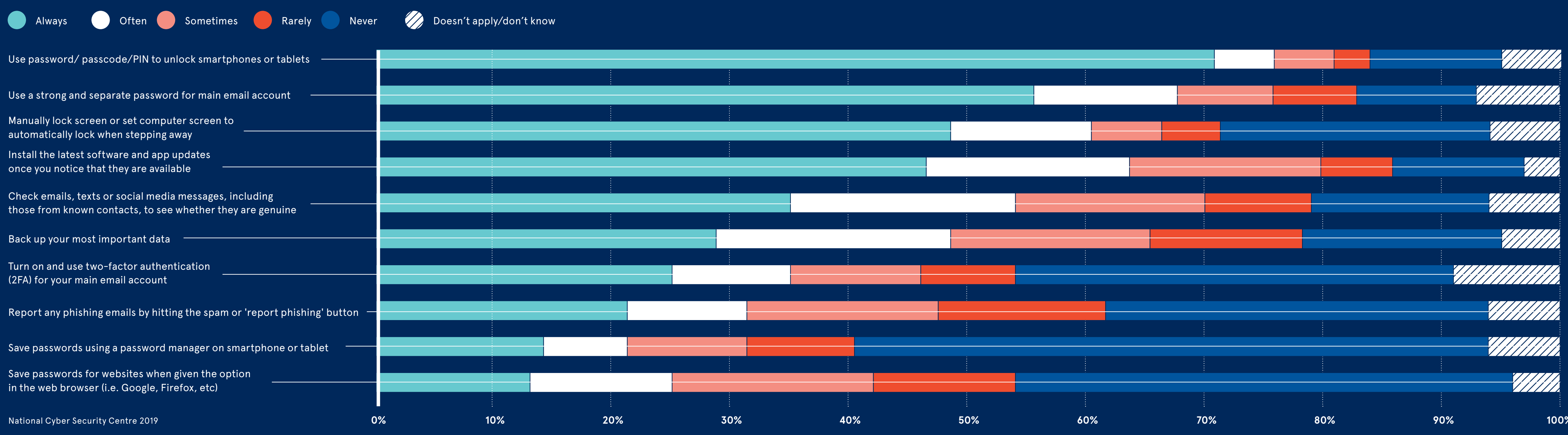
Survey of consumers across France, Germany the UK and United States



RSA 2019

HOW CONSUMERS PROTECT THEMSELVES ONLINE

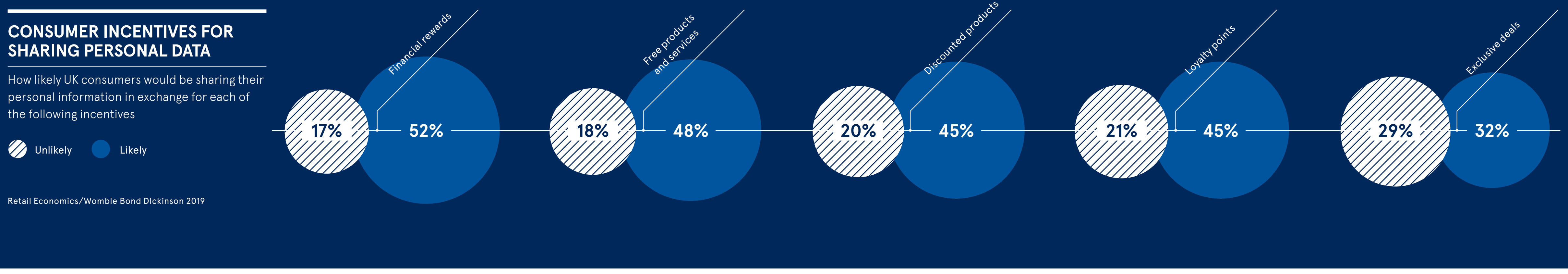
How regularly, if at all, UK consumers do the following



National Cyber Security Centre 2019

CONSUMER INCENTIVES FOR SHARING PERSONAL DATA

How likely UK consumers would be sharing their personal information in exchange for each of the following incentives



Retail Economics/Womble Bond Dickinson 2019

STRESS

How to stop CISO burnout

High levels of stress, an industry skills crisis and heavy workloads are just some of the reasons why some cybersecurity leaders are feeling overwhelmed

Cath Everett

Mangostar/Shutterstock

An eye-popping 81 per cent of executives in a chief information security officer (CISO) role in the UK feel burnt out, with nearly two thirds thinking of either leaving their job or quitting the industry altogether, according to a report by Goldsmiths, University of London.

The number-one cited source of stress is the need to comply with regulations, such as the European Union's General Data Protection Regulation, with two out of five respondents worried about being held responsible in the event of a security breach.

But there is also deep concern about everything from skills shortages and the size and complexity of IT environments to the ever-growing volume of threats.

So what is going on here? Are things really as bad as they would appear, with those in the CISO role on the verge of a mass walkout? Or are they simply being melodramatic and overreacting to the everyday pressure that comes with a high-level position?

For Amanda Finch, chief executive of the Chartered Institute of Information Security, neither scenarios ring true. While she is sceptical that the levels of stress burnout and disaffection are quite as bad as the figures would suggest, she believes people are undoubtedly feeling stretched and require more support.

"The situation's definitely not great," says Finch. "Most CISOs are stressed and are working at very high levels, so if they're not burnt out, they're probably working towards it. There's certainly a big problem there and this report is highlighting that."

However, she adds that most CISOs are very committed to what they do, which means more than anything she views the findings as a "signal of their frustration and desire to be heard as it's a very challenging role".

Anthony Young, director of information security specialist Bridewell Consulting, agrees. While he believes most people in the CISO role are unlikely to switch career paths entirely, the frustration they experience does tend to lead to a "fairly high degree of churn" in the hope that life will be better elsewhere. It's a scenario that can prove expensive in recruitment terms for their employers.

> **Most CISOs are stressed and are working at very high levels, so if they're not burnt out, they're probably working towards it**

"The job of the CISO is extremely stressful, especially considering the cyberthreat landscape, the risk of attack and the increasing sophistication of cyberattackers," he says. "However, the CISO's job is made even more stressful by a lack of budget and support at board level."

Both are imperative if security bosses are to be in a position to build the team they need around them and to implement an effective risk-based strategy supported by adequate tools and policies. But the problem is all too often organisations bring CISOs in to "appease regulators, shareholders and customers without granting them the necessary power of mandate and resources" to perform their role adequately, says Young.

This situation is also not helped by the cybersecurity industry's skills crisis, coupled with a lack of desire, in some instances, to pay the high sums necessary to hire scarce expertise. While such skills gaps are undoubtedly worse in areas where specialist technical know-how is required, such as penetration testing or cloud security, the difficulties involved in finding experienced talent are across the board.

As a result, most CISOs have vacancies in their teams they struggle to fill, which simply adds to the pressure of them having to be both constantly available and being held accountable for situations that are not always under their control.

Therefore, to try to address the issue and help those in a CISO role "get off the merry-go-round", Finch recommends widening the potential talent pool beyond trained individuals, who can hit the ground running from day one.

Instead she suggests targeting people with transferrable skills, who could benefit from cross-training. An example includes reskilling individuals with analytical expertise, such as business analysts and project managers, as risk managers.

Another potent means of helping to reduce workloads and take the pressure off is for the board to sponsor, and invest in, security awareness training for the workforce as a whole to make it clear that everyone, not just the CISO, is responsible for organisational safety.

Azeem Aleem, vice president of consulting at NTT Security, explains: "It's about everyone working with the CISO to protect the organisation. Otherwise, security controls are bypassed as people see them as a hindrance, and so they unwittingly make themselves and the organisation vulnerable."

But just as vital is that senior executives and those in the CISO role find ways to communicate with each other more effectively. For members of the board, this involves explaining what they need to know and helping their CISOs to express security risks in more of a business and operational risk context, not least to understand the support they require.

For CISOs, on the other hand, it is less about discussing individual security breaches and more about clarifying how such incidents could affect the business, its ability to function and the bottom line. It is also important to explain how cybersecurity can act as a business enabler.

Haroon Malik, cybersecurity consultant and strategist, explains the rationale: "It's about digital trust. If cybersecurity is intertwined with new product development, customer trust is heightened. Ten years ago, people didn't care, but some companies won't do business with you now if you can't prove you're taking security seriously."

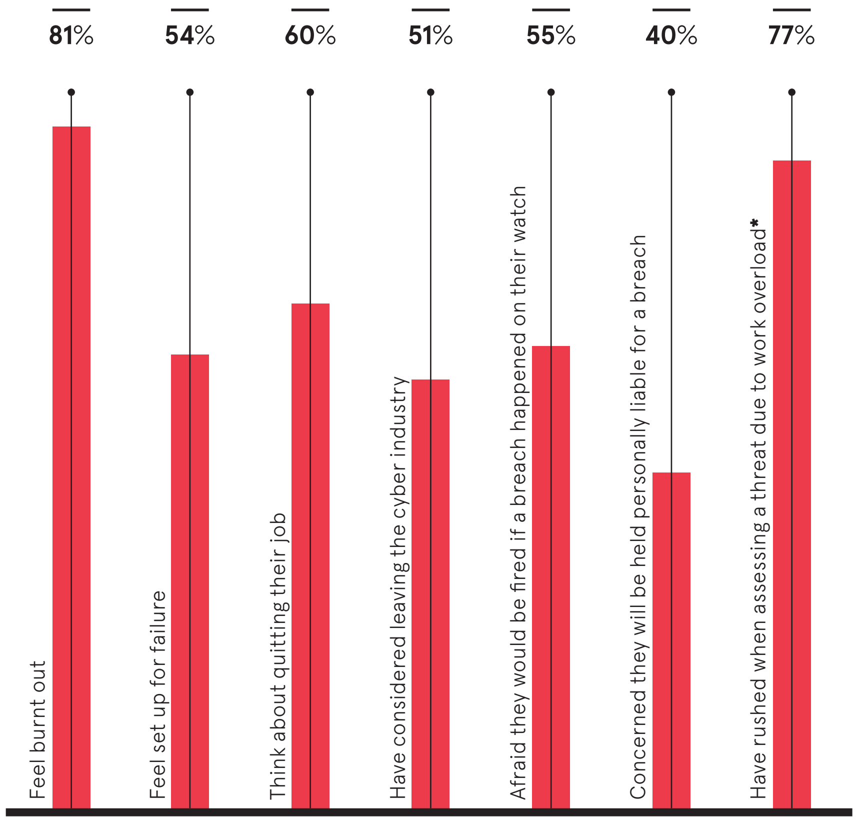
Once CISOs can carve out some space and move beyond their usual firefighting mode, it frees their time up to develop a more strategic risk-based approach to activities, thus creating a virtual circle.

As Aleem points out, even though there will never be such a thing as 100 per cent security, CISOs are currently made liable and accountable for securing everything in the organisation, which results in high levels of stress as they attempt to mitigate every risk.

But he concludes: "It's much more effective to adopt a risk assessment approach. The idea is that if you can identify your crown jewels, you know what to protect and where to focus your budget. If you don't, you just end up running around like a headless chicken and that's way burnout lies." ●

CYBERSECURITY OVERLOAD

Survey of cyber professionals in the UK



*Average answer for respondents across the UK, Germany and France

Goldsmiths/Symantec 2019

Commercial feature

Human error puts companies at biggest risk of data breach

Data breaches are far more likely to be caused by an employee sending an email to the wrong person than a malicious outsider, leaving companies focusing on the wrong area

Fear of suffering a data breach is now one of the top issues that keep board directors awake at night. High-profile cyberattacks on major brands, such as British Airways, Tesco and TalkTalk, have not only come at a significant financial cost, but also caused great reputational damage.

As a result, investment in the best cybersecurity solutions to prevent such attacks will exceed $1 trillion by 2021, according to analyst firm Gartner.

The last couple of years have seen the number of data security incidents reported to the UK Information Commissioner's Office (ICO) increase by 75 per cent as companies were getting their house in order for the European Union's General Data Protection Regulation (GDPR).

Yet a huge 88 per cent of them were not the result of deliberate cyber incidents, but rather simple human error. More than a third were security incidents relating to data being emailed, posted or faxed to an incorrect recipient by mistake.

"Malicious cyberattacks are certainly an important area, but the biggest risk is actually within organisations and it is worryingly overlooked," says Dean Sappey, president and co-founder of DocsCorp, a software firm for document professionals.

"Organisations have a huge amount of document-based information in the likes of Microsoft Word, Excel and PDFs, and information is commonly being sent out to customers, partners and so on. That's where it's far easier for information to be sent to the wrong people, not from any sort of fraudulent activity, just accidentally sending it to the wrong person.

"We've all done it; put in the wrong email address and the moment you hit send it's too late. You can send another email asking the person not to read it, but that's almost guaranteed to have the opposite effect. We work with thousands of law firms, accountants, corporations and government departments that communicate a lot via email and the chances of sending to the wrong person are huge. How do we make that process more reliable and accurate?"

> **Malicious cyberattacks are certainly an important area, but the biggest risk is actually within organisations and it is worryingly overlooked**

The issue is not only preventing employees from sending emails to the wrong person, but also removing hidden metadata in documents. Track changes in Microsoft Word documents are commonly still present in the file even if you can't see them.

Famously, this landed Tony Blair's government in trouble when a review of the metadata in the Iraq War dossier revealed that much of the content had come from a US researcher and was not in fact new information.

A geotagged location is another piece of data that people are often unaware is hidden in a digital photograph they send to others, showing the exact place where it was taken.

DocsCorp's software provides integration with some systems to check automatically if a person who is being emailed is allowed to receive that message or document based on the particular role of the sender within the organisation. The software is also able to look at all the metadata inside documents and enables companies to set up policies always to remove, for example, track changes and geotagging information before being sent.

"It's not difficult to implement; it just takes the willingness of the organisation to ensure this massive area of potential leaks is covered," says Sappey. "Rapid developments in technology mean it is constantly getting easier and easier to press one button and suddenly lots of information is collated and sent out. The introduction of the GDPR makes something that was previously just embarrassing for a company now significantly damaging financially.

"The cost of implementing a solution to eliminate the issues of human error and hidden metadata is a small fraction of what you spend on a copy of Microsoft Word or Windows, and entirely minuscule compared to what you face if you suffer a data breach and are fined by the ICO."

For more information please visit docscorp.com

DocsCorp
Work smart

OPINION

'There is no time like the future and, ultimately, it is in our hands'

Resilience is at the heart of information security. As threats adapt and evolve and we accept that systems will be compromised, it is no longer enough just to have strong defences in place. The sophisticated tools and techniques of threat actors will find a way around them. Organisations, their security architecture, systems, policies and strategies need to be resilient, able to cope, recover and, most of all, to learn from incidents.

Our sector as a whole needs to be resilient; human skills and expertise are at the heart of this. We must attract, recruit and retain the talent and skills to tackle new and emerging risks and challenges. We must also embrace diversity in all its forms to find, nurture and train professionals.

It is the responsibility of every organisation to drive inclusivity and diversity in the industry. We should look beyond the traditional routes into information security and think about other transferable skills and attitudes that can offer so much. These include broader business skills, such as the ability to negotiate, financial acumen and leadership skill, that are increasingly needed as part of a modern-day security team.

It also includes skills from outside the industry, so it is encouraging to see organisations starting to recruit more people from sectors like healthcare, the emergency services, design and gaming.

But resilience goes much further than this. We, as infosecurity professionals, need to be resilient ourselves, developing new skills and, on a personal level, being resilient to the pressures and stress currently facing our industry.

Employee mental health and wellbeing should be an essential consideration for all employers and be part of company culture and organisational values. But perhaps we could do more in an industry that is faced with growing cyberthreats, longer working hours and individuals often having to make up gaps left by under-resourced teams. It's clear from what we are hearing from our community of chief information security officers that infosecurity professionals are under more pressure than ever before.

But with challenges come opportunities. The industry is undergoing a huge transformation as it embraces new and emerging technologies, such as quantum computing, data analytics and artificial intelligence tools, which can play a key role in enhancing the capabilities of security systems to identify and mitigate risks, and ease the pressure on security teams.

As an information and cybersecurity community, we can help to keep our world safe and unlock more of the good things that technology promises and delivers. There is no time like the future and, ultimately, it is in our hands. But this goes beyond just the information security industry and out to a wider group of individuals and organisations.

By working together, companies, governments, industry bodies, academia, suppliers and other stakeholders can share their knowledge and intelligence, learn from each other and get ahead of cybercriminals. This need to collaborate and share knowledge has never been more important as new kinds of threats emerge from new breeds of attackers, and we need to stay one step ahead.

Resilience is our conference theme this year, addressing the most relevant and decisive factors in information and cybersecurity in the next five years.

By building resilience across the industry, we can move towards a more secure world and a more secure future. ●

MOST IMPORTANT ELEMENTS OF A SUCCESSFUL CYBER-RESILIENCE APPROACH

Findings from the latest Infosecurity Europe Twitter poll in February, drawing nearly 7,000 responses

40% of respondents said human skill and expertise was the most important element

22% said implementing best practice

20% said governance and compliance

Nicole Mills
Exhibition director
Infosecurity Group

C-SUITE

Fighting threats from all sides

In an era when cyberthreats are constantly evolving and all business leaders must be security experts, what role should each member of the C-suite play in protecting the business?

Davey Winder

CEO

Chief executives are accountable for the whole company and its performance. They set the tone and pace for the full breadth of the corporate approach to its market and environment. The right cyber approach by C-level positions not only protects the business from threats, both financially and reputationally, but can also create value in the eyes of customers, stakeholders and peers.

Cybersecurity is only important to an organisation if the CEO and board make it so. CEOs must create a culture of security within the business and invest their personal time and resources to back up their words and promises. They must ensure they are kept up to date with critical cybersecurity concerns and are knowledgeable of the issues and associated opportunities.

"It is essential CEOs elevate the chief information security officer to a position of prominence with authority, and understand their cyber-risk aperture by baselining against industry best practices," says Mark Testoni, CEO of SAP's national security arm SAP NS2. "In addition, they should create and fund a plan to get the company where it needs to be in terms of cybersecurity."

CFO

While chief financial officers don't necessarily have to understand the full technical aspects of cybersecurity, they must be aware of the financial risks associated with the ever-increasing number of cyberthreats. The importance of this is emphasised by the harsh penalties which can potentially be given as a result of General Data Protection Regulation (GDPR) non-compliance: up to €20 million or 4 per cent of annual global turnover. This serves as a real threat to any C-level positions and puts it firmly on the CFO's radar.

Given that any data breach could seriously impact the reputation of an organisation, it falls to the CFO to ensure organisations are not only compliant with regulations, but also well protected. These risks must be taken into account when the CFO is advising on growth and cost-saving initiatives. Therefore, they must work closely with cybersecurity professionals to understand the risks, ensure that any proposals take into account cybersecurity implications and lend all reasonable support to any initiatives aimed at protecting the business.

"In a modern organisation, there is an ever-evolving overlap between cybersecurity and financial risk," says Mark Blakemore, CFO at Compleat Software. "As a result, I believe the relationship between CFO and chief information security officer is an increasingly symbiotic one. While a CISO can present the risks and work in a more technical fashion, a CFO can also help improve security by assisting in translating risks into a language better understood by senior leaders."

COO

Traditionally the second-in-command leader among C-level positions, chief operating officers are focused on operations and business efficiency. They play a central role at the heart of a business and therefore need to play a central role in ensuring it is protected from threats.

The COO needs to be asking the hard questions and recognising that unquantifiable cybersecurity risk is negligence. They need to reject fallible, sub-par solutions and instead look to incorporate new and innovative approaches, for example moving away from traditional, reactive responses to cybersecurity that often fail businesses and instead looking into more proactive moves that really embed security principles into processes.

The COO must work with different leaders across the company to ensure all parts of the business are working together to deliver the same goal, not only protecting the business from damaging threats, but also building positive differentiation from its competitors.

"With companies increasingly aware of the cyber-risk introduced by partners and suppliers, creating a digitally pure enterprise that can confidently boast risk-free sharing of business information is immensely valuable, and that's where the COO can play a crucial role," says Dan Turner, CEO at cybersecurity firm Deep Secure. "Any business that can establish a track record for guaranteeing its users, partners and customers access to clean, threat-free business content and services will differentiate themselves in today's dangerous cyber landscape."

CMO

Technology is a firmly established part of marketing and customer experience. The role of chief marketing officers is rapidly changing and technology is becoming more deeply embedded in their responsibilities as they drive digital transformation within the organisation. Therefore, it is essential they fully understand the ongoing dangers of cybersecurity and GDPR.

CMOs and their marketing teams manage confidential data so must understand the principles of cybersecurity as part of their responsibility to be compliant and responsible for where information is stored, how it is managed and whether it is being used in a secure way.

The rise of marketing technology, or martech, has seen emerging innovation, including social media, design, email marketing and automation apps, become the norm for marketing campaigns, which presents an opportunity to hackers. Of all C-level positions, CMOs must have the strongest security awareness of how technology is used in the business.

"Working collaboratively alongside their C-suite colleagues, CMOs should ensure the right cybersecurity technology is implemented to protect the organisation and its customer data, and help the business achieve its goals," says Faye Eldridge, head of demand at Doherty Associates. "CMOs can also advocate better cybersecurity practice within the organisation by providing marketing communications on cybersecurity awareness to employees."

CRO

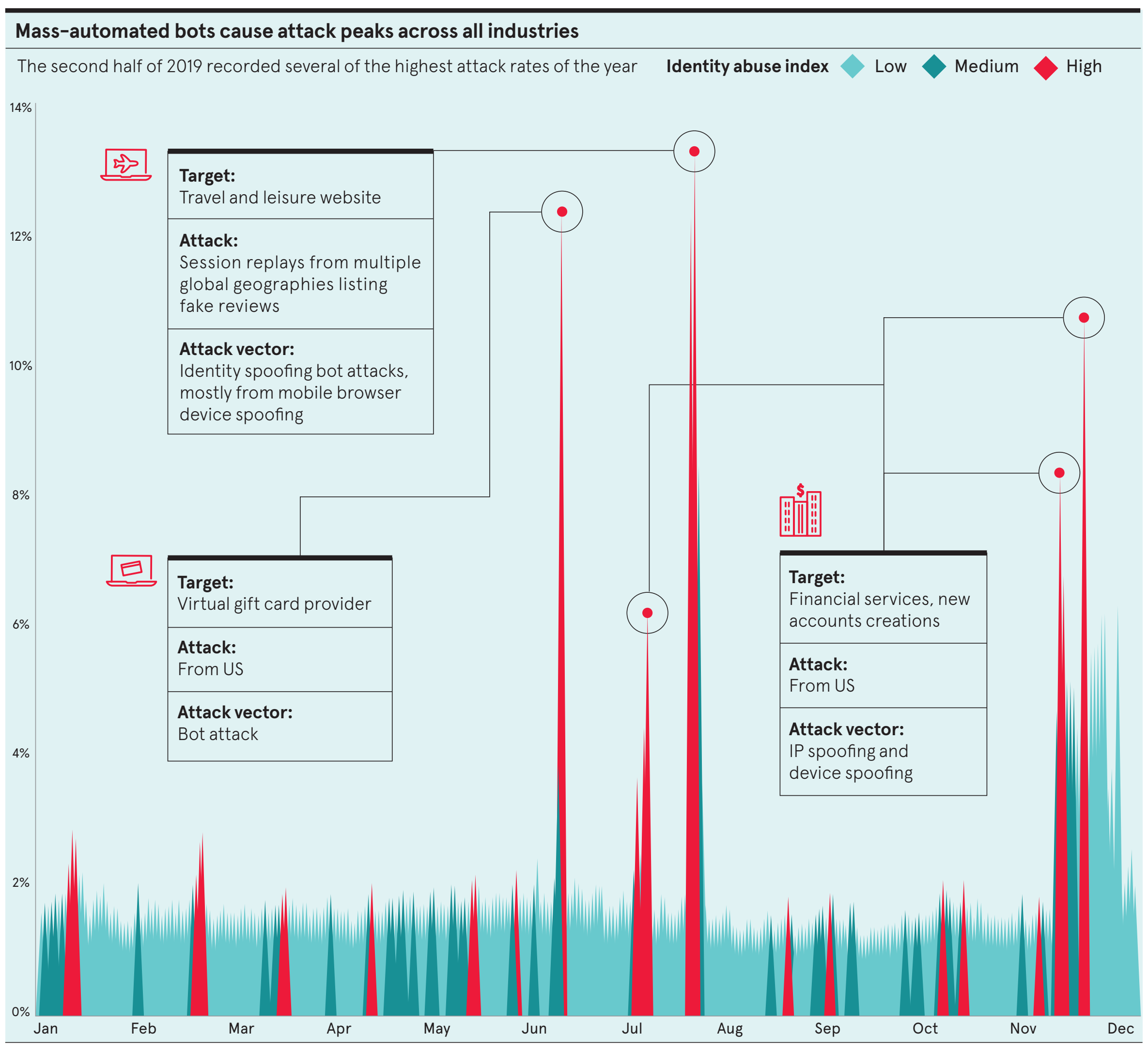
The chief revenue officer is responsible for all sales generation across the company and this includes the processes business development teams adopt. It puts the CRO in a similar boat to the CMO, ensuring sales staff are aware of their responsibilities to be GDPR compliant when attempting to acquire leads and applying basic security practices to their outreach.

To protect companies from cyberthreats effectively, CROs must foster a culture of security and accountability among the sales team. Cybercriminals are always finding new ways to attack businesses, exploiting vulnerabilities in technology and the humans who use it. As a result, CROs need to be multidisciplinary. While this doesn't mean deep expertise, it does require a deeper awareness of the nature of cyber-risks and how they can be addressed.

"In today's threat landscape, businesses must go beyond establishing baseline protocols to create and maintain a secure environment," says Adam Philpott, Europe, Middle East and Africa president at McAfee. "The key to achieving cyber-resilience within an organisation is collaboration and understanding across the board. C-level positions and cybersecurity experts need to find a common data-language to understand the risks and how to adapt to manage them." ●

Mass-automated bots cause attack peaks across all industries

The second half of 2019 recorded several of the highest attack rates of the year



Battle of the networks

Rebekah Moody, director, Fraud and Identity at LexisNexis® Risk Solutions, reveals the latest insights from the firm's *Cybercrime Report* and how its Digital Identity Network® is helping to fight an increasingly interconnected network of fraudsters

Q Your biannual Cybercrime Report is always highly anticipated due to the volume of transactions you process. What trends caught your eye in the latest report?

A We process more than 35 billion online transactions a year globally so that gives us a really interesting perspective on what's going on in the world of cybercrime. Our latest report, which covers the period between July and December 2019, shows quite a significant tipping point in terms of the platforms that fraudsters target. Four years ago, mobile devices made up about 20 per cent of our network traffic. In the latest report, it's about two-thirds. The shifting consumer behaviour from desktop to mobile has clearly been happening for a long time, but there were always more attacks on desktops than on mobile. That's partly because the volume was slowly shifting, but also partly because fraudsters traditionally saw desktop transactions as an easier target because mobile transactions are set within the often more secure framework of a mobile app, with the likes of fingerprint biometrics, for example. In the last six months of 2019, however, mobile attacks outpaced desktop attacks by volume for the first time.

Q Mobile usage has exceeded desktop for some time now. Why is it only just recently that fraudsters have decided to target this platform more than desktop?

A One of the reasons it happened in this period is because we did see a big growth of global bot attacks primarily targeting mobile app registrations, so it might be that in the first six months of 2020 we see those attack volumes edge back towards desktop again. However, a mobile bot attack, in itself, indicates a clear shift in fraudsters' approach. We've seen big, automated bot attacks in the network consistently over the last few years and the fact that fraudsters are now using bots to target mobile applications indicates a change in their behaviour.

Q What does this mean for organisations and how they approach cybersecurity?

A Any one individual solution can eventually be broken by fraudsters, but layering up multiple tools together is a really good way to protect organisations and their customers. Most organisations have been thinking about mobile security for a number of years now, but there are some evolving technologies that are really interesting, particularly in the context of regulation. One of the most innovative emerging technologies at the moment is behavioural biometrics. That doesn't refer to fingerprint or iris scanning, but rather identifying high-risk behaviour from the way users interact with their devices. On mobile, this could mean the way they swipe, hold their phone or touch their screen. All these pieces of information can be combined to understand and identify risk, and be used in the future as one component of a strong customer authentication workflow to support the second European Union Payment Services Directive (PSD2).

Rebekah Moody
Director, Fraud and Identity
LexisNexis® Risk Solutions

Q What have you been able to learn about the way fraudsters operate?

A Last year we started tracking individual fraudsters using their digital identity and we found they were operating across multiple organisations within our network. In our latest report, we took our analysis a step further by visualising the pattern of when a device that had been associated with a confirmed fraud event at one organisation had then been seen at another organisation. By connecting these events, we were able to see this huge network of interlinking fraudulent activity. We broke those networks down into specific smaller networks that we see operating across particular regions or industries. The global network we mapped out had around 73,000 devices that were associated with a fraudulent event at one organisation and then recorded at another. During just a one-month period, those transactions amounted to more than $40 million of monetary exposure to this network of cross-organisational fraud. It feels like if they can work in that kind of advanced and interconnected way globally, they must have a very advanced set-up and process. This networked concept of fraud was a real eye opener.

Q How is LexisNexis Risk Solutions helping companies deal with this network of fraudsters?

A It takes a network to fight a network and so we are building that through what we call the LexisNexis® Digital Identity Network®, which is a crowdsourced repository of digital identity intelligence harnessed from these billions of global transactions. With each transaction we can look at numerous pieces of information, such as the device integrity, location data, user behaviour and whether there is any threat intelligence associated with the online transaction. From all these insights we are able to build a digital identity for each user and our technology can then flag if any activity seems inconsistent or unusual.

We are using all of the individual components of someone's digital identity, stitching them together and using that as a baseline to analyse and understand whether transactions are high risk or trusted. On top of that there are many other components we layer in for additional security. We have numerous physical identity solutions that customers can use, either in know-your-customer, or KYC, requirements or to verify the physical identity of a user, as well as a decision platform, which incorporates machine-learning tools and advanced behavioural analytics to better model fraud risk. We're then developing new and innovative solutions such as behavioural biometrics, which we recently launched, to layer in additional data about how users interact with their devices.

This holistic solution allows us to detect the macro attacks, like automated bots, as well as the individual attacks on customer accounts, and even social engineering attempts. A key challenge for financial institutions at the moment is fraudsters targeting customers by calling them, impersonating the bank, playing on their fears by saying their account has been hacked and then gaining remote access to steal from them. Our system can help organisations detect if this is happening and help them block high-risk behaviour before it jeopardises good user accounts. The ability to compare the physical identity of a user with the digital identity and behavioural information provides a layered solution to protect organisations and their customers.

Mobile attacks outspace desktop for the first time

19BN
Transaction processed

401M
Attack volume

171%
Growth in mobile apps attack rate YOY

Q How do you foresee the cyberthreat landscape continuing to evolve in the coming years?

A We will continue to see this macro to micro trend where attacks are happening on a mass scale, but also an individual scale. That means more mass-scale, global attacks happening across country borders and industries as fraudsters look to maximise their success. In addition, we are likely to see more social engineering attacks, a popular tactic with cybercriminals who often target vulnerable people less likely to detect what is occurring. Being able to identify attacks across this very broad spectrum is important. Fraudsters will always look for the lowest common denominator to attack and generally the customer will be the weakest link in the chain, so it's crucial organisations implement the solutions that really enable them to protect their end-users from the effects of fraud.

For more information please visit www.risk.lexisnexis.com/cybercrime-report

LexisNexis® RISK SOLUTIONS

Commercial feature

Culture triumphs in the race to deal with data privacy

As executives learn to distinguish between data security and privacy, they should build a culture that ensures sensitive information is controlled and handled appropriately

Data privacy has climbed the boardroom agenda in recent years as executives are increasingly alarmed by high-profile examples of companies that have suffered breaches, resulting in exposure of their customers' sensitive, personally identifiable information.

The last ten years have seen enormous data growth. According to analyst firm IDC, the amount of data in the world more than doubled every two years throughout the decade to reach around 40 trillion gigabytes this year, and the rate of growth will continue to accelerate. During that time, the data organisations hold has become something they add to their balance sheets and leverage to support their overall valuation as a business.

The 2010s was also the decade many companies lost the trust of customers because of the way they handled, or mishandled, their sensitive data. Introduction of the General Data Protection Regulation (GDPR) prompted many people to recognise digital versions of themselves are for sale.

Yet while these issues certainly saw data privacy appear on the board's radar, organisations still fail to distinguish between data privacy and data security. Companies have been discussing and purchasing solutions to deal with data security for many years now, but understanding the difference between security and data privacy could help them see why, despite their large investments, breaches continue to occur.

"When boards start to discuss what their data privacy programme is, the answer often comes back as data security," says Kevin Coppins, president and chief executive at Spirion, which provides data discovery and classification tools to help companies protect sensitive personal data. "Understanding that you can have data security without data privacy is relatively new. Data privacy has to have a strong cultural element to it.

"If somebody breaks into your organisation and steals last week's lunch menu, nobody cares. If somebody breaks into your organisation and steals all your partners' and employees' data, suddenly it makes a headline. Although people have done a pretty decent job at data security, the pace at which external and internal bad actors can steal data has outpaced what you can do from a security standpoint.

"New regulations are now forcing organisations to recognise that some data is different and breaches occur because of the speed at which sensitive data replicates. It doesn't just live in a particular database; it lives in every nook and cranny of your organisation and is replicated across cloud servers as fast as the eye can blink. The threat surface has grown exponentially and there hasn't been the same focus on sensitive data components as there has been on building security around the perimeter."

> **Approaching data privacy in the right way requires a culture shift driven from the very top of the business**

Approaching data privacy in the right way requires a culture shift driven from the very top of the business. Firstly, there must be a recognition that the true victim of a data breach is not the company; it's the person whose records were stolen. Breaches can be personally devastating, so the anonymising of victims of data breaches is something that needs to end and the personalisation of breaches needs to begin.

Secondly, C-suite leaders need to shoulder not only the financial responsibility of any data breach, but also the resulting reputational damage and loss of customer trust. That trust, once lost, is very difficult to regain and, if customers are no longer granting access to their data, companies will soon lose their competitive edge. Reputational damage has a far longer-lasting effect than the financial cost of a breach.

"Getting an organisation to understand and personalise data privacy is the responsibility of the C-suite because that's who drives culture," says Coppins. "It needs to be personal. It is the person in the office cube next to you and their kids whose information was stolen, and they will be impacted for the rest of their lives. It isn't just a process or a technology; it's a culture of respecting this concept of privacy and understanding digital privacy is the same as personal privacy.

"At Spirion, data privacy is part of who we are, and until C-suite execs understand the value of reputation and trust, a culture of data privacy is not going to purvey through the organisation and they'll continue to treat any data as any data. A lot of responsibility lives there and it's much more important than setting out a policy or buying a few different vendor tools to say we care about privacy. A cultural shift must happen."

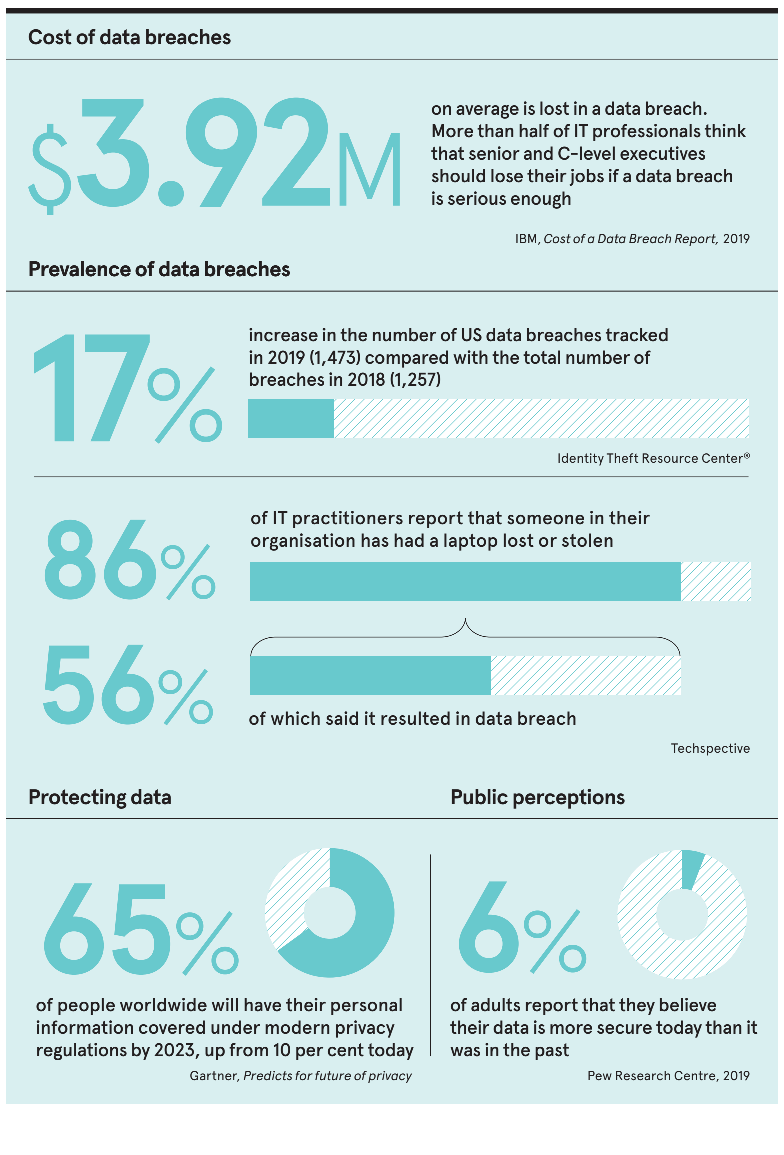
Spirion's technology enables organisations to discover and validate the location of personal information in their information ecosystem, and then classify and control it according to the data protection mandates they're subject to, such as the CCPA (California Consumer Privacy Act), GDPR or even specific contracts. This enables companies to get the big picture of how data flows through the organisation, and gain real command and control over that data.

The company enables organisations to meet the requirements of new data protection laws because creating a data inventory is so fundamental to compliance. It's also central to creating a successful data protection programme. In terms of technical security controls, data classification is foundational to other controls, such as data loss prevention and next-generation firewalls to enforce an organisation's data protection standards.

"Despite the view that breaches are always a result of bad actors, much of the danger to personal data is simply from organisational insiders who mishandle data and expose it to the world," says Scott Giordano, vice president and senior counsel, privacy and compliance, at Spirion.

"Data classification is hugely important, not only to identify sensitive data, but also to help companies build the right culture. Unless personal data protection is engrained in the culture, all the money in the world will not help. The old saying about culture eating strategy for breakfast couldn't be more pertinent."

For more information please visit spirion.com

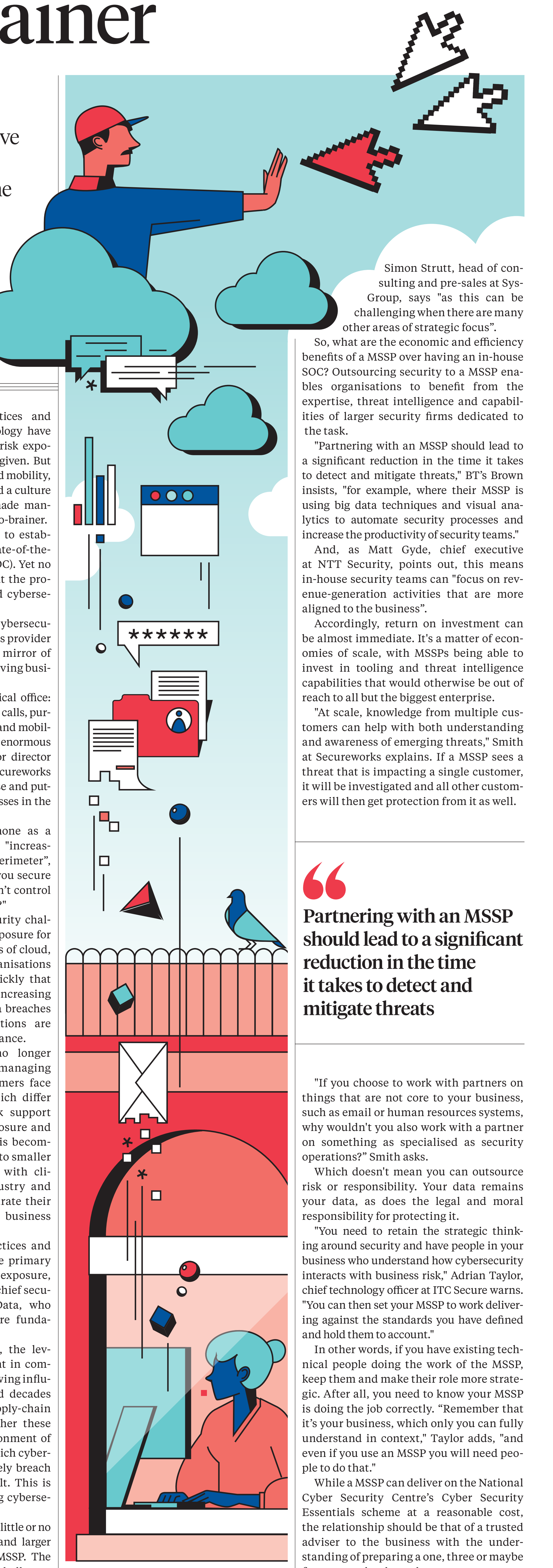


OUTSOURCING

Managed security services are a business no-brainer

Managed security services providers can be transformative for organisations of all sizes, and become trusted advisers in the understanding and awareness of emerging cyberthreats

Davey Winder



Changing business practices and advancements in technology have increased cybersecurity risk exposure for business; that much is a given. But equally, increased connectivity and mobility, evermore reliance on the cloud and a culture of digital transformation have made managed security services a business no-brainer.

Not every business can afford to establish and run a fully staffed, state-of-the-art security operations centre (SOC). Yet no business can afford to be without the protection that such a sophisticated cybersecurity solution provides.

The benefits of outsourcing cybersecurity to a managed security services provider (MSSP) are best reflected by the mirror of risk management in a rapidly evolving business environment.

Imagine a typical day in a typical office: email, expense reports, conference calls, purchase orders and so on. The cloud and mobility, "two small words that belie enormous complexity", as Don Smith, senior director of cyber intelligence at MSSP Secureworks puts it, are extending the enterprise and putting many of these business processes in the hands of an external provider.

Just the rise of the smartphone as a business tool has created an "increasingly intangible, amorphous perimeter", he says, before asking: "How do you secure yourself in a world where you don't control everything, anything, absolutely?"

Let's consider the biggest security challenges that are increasing risk exposure for the average business: the three Cs of cloud, cyber and compliance. Many organisations have moved to the cloud so quickly that their security hasn't kept up. The increasing number of cyberattacks and data breaches reveals that criminal organisations are aware of this. Plus, there's compliance.

"Just being compliant is no longer enough," warns Kevin Brown, managing director of BT Security. "Customers face increasingly stringent rules which differ between geographies, and seek support to understand their current exposure and help remedy issues." The latter is becoming increasingly important even to smaller organisations, especially those with clients in a highly regulated industry and who need to be able to demonstrate their cybersecurity credentials to do business with them.

You need to look beyond practices and technology when it comes to the primary factors that are impacting risk exposure, according to Charl van der Walt, chief security strategy officer at SecureData, who argues the important drivers are fundamental and systemic.

He cites criminal innovation, the levels of state-sponsored investment in computer hacking developments, growing influence of security regulations and decades of large-scale, accumulated supply-chain risk and technical debt. "Together these systemic factors create an environment of chaos and unpredictability, in which cyberattack, compromise and ultimately breach are inevitable," says van der Walt. This is where the benefits of outsourcing cybersecurity come in.

Both smaller organisations with little or no current cybersecurity capability and larger enterprises are a good fit for a MSSP. The larger enterprise can address the challenges of scale and volume, helping their internal security teams "to be more efficient without the need to increase headcount or overwork employees", according to Eoin Keary, co-founder and chief executive of edgescan.

For smaller organisations without a dedicated IT team, let alone a dedicated security team, there's an obvious benefit in outsourcing cybersecurity. But even those in the middle ground, with an existing security team, will find it helpful as a "means of staying on top of the key emerging threats", Simon Strutt, head of consulting and pre-sales at Sys-Group, says "as this can be challenging when there are many other areas of strategic focus".

So, what are the economic and efficiency benefits of a MSSP over having an in-house SOC? Outsourcing security to a MSSP enables organisations to benefit from the expertise, threat intelligence and capabilities of larger security firms dedicated to the task.

"Partnering with an MSSP should lead to a significant reduction in the time it takes to detect and mitigate threats," BT's Brown insists, "for example, where their MSSP is using big data techniques and visual analytics to automate security processes and increase the productivity of security teams."

And, as Matt Gyde, chief executive at NTT Security, points out, this means in-house security teams can "focus on revenue-generation activities that are more aligned to the business".

Accordingly, return on investment can be almost immediate. It's a matter of economies of scale, with MSSPs being able to invest in tooling and threat intelligence capabilities that would otherwise be out of reach to all but the biggest enterprise.

"At scale, knowledge from multiple customers can help with both understanding and awareness of emerging threats," Smith at Secureworks explains. If a MSSP sees a threat that is impacting a single customer, it will be investigated and all other customers will then get protection from it as well.

> **Partnering with an MSSP should lead to a significant reduction in the time it takes to detect and mitigate threats**

"If you choose to work with partners on things that are not core to your business, such as email or human resources systems, why wouldn't you also work with a partner on something as specialised as security operations?" Smith asks.

Which doesn't mean you can outsource risk or responsibility. Your data remains your data, as does the legal and moral responsibility for protecting it.

"You need to retain the strategic thinking around security and have people in your business who understand how cybersecurity interacts with business risk," Adrian Taylor, chief technology officer at ITC Secure warns. "You can then set your MSSP to work delivering against the standards you have defined and hold them to account."

In other words, if you have existing technical people doing the work of the MSSP, keep them and make their role more strategic. After all, you need to know your MSSP is doing the job correctly. "Remember that it's your business, which only you can fully understand in context," Taylor adds, "and even if you use an MSSP you will need people to do that."

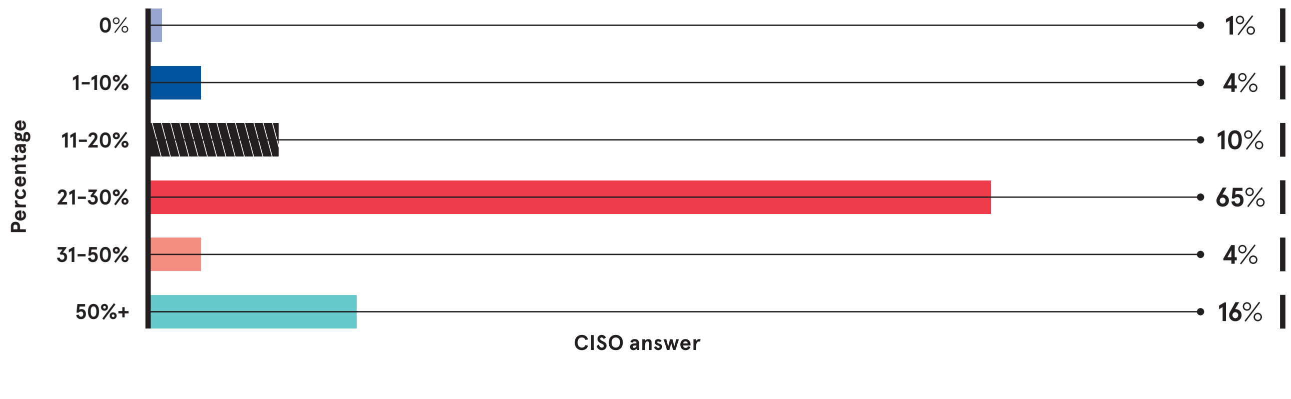
While a MSSP can deliver on the National Cyber Security Centre's Cyber Security Essentials scheme at a reasonable cost, the relationship should be that of a trusted adviser to the business with the understanding of preparing a one, three or maybe five-year technology plan.

As Ian Thornton-Trump, chief information security officer at Cyjax, concludes: "Improving customer security through controls and a technological roadmap is truly the win-win cybersecurity scenario everyone is in need of." ●

OUTSOURCED CYBER OPERATIONS

Percentage of operations outsourced to external provider, according to CISOs from large companies

Deloitte 2019



Manny Pantoja/Unsplash

CORONAVIRUS

Cashing in on coronavirus in the WFH era

With the whole nation working from home, cyber hackers are looking to exploit vulnerabilities in an attempt to steal valuable information

Oliver Pickup

Think very carefully before clicking on a tempting link purporting to be from the World Health Organization (WHO), or similar, with positive information about the cure for COVID-19. Chances are it'll be a hacker preying on your understandable anxiety about the coronavirus pandemic.

In haste to uncover the supposed good news you could inadvertently reveal personal and professional secrets. Indeed, in these strange times, when it comes to cybersecurity, it's worth stopping and asking yourself: "WHO – can you trust?"

As millions of us scramble to make sense of this black swan event, and home-working becomes the new normal, criminals are seeking to capitalise on the widespread panic – and succeeding, alas. New coronavirus-themed phishing scams are leveraging fear, hooking vulnerable people and taking advantage of workplace disruption.

Data from artificial intelligence endpoint security platform SentinelOne shows that from February 23 to March 16 there was an upward trend of attempted attacks with peaks at 145 threats per 1,000 endpoints, compared to 30 or 37 at the start of that period.

"The most effective phishing attacks play on emotions and concerns, and that coupled with the thirst for urgent information around coronavirus makes these messages hard to resist," says Luke Vile, a cybersecurity expert at PA Consulting. "Societally, we've never experienced this situation before, so all rules are off in terms of how people behave. While there is an intense urge to react to good news, it is risky."

In the UK alone, victims lost over £800,000 to coronavirus scams in February, reports the National Fraud Intelligence Bureau. One unlucky person in particular was left £15,000 lighter after buying face masks that never arrived. Who would confidently guess at the March figure?

Banking trojan malware is masquerading as a WHO-developed mobile application helping individuals recover, or virtual private network (VPN) installers. And consider that Check Point research shows some 4,000 COVID-19 domains have been registered this year, many likely fronts for cybercrime.

"So-called 'scareware' will only ramp up as uncertainty rises and online searches increase as people seek information about the outbreak and solutions," predicts Terry Greer-King, vice president of Europe, Middle East and Africa at California-headquartered cyber organisation SonicWall. "In 2019, malware and ransomware took a fall, 6 per cent and 9 per cent respectively. Now they are coming back because of the global health crisis."

Proofpoint senior director Sherrod DeGrippo notes that cybercriminals have "sent waves of emails that have ranged from a dozen to over 200,000 at a time", and the number of campaigns is "trending upwards". He says: "The COVID-19 lures we've observed are truly social engineering at scale.

"They know people are looking for safety information and are more likely to click on potentially malicious links or download attachments. Approximately 70 per cent of the emails Proofpoint's threat team has uncovered deliver malware and a further 30 per cent aim to steal the victim's credentials."

Dave Waterson, chief executive of SentryBay, a UK-based company specialising in software to protect applications and endpoints, notes that COVID-19-infected bodily fluids are selling for just $1,000 (£850) on the Dark Web. He forecasts that cyberattacks will rise by "up to 40 per cent" during the coronavirus pandemic.

As working from home becomes more predominant he warns: "It is down to organisations to ensure any endpoint that an employee is using is fully protected. And as the Absolute 2019 Global Endpoint Security Trend Report showed, 42 per cent of endpoints are unprotected at any given time."

Worryingly, Apricorn research published last year found that one third of IT decision-makers admitted their organisations had suffered a data breach as a result of remote working. Further, 50 per cent were unable to guarantee that their data was adequately secured when being used by remote workers.

The surge in virtual conferencing and other collaboration tools could expose more vulnerabilities for hackers to exploit. "Companies quickly adopting consumer-grade video conferencing can make it easy for an attacker to pretend to be a member of staff," points out Elliott Thompson, principal cybersecurity consultant at SureCloud. "The industry is going to have to be dynamic and responsive on this front – as we always try to be."

What, then, can businesses and their workers do to shore up their cybersecurity? The government's National Cyber Security Centre published a home-working guide earlier this week that offers tips for organisations introducing home-working as well as highlighting the telltale signs of phishing emails.

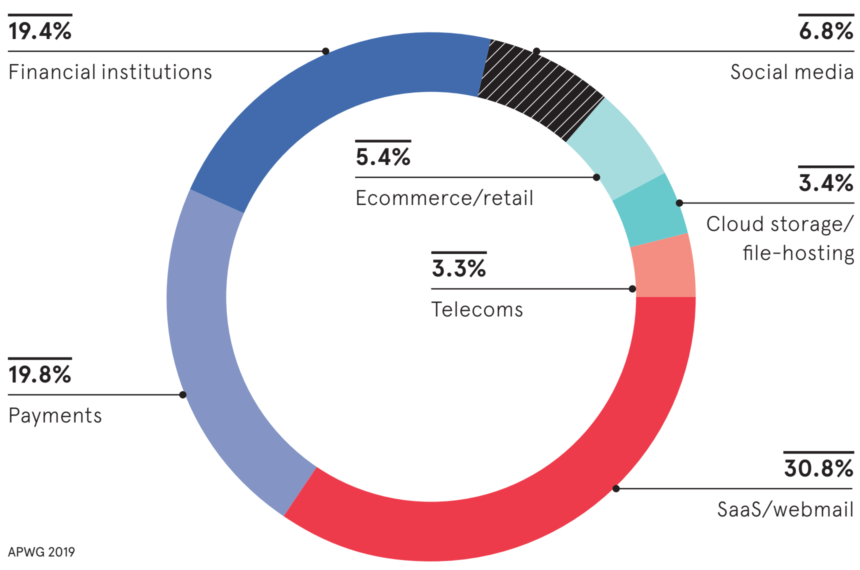
Robert Krug, the network security architect for antivirus software giant Avast, offers more evocative advice. "Computer viruses can spread just as easily as human viruses," he says. "Just as you would avoid touching objects and surfaces that are not clean, so should you avoid opening emails from unknown parties or visiting untrusted websites.

"In short, the same steps that one takes to ensure they don't get sick should be translated into steps that keep devices and networks secure. You may use hand sanitiser to remove germs from your hands, and you should have an effective antivirus solution to keep germs off your computers and networks."

You have been warned. ●

MOST TARGETED SECTORS BY PHISHING ATTACKS

Share of total phishing attacks directed to the following sectors/industries



APWG 2019

Expert cybersecurity tips for home-working

Embrace quick and inexpensive wins
"Enable multi-factor authentication wherever possible, adding another layer of security to any apps you use," says Jeremy Hendy, head of Skurio. "Additionally, a password manager can help avoid risky behaviour such as saving or sharing credentials. Both types of products offer cost-effective solutions for organisations."

Go private
Roy Reynolds, technical director at Vodat International, says: "Having a VPN solution, which sits on the PC, laptop, or mobile device and creates an encrypted network connection, should be encouraged. A VPN makes it safe for the worker to access IT resources within the organisation and elsewhere on the internet."

Update cybersecurity for home-working
"Does your current cybersecurity policy include remote working?" asks Zeki Turedi, technology strategist at CrowdStrike. "Ensure the policy is adequate as your organisation transitions to having more people outside the office. They need to include remote-working access management, the use of personal devices, and updated data privacy considerations for employee access to documents and other information."

Only use work devices
"Communicate with colleagues using IT equipment provided by employers," warns Luke Vile of PA Consulting. "There is often a range of software installed in the background of company IT that keeps people secure. If a security incident took place on an employee's personal device, the organisation – and the employee – may not be fully protected."

Tighten up network access
Daniel Milnes, an information lawyer at Forbes Solicitors, says: "Without the right security, personal devices used to access work networks can leave businesses vulnerable to hacking. If information is leaked or breached through a personal device, the company will be deemed liable."

Commercial feature

Coronavirus tests security systems and policies

James Arthur, partner and head of cyber consulting at Grant Thornton, shares tips for cyber-resilience as an unprecedented volume of UK employees work from home during the COVID-19 outbreak

Q How is the COVID-19 outbreak affecting companies from a cybersecurity perspective?

A Many organisations haven't really adopted agile or remote working before, but are now effectively being forced to tell employees to work from home. One of the big risk factors, especially when companies share data with external parties, is the security of end-devices. If a device is within your corporate policy, it hopefully has the basics such as patching, anti-virus, monitoring and a secure VPN already configured. But if staff or suppliers are connecting from a third-party device, including personal computers, they are much less likely to have the same protections. This can open companies up to the same range of threats as home users, such as unsecured wifi and routers that haven't had their default passwords changed. By doing so, companies are increasing their potential attack surface and are increasingly vulnerable to the kinds of opportunistic cybercriminals who look for easy targets.

Q How important is it that organisations consider cybersecurity a core business risk, rather than just something IT is worrying about?

A We've been saying for some time now that businesses should always think of cyber as a core business risk, not just something for IT to worry about. Our own research found that three out of four mid-market firms have suffered some kind of cyberattack in 2019, and that was prior to COVID-19. The board must view cybersecurity as an ongoing risk and be aware that 80 per cent of all known threats can be fixed with basic cyber hygiene. This isn't about telling companies they need to spend millions on expensive software. People tend to be the soft underbelly of organisations, so it's simply about making sure those who are working remotely have sensible, pragmatic and proportional controls in place and are aware of the threat.

Q What is your advice to companies in terms of what controls should be?

A The natural response will often just be to make sure everything is available remotely, but blanket access could have damaging consequences. On the flip side, trying to lock down access to everything is not the right approach because employees still need to be productive and many will find ways around it anyway. Instead, companies must think carefully about what access they really need to provide and how they're monitoring that. They also need to ensure they have an incident response plan in place. The cyberthreat level is likely to increase further before it returns to normal, but if you have a strong incident response plan that can work remotely then you're in a much stronger position.

Q Beyond these physical controls and systems, how can organisations ensure staff are aware of the right things to do while working from home?

A Awareness is vital. The entry point to many attacks or breaches is staff simply not paying attention to a password policy, not patching their systems or falling for various phishing emails. We're seeing a big increase in cybercriminals enticing people to open links posing as important information relating to COVID-19, so it's important they know how to spot them. A lot of this must come from top-down leadership and impactful messaging. You have to find ways to efficiently communicate with and engage your staff, and make sure people are leading by example. It may be that a short phone call from seniors or team leaders is much more effective than emails that are going to be ignored.

Q How is Grant Thornton helping companies deal with cybersecurity through this challenging period?

A We're absolutely advising prudence, not panic, and we're able to support companies both proactively and reactively. Proactively, we help them understand their risk and identify pragmatic and proportionate steps to reduce this. On the reactive side, we have a large incident response team to help people who think they may have been hacked. The key is quickly understanding if there has been a real compromise and, if so, what data has been affected. Our experienced investigators use forensic techniques to tell you exactly what has been touched. However, it's most important to reiterate that COVID-19 is not the first major risk businesses have faced and it won't be the last. This just reinforces the importance that cyber is aligned to core business resilience at all times.

James Arthur
Partner and head of cyber consulting
Grant Thorton

For more information please visit grantthornton.co.uk/services/risk/cyber-advisory

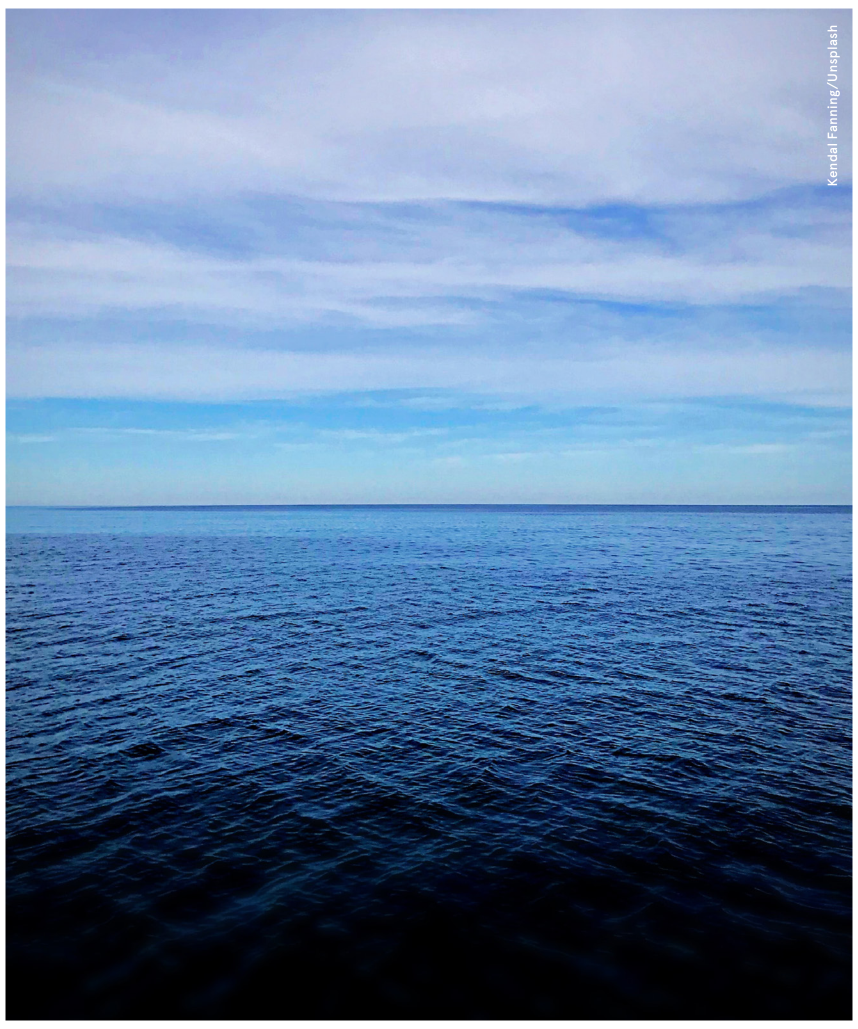
Grant Thornton

FUTURE THREATS

Five cyberthreats on the horizon

Cybersecurity is an ever-changing game requiring information security professionals to keep abreast of the evolving threat landscape. Here are five emerging risks to keep an eye on

Davey Winder


Kendal Fanning/Unsplash

Deepfakes

Deepfakes combine existing video images along with whatever the creator of this artificial intelligence-driven synthesis wants the person to be saying. These are likely to be used against banks, according to Tim Dunn, commercial director at ValidSoft. "As deepfake technology evolves, it will represent an advanced method of social engineering," he says. “The widespread use of web and app-based video channels will provide the opportunity for advanced deepfakes to fool both agents and AI bots alike." It seems the best bet when it comes to future mitigation will be biometric voice synthesis detection that can identify the fakes.

Counter-incident response

Staying inside the target network is key to a successful cyberattack; the longer they are in, the more they can get out. Counter-incident response does what it says on the tin: it turns off antivirus, firewalls, anything that might trigger detection. "The longer they have to achieve their goal, be that lateral movement, island hopping further up the supply chain or data collection, the better chance they have of success,” says Rick McElroy, head of security strategy at Carbon Black. Mitigation will have to include machine-learning-powered technology to filter the noise in incident reporting so security analysts can respond to the real events as quickly as possible.

Automated attack methodology

Just as security operations centres are starting to apply intelligent automated incident response filtering, so criminals are finding that automated attack methodology works well on their side of the security fence. "Automated, active attacks are escalating and causing massive damage to organisations that have been targeted," says Chester Wisniewski, principal research scientist at Sophos. They begin with automated mass reconnaissance scans and basic malware infections, with human involvement coming later to see what's been caught in the net. "These are essentially criminal penetration tests," Wisniewski warns. Mitigation? Keeping your cybersecurity emergency basics in place.

Big game hunting

Rather than adopt a scattergun approach of automated malware infection, big game hunters take their time to target key organisations for the best return. The weapon of choice is ransomware, which employs well-tested and human-powered reconnaissance, delivery and lateral-movement tactics, techniques and procedures. "The wider e-crime network has been seen to be leveraging this approach more widely," explains Zeki Turedi, technology strategist at CrowdStrike. ”As a highly devastating yet effective tactic, we can only see this continuing." Mitigation requires proactive monitoring for indicators of attack by capturing all raw events to detect malicious activity not identified by traditional prevention methods.

Disinformation

Disinformation is the deliberate act of providing and spreading inaccurate information with the aim of manipulating perceptions and influencing decisions be they political or business in nature. "Lies are a fact of life," says Rodney Joffe, former cybersecurity adviser to the White House and currently senior vice president and fellow at Neustar. "But the Internet has enabled this to occur at scale with close to 100 per cent reach." Lack of jurisdiction and absence of physical validation makes it almost impossible to tell truth from lies. "The best we can do is continually develop methods of validation and authentication, and ensure this is part of every process, both commercially and personally,” Joffe concludes.

OPINION

‘The need and ability to manage risk does not cease at an organisation's boundaries in this increasingly connected world’

Security breaches hit the headlines far too frequently. This makes cybersecurity a priority for organisations worldwide, with global spending expected to swell to $157 billion in 2023, up from $60 billion in 2019.

Add into this that the worldwide installed base of internet of things devices is set to total nearly 35 billion units this year, representing 35 billion chances for hackers to compromise security. In the rush to bring new mobile products and services to market, security and privacy were at best an add-on to development and at worst ignored completely. The cybersecurity headache for executives gets even bigger.

Even though enterprise boards are more than aware of the need for a strong cybersecurity posture, just 11 per cent of organisations have fully implemented a proactive approach to cybersecurity and digital risk, according to a survey conducted by Omdia. Luckily, this situation is changing for the better.

Organisations recognise that handling new risks is a consequence of expanding digitalisation. The need and ability to manage risk does not cease at an organisation's boundaries in this increasingly connected world. For digital risk, adversarial and accidental threats are grouped together to become the focus of consideration; examples include organised criminal groups, nation states, malicious insiders and accidental insiders. In this context, an "insider" is anyone with access to organisational systems that an outsider would not have.

Regulation has played a big role in effecting change. The European Union’s General Data Protection Regulation, the California Consumer Privacy Act and dozens of other pieces of legislation around the globe have driven data protection up the list of importance. In turn, regulations have raised standards and visibility among company decision-makers, backed up by imposing sanctions on companies that suffer security breaches by failing to take cybersecurity seriously enough.

On the consumer side, there is also growing security awareness. This doesn’t necessarily mean consumers are practising security-positive behaviour, but it does mean they are more attuned to security incidents and breaches when they hit the headlines. Opportunistic litigators are launching claims against companies. With this increasing consumer awareness, enterprises that have suffered breaches can incur reputational damage, lose customers, receive regulatory fines, face legal action and see a temporary or longer-term impact on share price.

Enterprises must continue to pursue digital transformation projects with the objective of improving the products and services they provide to customers. However, such projects must go hand in hand with assessing the associated risks and deciding between acceptance, mitigation and transference of the identified risks.

Security technology vendors and service providers have some highly sophisticated capabilities in their arsenal. But presenting these capabilities as all-encompassing would be a mistake. Instead, enterprises want to know how a security product or service improves their security posture as part of the overall security controls deployed by the organisation. ●

$157bn

estimated global spending on cybersecurity in 2023, up from $60 billion in 2019

35bn

estimated global spending on cybersecurity in 2023, up from $60 billion in 2019

11%

of organisations have fully implemented a proactive approach to cybersecurity and digital risk

Maxine Holt
Research director, cybersecurity
Omdia

Commercial feature

Evolution demands revolution: embracing secure digital transformation

Across major enterprises, technological change provides the opportunity to evolve, but it also introduces the unknown. Companies can embrace this through understanding and managing their cyber risk

Digital transformation is a regular business reality. Where market forces and changes in business models used to evolve over decades, now companies must continually address what they do and how they operate to remain competitive. This requires organisations to innovate and embrace new technologies and ways of working.

The risks and challenges that come with digital transformation must not be overlooked. Many large organisations still have legacy systems that are decades old, which means changing and, importantly, securing them is no trivial effort.

Augmenting these proven capabilities with market-leading businesses tools, such as advanced analytics, automation and artificial intelligence, can introduce significant risks that companies are not prepared for. Many industries have seen complete disruption in the way they operate and in their level of technology reliance, with the pace of change set to continue.

The prospect of managing this change and tackling new and unknown threats can cause some risk-adverse companies to defer from embracing technology transformation altogether. According to Cybersecurity Ventures, cybercrime damages will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015.

While such caution may limit their exposure to cyber threats in the short term, the long-term damage from having failed to adapt the business for the digital age could potentially prove fatal. Companies must undoubtedly transform, but learn do so in a secure way.

Managing cyber risk

“Nothing quite vaporises enterprise value as quickly as a cyber incident,” says Richard Hanlon, chief commercial officer, Europe, Middle East and Africa (EMEA), at Aon's Cyber Solutions. “As companies go through these transformations, greater cyber resilience isn't going to be achieved solely through technology, governance or compliance. They have to look at it as an iterative process with no straight line or singular approach and adopt a holistic view to cyber risk management.

“Many organisations, of course, want to insure the risk to get it off their balance sheet, but don’t take a step back to ensure they've adequately assessed their risks, vulnerabilities and put appropriate programmes in place.

“This is a process issue and data becomes key. A more holistic approach recognises there is a valuable data ecosystem available within the various assessments, risk quantifications and responses to cyber incidents. The more organisations leverage those insights to dynamically assess the threat and, importantly, do something about it, the more cyber resilient they become.”

Cyber risks are inescapable. No organisation will ever be able to eradicate cyber threats or remove the risk of reputational damage should an incident occur. For those organisations that recognise increasing their security is part of an ongoing and iterative process, management of this risk does become achievable.

Aon partners with companies throughout this journey and can engage at any given touch point, whether that is assessment, quantification, insurance or incident response. This works best when companies are active participants in managing risk and engaged in a greater ecosystem of continuous review, improvement and investment in cyber risk management. Aon refer to this as the “Cyber Loop”.

Given this rate of change and the scale of increased threat, many organisations are unsure of whether they are doing enough, too much or taking the wrong approach entirely. Clearly, tackling this challenge is unique to each environment, but every company must first accept the risk exists and that it cannot be dealt with through any single measure.

Once organisations have gained an understanding of their cyber risk, they can start to manage it. This is achieved through building a robust cybersecurity programme, which includes developing the right polices and processes, deploying the right tools and aligning all the capabilities that form part of their efforts to protect against the risk.

Utilising technology

“It is hugely advantageous to utilise advanced tools, techniques and monitoring capabilities,” says Kraig Rutland, vice president, EMEA, Cyber Security, at Aon's Cyber Solutions. “Having said that, many organisations make considerable investments, but struggle to align them to their actual risks, which is where we are often engaged.

“In one use-case, we may work with a business to understand exactly what they should be monitoring and how they should be monitoring it, helping them use their existing technologies in a way that provides direct visibility of systems posing the highest risk.”

This is not just about monitoring, but how change is delivered. Another example of how Aon works with companies is by supporting their cloud adoption. Organisations are keen to embrace the benefits of cloud infrastructure, but often cautious to migrate critical systems due to the associated cyber risks. Aon helps them to understand those risks and then make the necessary change through managing them accordingly.

“Developing these processes and configuring all these technologies can be difficult, but it all comes down to ensuring your processes, technologies, systems and teams are actively helping you gain visibility or reducing the key cyber risks faced by your business,” says Hanlon. “There is still a need for a much deeper understanding of what the worst-case scenarios are in terms of the financial impacts due to cyber threats and in understanding cybersecurity is not an IT risk, but an enterprise risk.

Rutland adds: “If you're midway through a digital transformation, your business and IT environment are likely to be experiencing constant and rapid change that’s hard to keep on top of.

“Through good practices, many organisations will have tools and processes in place, but they may not be making the most of them and getting the right business insight and reporting to support their operating model. This is particularly true when it comes to incidents. It is one thing being alerted to an incident; it's another having the right processes and procedures to handle that incident effectively. We help refine these processes and improve existing security investments to help tackle cyber risk.”

Human element

Culture can be the most important element of a successful cybersecurity strategy. A company’s biggest strength is also often its greatest weakness: people. Cybercriminals won’t stop to get what they need, including targeting employees to gain access, data or otherwise. A key way to combat this is awareness, which must spread through an entire organisation and start at the top. If C-suite leaders don’t understand they are ultimately responsible for all risk-management efforts, there’s a problem.

This is important when safeguarding not just their operational responsibilities, but also themselves. According to Verizon research, C-level executives are twelve times more likely to be pursued by cybercriminals and nine times more likely to be victimised, typically by social engineering techniques, for influence, reputational damage, access to data or 71 per cent of the time for financial reward.

“The culture has to permeate out of the boardroom to the C-suite and then trickle down,” says Hanlon. “Yet too often we are called in by chief information security officers (CISOs) because senior colleagues are not fully appreciating that cyber awareness needs to be deeply embedded into organisational culture. Active engagement, support and sponsorship from the most senior levels within a business are critical to tackling the cyber risks and unlocking the necessary culture required to enable secure technological change.”

As businesses navigate ongoing digital transformation, assessing, understanding and managing cyber risk requires a wide range of competencies. Aon leverages a combination of experiences comprising technical acumen, analytics and business risk to support cybersecurity and risk-management objectives, enabling secure transformation.

For more information please visit www.aon.com/cyber-solutions

Richard Hanlon
Chief commercial officer, EMEA
Aon's Cyber Solutions

Kraig Rutland
Vice president, EMEA, Cyber Security
Aon's Cyber Solutions