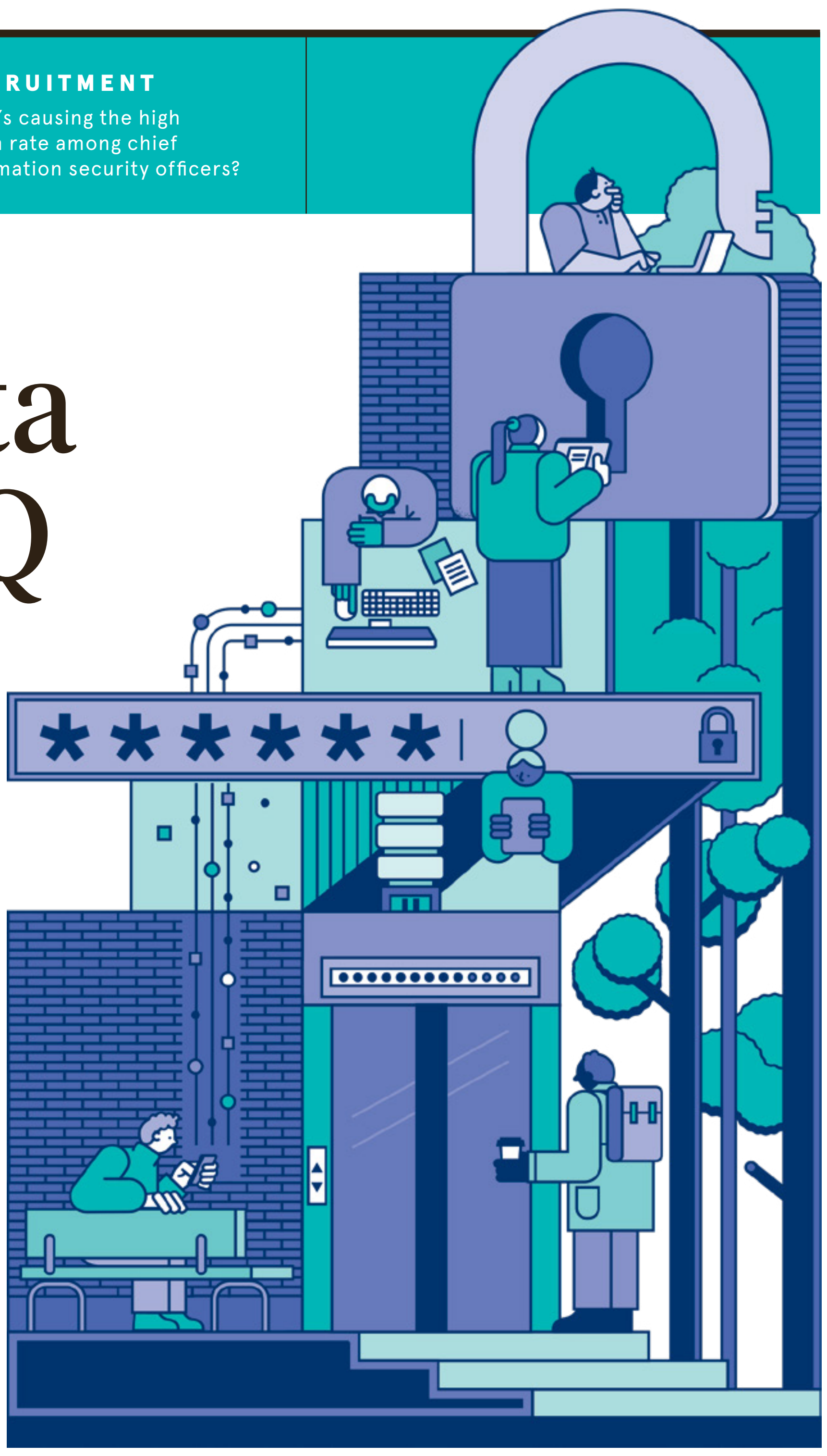
INDEPENDENT PUBLICATION BY

RACONTEUR

RACONTEUR.NET | #0759 | 12/09/2021

CYBERSECURITY



HYBRID WORKING

Suspect device: the data risk coming back to HQ

Workers returning to the office after a long period of remote working represent a potential cybersecurity threat that their employers can ill afford to ignore

Chris Stokel-Walker

When the world changed last year, so did the way that many of us do business. In an instant, the workplace shifted from the purpose-built office to living rooms, kitchens and spare bedrooms throughout the land. It was a cybersecurity nightmare for some companies: 65% of medium-sized UK firms said that they'd had at least one attack or breach in the year to 22 January 2021, according to figures published by the UK Department for Digital, Culture, Media and Sport.

But, as the world of work begins to get back on an even keel and businesses adapt to a hybrid model of home and office working, there are more new risks to face. Well over half (61%) of UK employees use their own mobile phones for work, while 44% use their own laptops, according to a survey by security platform provider Armis.

"People have become comfortable using a variety of connected devices while working at home," says Paul Davis, the company's regional vice-president in EMEA. "The issue of unsecured devices posing a risk to businesses isn't exactly news, but this will be exacerbated by a surge in the number of devices that will potentially connect to corporate networks."

It's a challenge that businesses are facing everywhere. IT company SoPost, which employs 65 people around the world, has always been a hybrid workplace. But the pandemic has obliged employees to do a lot more remote working, reports its founder and CEO, Jonny Grubin. His firm has also hired 35 people during the Covid crisis, so it has ensured that all devices used in the business can be managed remotely. Doing so requires strong leadership.

"From a managerial perspective, there may be issues with how the return to a centralised workspace will be handled," says Abigail McAlpine, a cybersecurity expert at the Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research at Sheffield Hallam University. "How organisations handle the human aspects of security is just as important as their technical work."

> "Security is important, but notifications to update systems may not be a priority to people when they're busy in their jobs

McAlpine recommends that businesses give their employees a crash course in cybersecurity as they come back to the office, even if it's only as part of a hybrid working arrangement. "A lot of things that may seem basic may have felt unnecessary to people working alone and secure at home, such as locking computer screens when leaving their desks or password-protecting their devices," she says.

It isn't just reinstating good cybersecurity habits that businesses might need to do. In the rush to ensure business continuity when the pandemic struck, many workers made do with whatever they could get their hands on – including tablets, phones and laptops that are shared by their family members – and which now hold the keys to a business kingdom.

"Anyone in a position of authority should encourage conversations about the potential security issues with a bring-your-own-device policy [BYOD]," McAlpine says.

SoPost issues its employees with company laptops or desktop computers. "These are supposed to be used for business purposes only, but I'm sure that people may watch Netflix on them," Grubin admits.

But datasecurity is bolstered through a remote device management programme called Jamf, which allows machines to be set up remotely and security patches installed by the company's IT department.

"Security is important, but notifications to update systems may not be a priority to people when they're busy in their jobs," Grubin says. "Jamf enables us to see the status of every device, so we know exactly what applications everyone is running."

The prospect of understanding an entire organisation's cybersecurity needs may seem daunting when businesses are struggling to manage the return to the office. Yet employers are conscious of the risks. Four in 10 firms in a recent survey by web hosting company Ionos admitted that they had cybersecurity skills gaps, for instance.

"Security departments will need to prepare a proactive security plan with specific policies to ensure that staff can continue to use these devices in the office," Davis warns. "It's better to have an extra layer of security than suffer the consequences of a breach."

But that needn't be a significant undertaking, according to McAlpine, who believes that education can go a long way.

"Half an hour of discussion about potential issues, gathering employees' insights, opinions and questions, will provide better opportunities for understanding both the short- and long-term risks," she says.

Indeed, the great working reset is a chance to create a security-conscious culture in an organisation. McAlpine recommends appointing "security ambassadors" to lead the rethinking of cybersecurity matters and to smooth the transition to the new world of work. Above all, she advises placing the issues front and centre in the minds of all staff.

"Security is an element of every employee's role, not just those in IT," she stresses.

Yet it's also vital for organisations to acknowledge the changing world of work. Employees won't always be in the office and under the watchful eye of colleagues and their IT department. As hybrid working takes hold, the movement of devices into and out of offices is inevitable. So a new contract with employees that takes the new realities of working life into account, while keeping things as secure as possible, is important.

"Remote and hybrid working look set to become the norm for millions, so businesses need to ensure that their information security and privacy management systems are overhauled to reflect the changes to the threat landscape," says Steve Lamb, principal consultant at Bridewell Consulting.

It's unrealistic to expect employees not to use their home computers or networks to dip into key work documents, he says. So, instead of barring this practice outright, it's important to control how those devices connect to the corporate network.

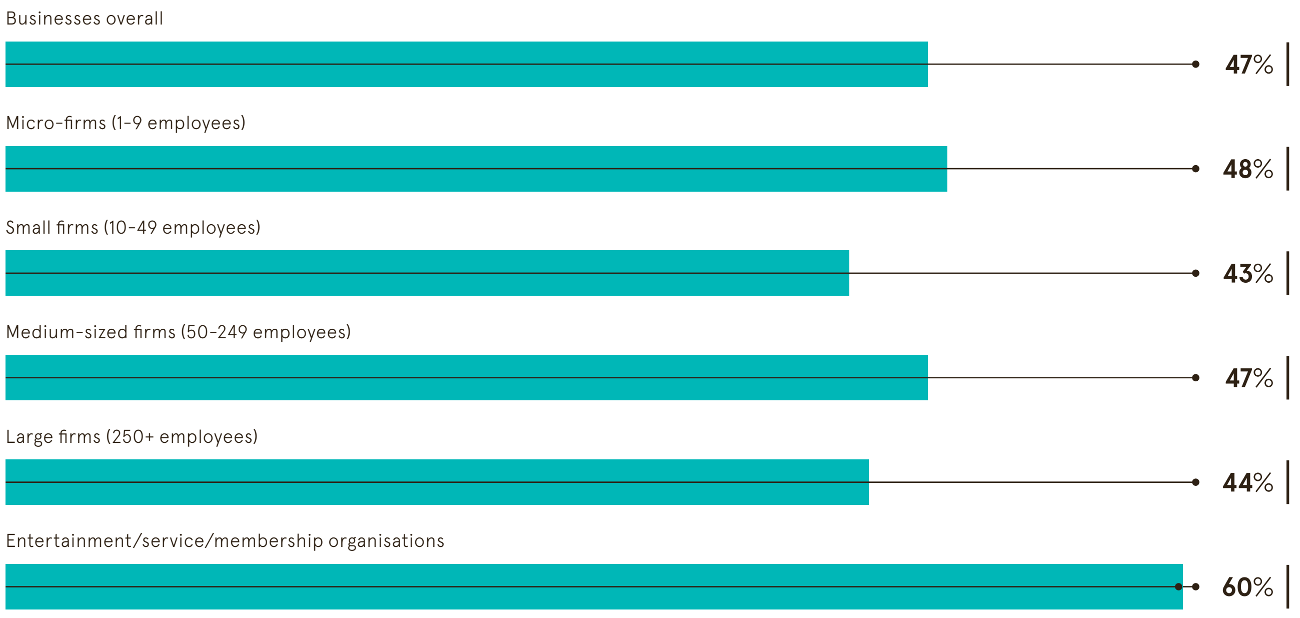
"Organisations will need to prevent employees from connecting to business networks and using any personal devices that don't have basic security controls," Lamb says.

Likewise, it's better to allow employees to access internal networks – where security is likely to be stronger – than to save files locally, according to McAlpine. Loss or misallocation of data is more likely when saving material off work networks. Firms without appropriate BYOD policies will find it harder to track documents when they are shared to different devices.

But a large part of managing the risk entails managing people. "It's a lot about education and conversation," says Grubin, who ensures that all SoPost employees undergo training in data security. It's a model that keeps his company safe – and it could help to secure yours too. ●

WHICH BUSINESSES SUPPORT BYOD?

Percentage of staff in the following enterprises who regularly use their own tech to perform work-related activities



Department for Digital, Culture, Media and Sport, 2021

61%
of UK employees use their own mobile phone for business purposes

44%
use their own laptops

61%
intend to return to the office with their personal devices

Armis, 2021

Distributed in
THE SUNDAY TIMES

Published in association with
info security
STRATEGY | INSIGHT | TECHNOLOGY

Contributors

Sean Hargrave
A freelance journalist
specialising in technology
and digital marketing.

Christine Horton
A long-term contributor to
specialist IT titles, including
Channel Pro and *Microscope*.

Charles Orton-Jones
An award-winning journalist
who was editor-at-large at
LondonlovesBusiness.com.

Chris Stokel-Walker
A journalist and author
specialising in technology
and culture.

Ouida Taaffe
The editor of *Financial World*,
the magazine of the London
Institute of Banking & Finance.

Finbarr Toesland
A freelance journalist
specialising in technological,
commercial and economic issues.

Davey Winder
An award-winning journalist
and author specialising in
information security.

Peter Yeung
An award-winning journalist
with a background in
social anthropology.

raconteur reports

Publishing manager
James Studdert-Kennedy

Managing editor
Sarah Vizard

Deputy editor
Francesca Cassidy

Sub-editor
Christina Ryder

Head of production
Justyna O'Connell

Design and production assistant
Louis Nassé

Design
Pip Burrows
Kellie Jerrard
Celina Lucey
Colm McDermott
Samuele Motta
Nita Saroglou
Jack Woolrich
Sean Wyatt-Livesley

Illustration
Sara Gelfgren

Art director
Joanna Bird

Design director
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 Media

/raconteur.net
@raconteur
@raconteur_london

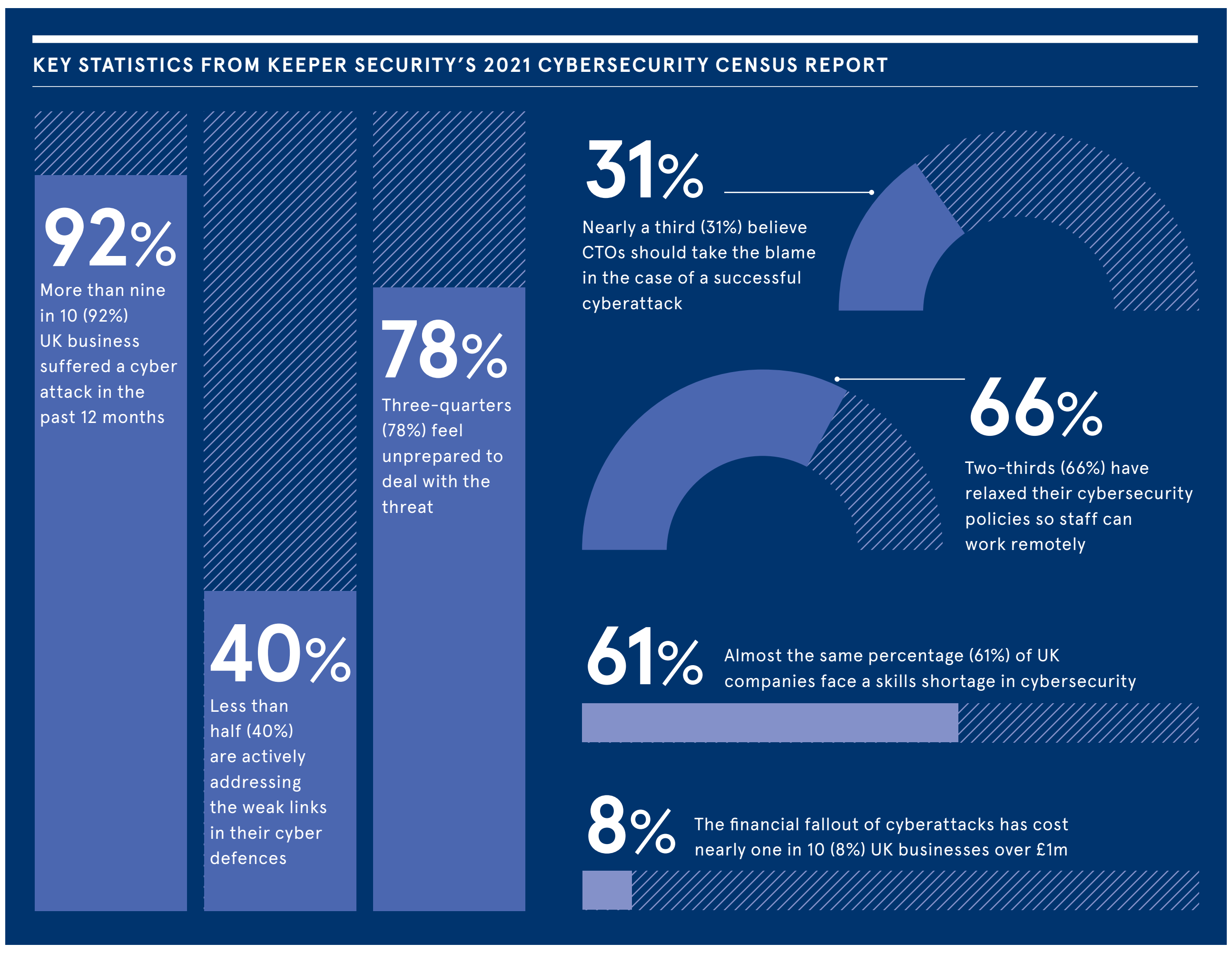
raconteur.net /cybersecurity-2021

Commercial feature

Companies must act now to defend against cyber attacks

With 92% of UK organisations suffering a cyberattack in the past year, business leaders need to be proactive and take greater responsibility. Additionally, the private and public sectors have to work together to combat increasingly successful and entrepreneurial cybercriminals

KEY STATISTICS FROM KEEPER SECURITY'S 2021 CYBERSECURITY CENSUS REPORT



Ransomware has become a massive business which is making cybercriminals billions of dollars, annually. In fact, they have productised it as ransomware-as-a-service (RaaS) which allows entry-level cybercriminals to license powerful software to quickly execute attacks. Even more pervasive and potent are the proficiently organised RaaS cartels who are targeting thousands of companies each month. According to Keeper's 2021 Ransomware Impact Report, after a ransomware attack, 77% reported being unable to access systems or networks as a result, 30% were down for a day and 26% were offline for up to seven days.

Failing to be proactive and work together against increasingly sophisticated cyberattacks can have dire consequences for businesses. New statistics, published in Keeper Security's 2021 Cybersecurity Census Report, attest to the alarming reality.

Some 92% of UK organisations have suffered a cyberattack in the last 12 months, with well over two-thirds (72%) successfully breached more than once. However, fewer than half (40%) are actively addressing all of the weak links in their cyber defences.

The angles of attack are multiplying. Ransomware is becoming much more widely distributed and the barrier to entry is lowering, enabling criminals to easily license and use malware and ransomware.

The advancement and sophistication of technology are now coupled with an increased frequency of attacks and greater collaboration between cybercriminals. Companies must collaborate to defend against these threats.

Why it's imperative to be honest and report attacks

Cybercriminals are outpacing organisations in the cyber arms race. Business leaders must change their mindsets to be transparent about breaches, share knowledge and help one another fight back in this invisible, but critical, field of battle.

Keeper Security examines the core issue: 36% of IT decision-makers have kept a cyberattack on their business secret. There are several reasons why they have remained silent and didn't report it, but it is necessary – for everyone's sake – to be honest and open about attacks in order to fend off future threats.

The lack of reporting is apparent due, in large part, to sheer embarrassment; no one likes admitting to a mistake. Second, those in charge might want to mitigate legal exposure from stakeholders in the event that a significant data breach results in either a series of losses or a class-action lawsuit.

Additionally, there are implications for a business' brand and reputation to consider. This is all on top of the revenue losses and operating expenses arising from ransomware, which make up most of these attacks today.

Those facing the highest levels of risk are small and medium enterprises (SMEs) and small office/home offices (SOHOs), as they usually don't have access to, or budget for, sufficient IT support. SMEs and SOHOs are the low-hanging fruit for cybercriminals. With so many within easy reach it doesn't make sense for criminals to target the larger, better-defended players.

Bearing this in mind, the public and private sectors need to collaborate and come up with solutions to this exploding challenge, and SMEs and SOHOs have to get the support they require to survive in the cyberwar. Simple solutions such as password security systems and dark web scanning can be easily implemented, regardless of the size of the business.

Don't be an easy target: fight back against invisible enemies

Cybercriminals are incredibly smart, well-financed – sometimes by state sponsors – and can be entrepreneurial and collaborative. There is not much difference between the most successful and tremendously impressive cybercrime companies and those that operate legally in the private sector; both earn billions of dollars a year. But cybercriminals are able to work together and stay a step ahead of those businesses, putting pressure on the fragmented defense mechanisms in place.

The dark web is where the cybercriminals operate, and in that encrypted ecosystem they can access over 20 billion stolen correct combinations of usernames and passwords – also known as login pairs. More than 80% of data breaches are the result of password security issues. Most people (60%) reuse weak passwords on multiple apps and websites, giving cybercriminals an opportunity to exploit.

Password management platforms – such as Keeper Security's – that create high-strength, random passwords for every website application system are imperative for businesses. Other assets, like dark web monitoring tools, can detect when credentials floating around on the dark web match something on your network, allowing vulnerable passwords to be flagged and changed.

The 2021 Cybersecurity Census Report indicates that almost one-third (31%) of UK businesses will hold the chief technology officer directly responsible for a successful cyberattack on their organisation.

But blaming the CTO is ineffective. To stand the best chance of survival in the raging cyberwar, you need everyone doing their bit. There has to be c-suite buy-in and excellent cyber hygiene across the whole organisation. Fighting together is the only viable option in 2021.

Five steps to boost your cybersecurity

1 Take accountability – from the top down
Cybersecurity is the responsibility of everyone in an organisation, not just the chief technology officer or chief information security officer or even the IT department. It requires buy-in from the board and business leaders, and cyber hygiene must be tested and improved regularly.

2 A password management platform is essential
Given that weak passwords are by far the number one reason data breaches occur, a password manager – such as Keeper Security – will immediately improve your cybersecurity.

3 Deploy a data breach tool
In addition to a password manager, a data breach tool enables businesses to know when a credential is compromised on the dark web, enabling them to change the vulnerable password before it's too late.

4 Using a VPN is essential when working remotely
The rise of home working in the last year has led to poor cyber hygiene. As a bare minimum, all employees should use a virtual private network.

5 Be open and share knowledge
Cybersecurity software alone is not enough in this cyberwar: business leaders need to change their mindsets and keep abreast of evolving threats. A spirit of openness and collaboration will help boost cybersecurity against criminals, who are outpacing companies in terms of embracing technology and working together.

For more information please visit https://keeper.io/protect

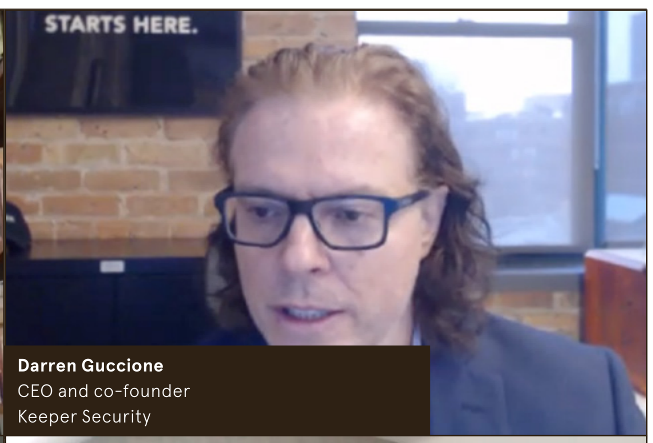
KEEPER
Cybersecurity Starts Here®

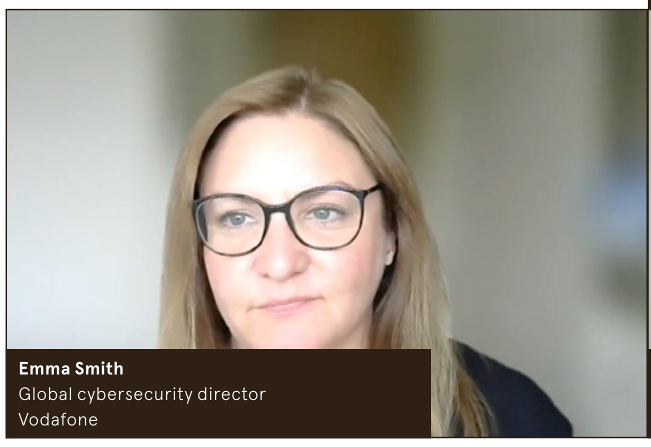
Commercial feature

Cybersecurity in the age of hybrid working

Cybersecurity has to be a high priority for businesses of all sizes in 2021. Most of all, they must share knowledge and collaborate to counter the criminals, who are becoming increasingly sophisticated, according to an expert panel

Adrian Asher
CISO and cloud architect
Checkout.com


Darren Guccione
CEO and co-founder
Keeper Security


Emma Smith
Global cybersecurity director
Vodafone

Shubhanga Prasad
Director, strategy
OakNorth Bank

Helen Rabe
Senior director, global cybersecurity
Abcam

Oliver Pickup

Q What does the cybersecurity landscape look like in 2021?

DG The coronavirus pandemic has been catalytic in forcing organisations to move to distributed remote work environments. This shift served up a buffet table for cybercriminals to ramp up their attacks, which increased from the dark web up to 600%. Ransomware-as-a-service is a huge issue now. It's prolific, pervasive, cartel-based organised crime in the worst and darkest way possible. They are attacking everything and no company, regardless of size or industry, is safe. However, 80% of the attacks are targeted to smaller entities, because of a lack of time and budget, they don't have sophisticated IT architectures or staff.

ES Between companies, we certainly shouldn't be competing in security. All of us need the whole ecosystem of companies – no matter how big, or small – to be secure, resilient to cyberattacks, which will require quite a bit of collaboration and support. We see a continuing increase in supply chain compromise to attack maybe more sophisticated companies, so it's in all of our interests to keep the whole ecosystem as safe and secure as possible. Additionally, smaller companies must understand which services are the most attractive to attackers and which are the most important to protect for their business.

> “Cybersecurity in an organisation should be like a football team; it can't all be left to the goalkeeper, or CISO

AA When, as a society, we went to predominantly working at home, it exposed the inefficiencies of the security logon process; two-factor authentication, for instance, is a poor use of a worker's time. What has become clear is that many firms have cumbersome remote working authentication processes that have impacted productivity. It's been a risk and an opportunity to get on top of that.

HR The circumstances meant we had to engage more proactively with our end users during the pandemic. They came to us with more direct questions about managing cybersecurity in both their professional and personal lives, and it's good that awareness is growing. I have never been a proponent of the statement, 'the human is the weakest link,' and I think the phrasing must change. The human is the one of our primary lines of defence. There is a mindset shift needed so that security becomes a lifestyle choice and that people adopt these behaviours with less reluctance.

SP Ultimately, everyone is responsible for ensuring the cyber defences of the organisation. Great security solutions help put locks in place, but it's a balance. You don't want to impose too much on the users or workers, but you need to be secure. There is no correct answer, but companies must keep calibrating their defences because cyber threats constantly evolve.

Q How has the role of chief information security officer (CISO) evolved over the past 18 months?

ES Cybersecurity in an organisation should be like a football team; it can't all be left to the goalkeeper, or CISO. We need the whole team tackling the opposition at every possible line; otherwise, we'll never win the game. Some basics must underpin the strategy – patching, hardening, vulnerability management, user-access management and passwords. These are all layers that make up a strong security posture. But companies need to be proactive and use detection or threat analysis tools, because prevention is better than the cure. Increasingly, I think the core role of the CISO is to distil a complex topic to something easy for the c-suite to comprehend to drive transparency and reporting on cybersecurity. 'Watermelon reporting' – where something looks green but is red when you slice into it – is not good enough.

HR Traditionally, most CISOs started off technically strong, but now I see many of us as strategic thinkers who can engage and reassure many stakeholders across the business. We're hybridised in our role; we need to understand the technology at some level, but we're not in the grassroots of it. I spent a great deal of my time last year with a lot of end user engagement, for example, advising people working in remote locations on the benefits of using the VPN and guiding them on best practice behaviours that protect our assets. As a result, the collaboration between non-technical business teams and the cybersecurity team has become stronger.

SP CISOs have certainly had to enhance the employees' knowledge of cybersecurity, sometimes across continents. It is a skill to know how to speak to different people at the right level – including the c-suite – so they understand what you need to tell them. We have found that gamifying training has helped engagement.

AA If you speak to your board about cybersecurity, you have to do so in a language they understand. As a CISO, you should always make it easier for people to do the right thing. If you are putting up security controls and people are trying to get around them, your controls are wrong. They have to be as seamless as possible. Ideally, they will be very strong, but completely hidden to not impact productivity.

Q What are the tools businesses need to combat cybercrime?

AA Passwords should be killed as soon as possible, and that includes PINs. It's crazy that we rely on humans to try and remember something that a computer is going to find hard to guess. It's an ineffective use of human computing power. Organisations should be looking to innovate in this area, so there is continuous authentication, zero trust, and session establishment, and it's all seamlessly going on in the background.

SP As a bank, we are hyper-obsessed about our customer experience, and we are looking to innovate around passwords and security. We are working with cybersecurity fintechs to use smartphones for behavioural authentication, allowing access if the user is in the expected geolocation and types in a pattern on their device as expected.

DG Innovation in this space is essential, but for the moment having a password management platform is the first key step to improving cyberhygiene, especially given the proliferation of the cloud and the demand for more strong passwords. It is virtually impossible to create and remember passwords for dozens of different applications from a human perspective. The Keeper Security platform enables the end-user to authenticate into any website app or system in a second without transacting with a password.

HR Cybersecurity training is a critical element, unfortunately it can be soporific and dry, so it needs to engage your end user. Our culture is young and dynamic, so we have boosted engagement in the last year by using anime videos to raise awareness and gain interest in the wider security education and training programme. These have helped to contextualise security, and we extended the training to friends and family, to improve awareness and cyberhygiene. This approach has made a huge difference.

ES In addition to challenges, new technologies also create positive opportunities. For example, 5G connectivity brings high reliability, low latency and new security features.

For more information please visit https://keeper.io/protect

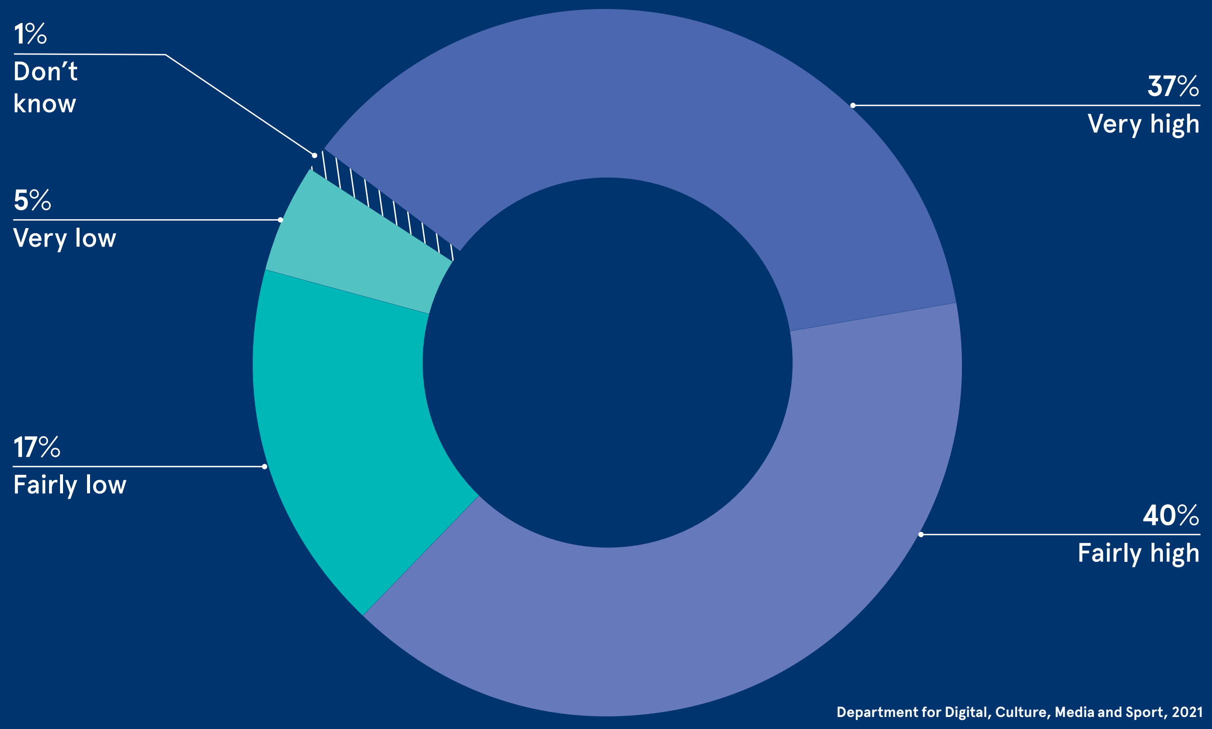
KEEPER
Cybersecurity Starts Here®

PAYING THE PRICE: THE RISE OF RANSOMWARE

Ransomware attacks have rarely been out of the news in 2021, while the rise of ransomware as a service has triggered a further crimewave. Such trends should heighten the stress levels of business leaders, but how prepared are their firms? And how best should they respond if they become victims of such crimes?

CYBERSECURITY IS NOT A MAJOR CONCERN FOR ALMOST A QUARTER OF COMPANY DIRECTORS

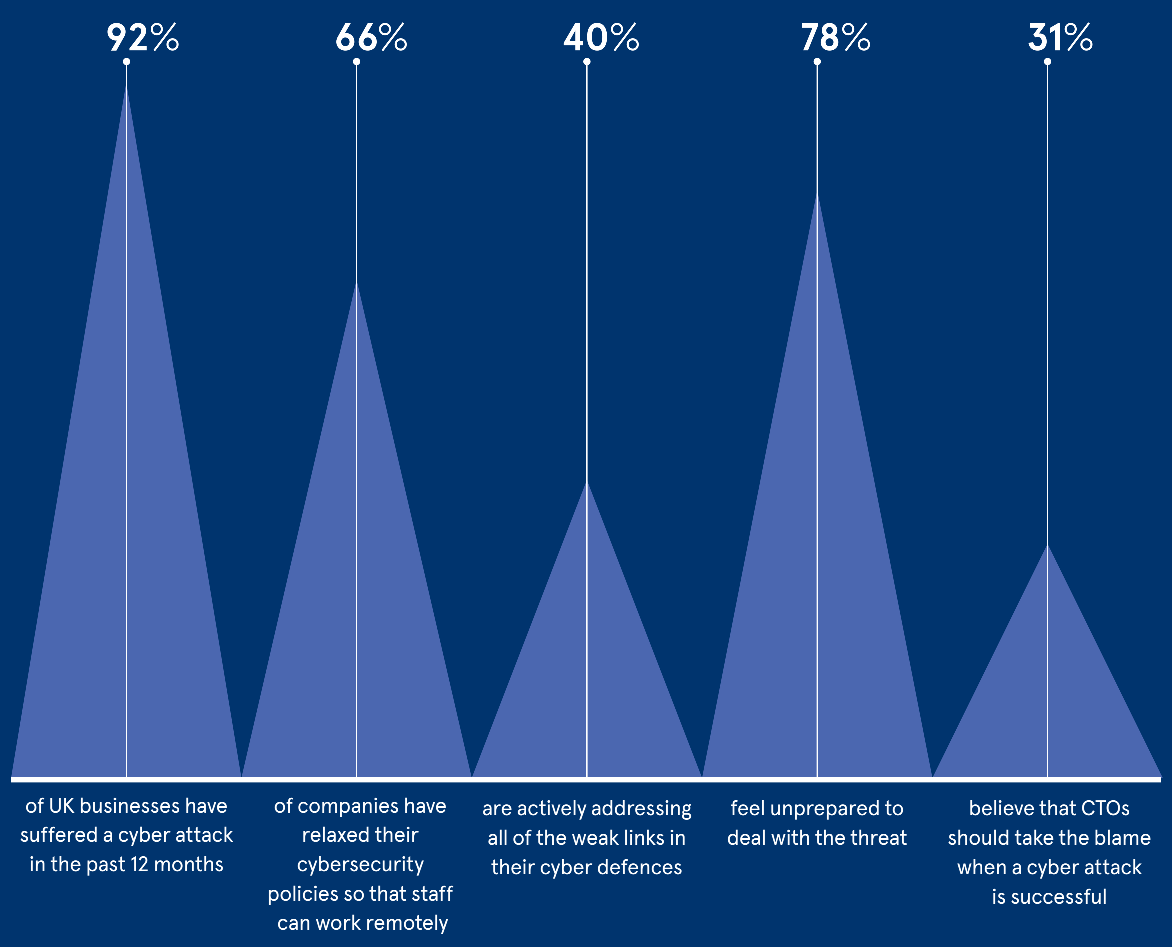
Priority given to cybersecurity by UK business leaders



Department for Digital, Culture, Media and Sport, 2021

THE UK CYBERSECURITY LANDSCAPE

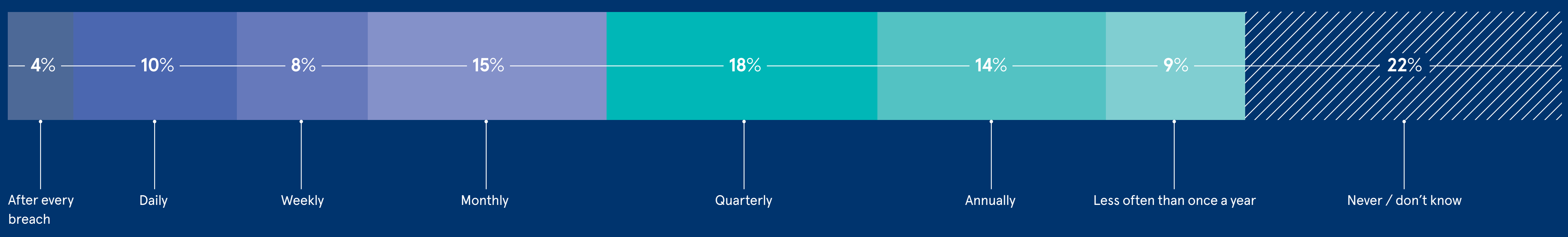
Most organisations have been attacked at least once since the start of the Covid crisis and most don't know how to shore up their defences – or even whose responsibility it is to do so



Keeper Security, 2021

MORE THAN 40% OF SENIOR MANAGERS IN THE UK ARE UPDATED ON CYBERSECURITY MATTERS ONLY ONCE A YEAR, IF THAT

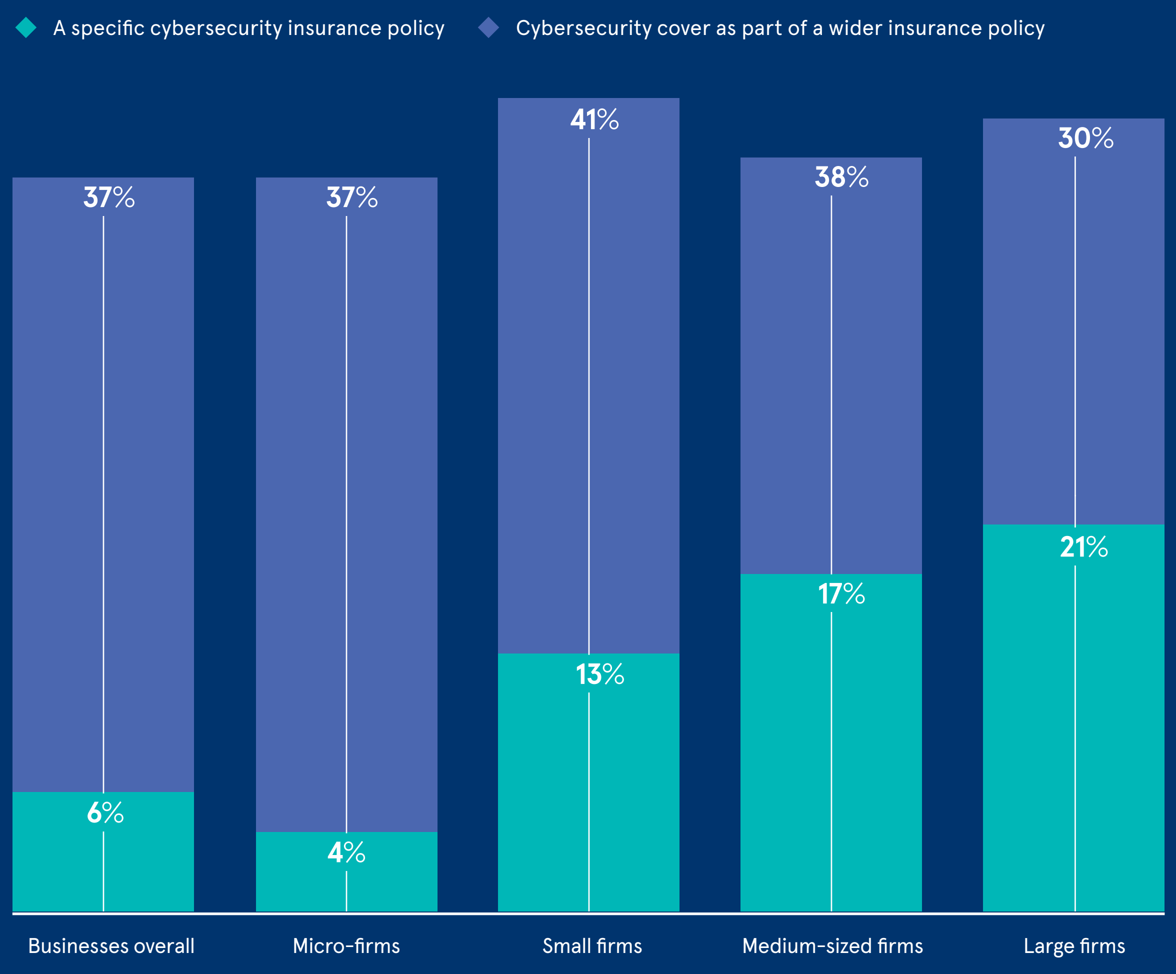
How often senior managers are told about cybersecurity issues



Department for Digital, Culture, Media and Sport, 2021

MOST BUSINESSES ARE NOT INSURED AGAINST CYBER THREATS

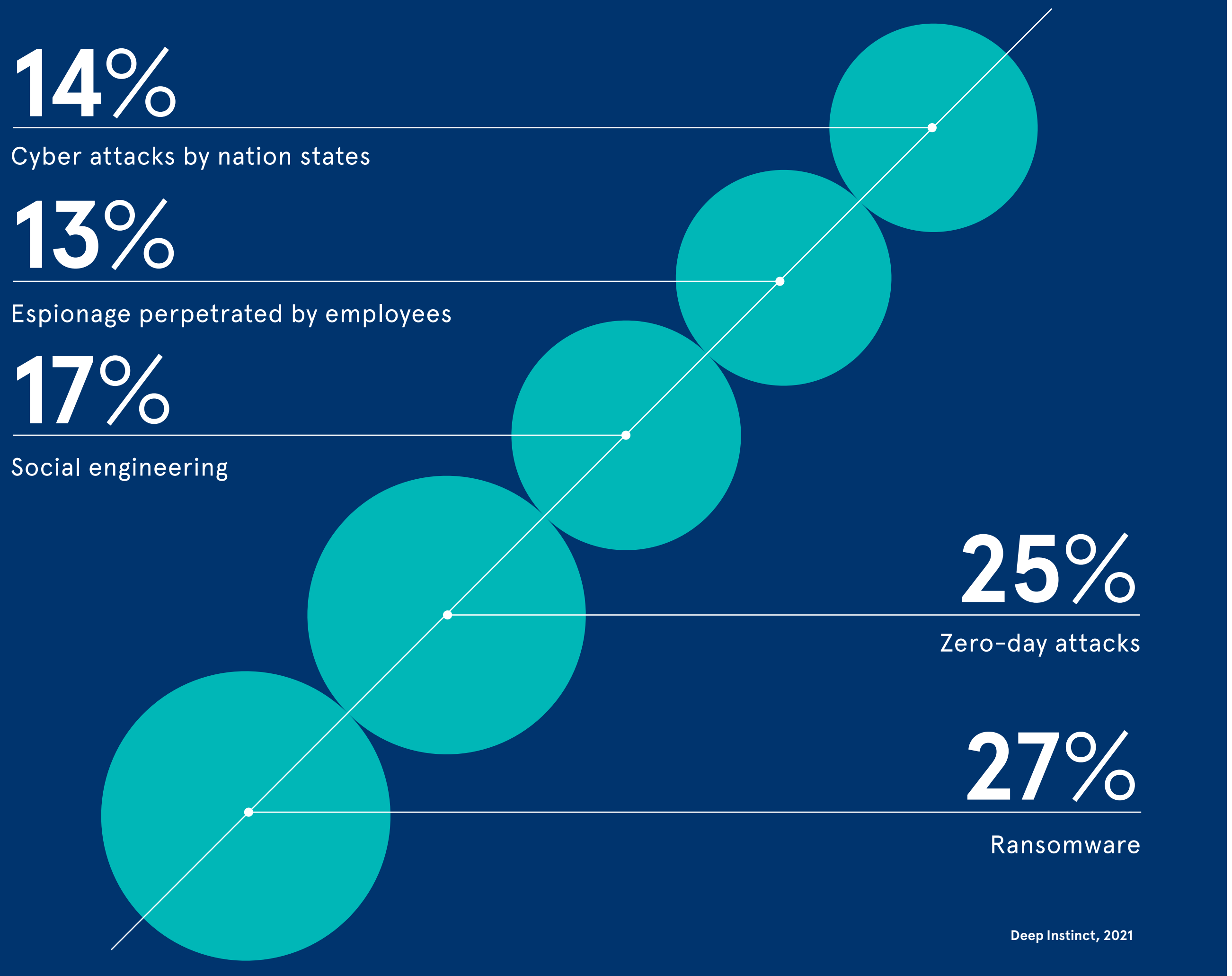
The percentage of UK businesses that report being insured against cyber risks in some way



Department for Digital, Culture, Media and Sport, 2021

THE MOST CONCERNING TYPES OF CYBER THREATS

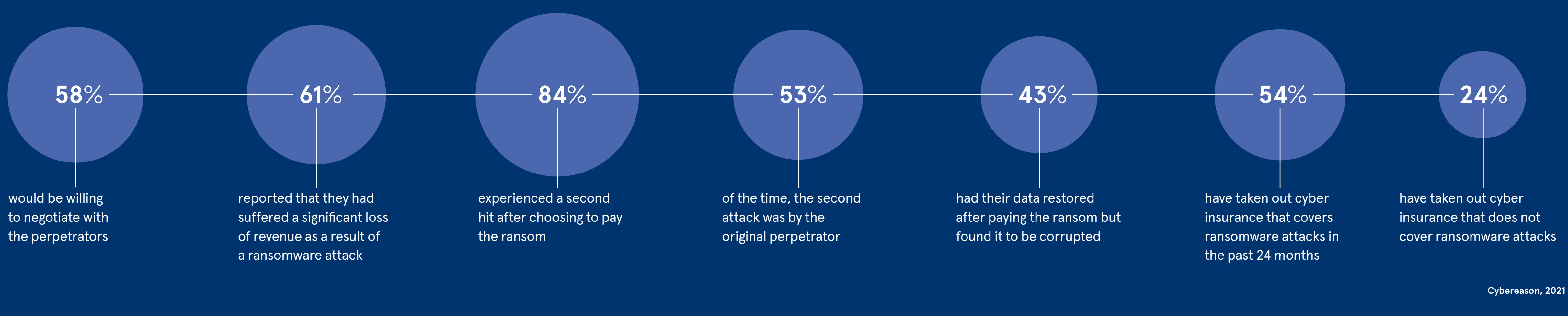
The biggest worries of cybersecurity professionals across North America and western Europe



Deep Instinct, 2021

PAYING THE RANSOM

Percentage of businesses that did / would do the following



Cybereason, 2021

CYBERCRIME

How to break the malicious feedback loop of ransomware

Ransom payments fuel this criminal industry, but discouraging them is a complex undertaking. Could making them illegal hurt businesses as much as the cybercriminals?

Davey Winder

Once upon a time, ransomware was more of a side dish than a cybercrime main course. In 1989, consumers got their first taste of the threat with the AIDS Trojan, which demanded a ransom of $189 to decrypt locked files. Fast-forward 30 years and everything has changed: consumers are no longer the target of ransomware and highly organised criminal operations are now more likely to demand six- or even seven-figure sums from the businesses they victimise.

Ransomware attacks have evolved from locking down network infrastructure to exfiltrating data, so backups no longer offer the protection they once did. The crime has also become a lucrative business model. The operations behind it often comprise several components: developers of the malware code and the operational software; affiliates that both execute the attack and gather intelligence beforehand; ransom negotiators; and even a technical support function to help victims recover their data.

Lisa Ventura, founder and CEO of the UK Cyber Security Association, says that the number of ransomware attacks increased globally by 150% last year – growth that isn't slowing down in 2021. "This volume of attacks makes ransomware the most impactful threat we face," she says.

Because many of the most prolific ransomware cartels are seemingly based in parts of the former Soviet Union where the long arm of the law cannot reach, stopping this crime is a real challenge. Going on the attack could be part of the solution, according to Ciaran Martin, professor of practice in the management of public organisations at the University of Oxford's Blavatnik School of Government.

"There is a role for offensive cyber activities, through the new National Cyber Force, which is working with US Cyber Command to attack the technical infrastructure that the criminals are using," says Martin, who was the founding chief executive of the UK's National Cyber Security Centre.

But perhaps there is a more straightforward option: outlawing ransom payments.

The commonality that binds all ransomware attacks is that payments fund the growth and development of this criminal endeavour. An obvious solution would be to cut off the funding by making ransom payments illegal.

Martin believes that allowing such payments encourages the lazy narrative that ransomware is an existential threat to the victims, who have no alternative but to pay up. The reality is a lot more complex than that, he says, warning that simplifying the picture only serves to help the criminals.

"Ransomware attacks usually are serious, but they aren't always an existential threat and they're rarely a threat to life," Martin argues, adding that paying up "often buys an only moderately effective decrypter key – and you still have to run this on battered systems in need of repair".

Research by managed service provider Talion, which founded the #RansomAware initiative to stop victim-shaming, has revealed that 79% of cybersecurity professionals favour outlawing ransom payments.

Mitchell Mellard, principal cyber threat analyst at Talion, acknowledges that there are many parts to the debate, but the fact remains that these criminals are enabled to continue with impunity by such rewards.

"I don't think that the option of payment should be shelved. But it should be regulated," he says. "Limit it to instances where the network or dataset is critical, such as a hospital or vital infrastructure."

> **Information-sharing is the only way to get ahead of the cybercriminals. They collaborate, so stronger collaboration is key to making our defences stronger too**

It has also been suggested that insurance policies which cover ransom payments are complicit in the rise of the ransomware threat and could be another area where regulation is required. Martin is clear about the role of insurance companies, which isn't to make public policy.

"You either ban ransom payments or you don't," he says. "Banning them via insurance doesn't achieve anything."

This isn't the same as saying that the insurance industry doesn't have a part to play. Engaging with the government and the businesses it serves to work out what has gone wrong is common sense.

Martin thinks the most important thing is to get insurance companies to enable the useful social function of incentivising good security. Without this, what Mellard calls a "malicious feedback loop" is put into play: the ransomware operators invest in new tooling, underground recruitment and the purchase of leaked credentials and exploits. This gives them a greater chance of success in the next attack – and so the cycle continues, he says.

By allowing a company to determine its security posture as an operating cost, instead of an essential part of the business requiring serious ongoing investment, ransomware insurance policies certainly appear to play their part in the feedback loop. But for how long?

Ian Thornton-Trump is CISO at Cyjax, a provider of intelligence on cyber threats. He recalls that, in virtually all of the thousands of ransomware attack cases he has researched since 2015, "successful attacks can be broken down into the failure of staff, a flaw in a process or a failure of security technology".

This leads him to believe that insurers will "start to baulk, refuse and reduce the amount of payments" they make under business interruption insurance or cyber-insurance policies for a risk that he views as entirely preventable.

There is a real sense of irony about the prevention of ransomware attacks, not least because some of the perpetrators will offer mitigation advice as part of the wrap-up process. Yes, you read that right: a number of ransomware cartels will disclose their access routes and advise victims on how to protect their networks more effectively from future incursions.

While it would never be a sound idea for organisations to take security tips from their attackers, sharing is something that should be on the ransomware mitigation agenda to break the threat cycle.

The #RansomAware initiative wants to play a key role in doing just that. The UK Cyber Security Association is part of this coalition of businesses that exists to share experiences, exchange ideas and pool intelligence – anonymously, if necessary – on ransomware attacks.

"Information-sharing is the only way to get ahead of the cybercriminals. They collaborate to make attacks more successful, so stronger collaboration is key to making our defences stronger too," Ventura argues.

Talking openly about attacks aids a better understanding of the techniques used, whereas pretending they aren't happening and working to prevent news from leaking to the media only benefits the criminals.

"The more that companies are willing to speak out about becoming victims of ransomware attacks," Mellard says, "the faster and more comprehensively the information security sector can develop detection techniques and countermeasures to the tools employed by ransomware groups."

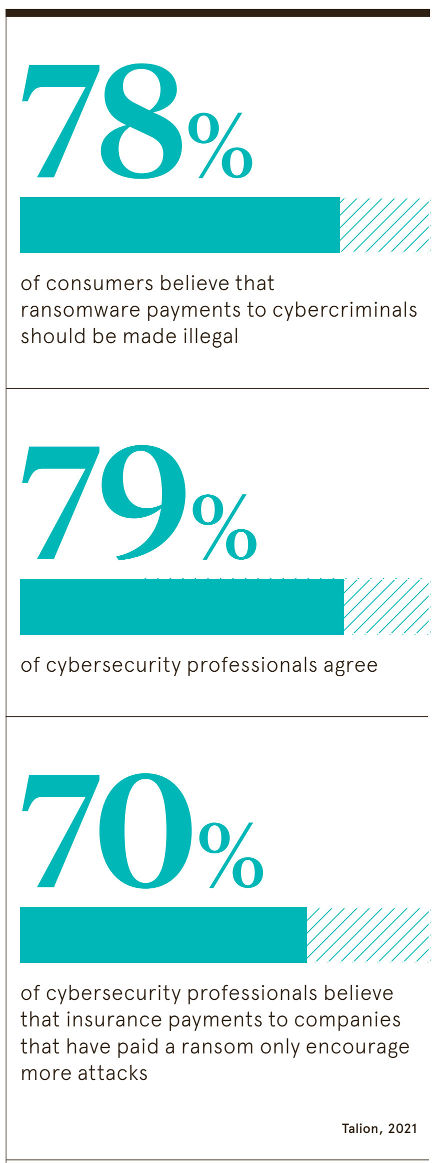
But such initiatives cannot succeed on their own. Government programmes and regulations need to be part of the process.

Thornton-Trump even suggests that the judiciary perhaps considers that the use of client-attorney privilege to avoid having to report cybercrimes is making it harder to prosecute the perpetrators.

"Using this mechanism when it comes to the disclosure of the details of a data breach is detrimental to the greater good," he says. It's a point that many cybersecurity experts agree with, unlike the more hotly debated question of banning ransom payments.

Martin sees the case for making it mandatory for victims to disclose ransomware attacks to the authorities as a slam dunk.

"I can't think of a single decent argument against this – and I haven't heard one," he says. "The government should implement it at the earliest opportunity." ●



78%

of consumers believe that ransomware payments to cybercriminals should be made illegal

79%

of cybersecurity professionals agree

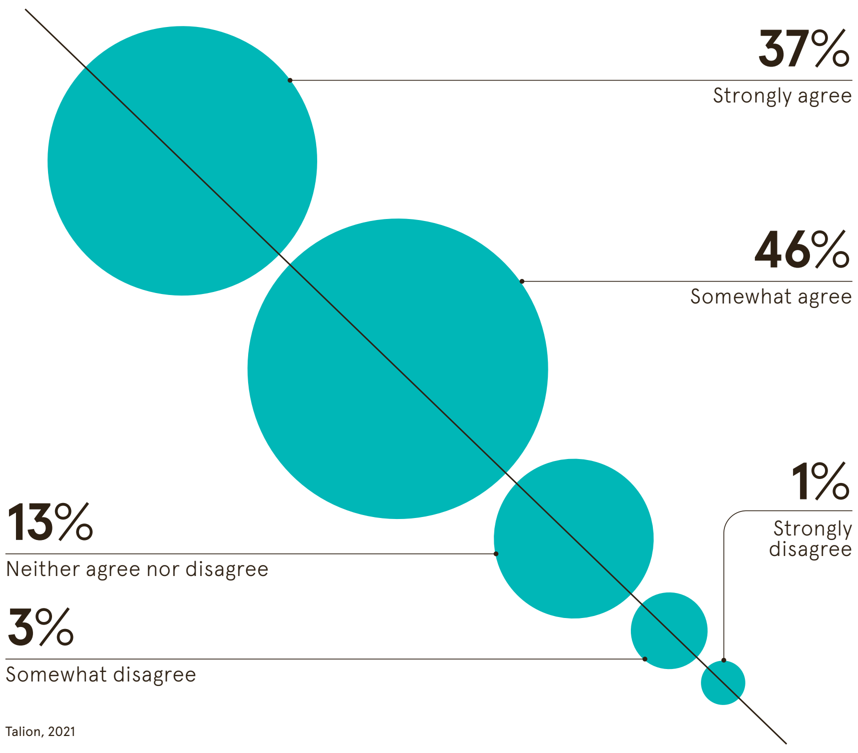
70%

of cybersecurity professionals believe that insurance payments to companies that have paid a ransom only encourage more attacks

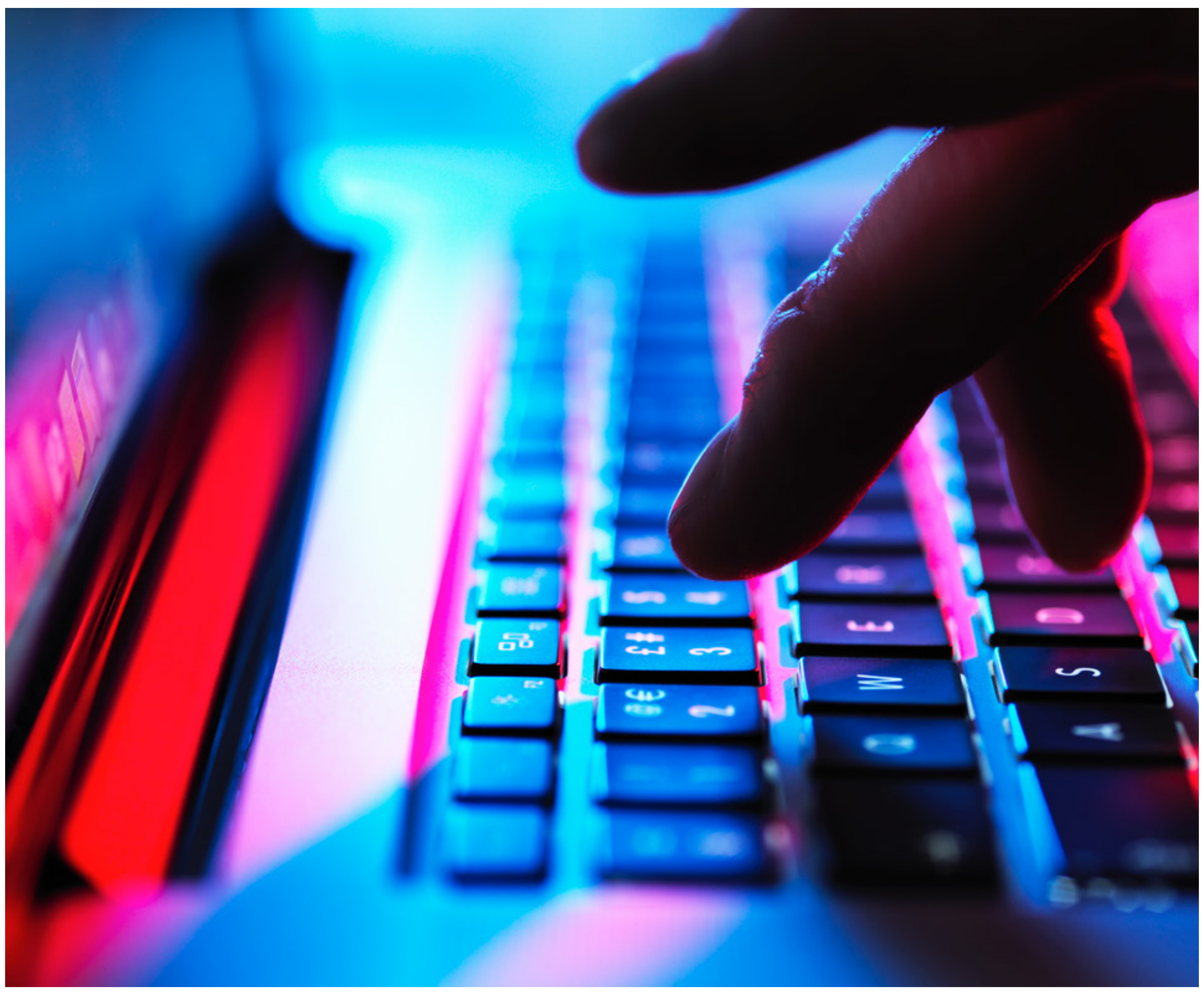
Talion, 2021

THE BLAME GAME

Percentage of UK workers who responded in the following ways to the following statement: "It is a cybersecurity failing when an organisation is infected with ransomware"



Talion, 2021



ETHICAL HACKING

Inside the world of the penetration tester

Ethical hackers probe their clients' systems to find weaknesses. But how, exactly, do they go about this?

Charles Orton-Jones

A vital aspect of cybersecurity is to hire a penetration tester. This is a 'white hat' hacker who will search for vulnerabilities in their client's systems. If they find a way in, the hole can be patched before the bad guys discover it.

Many businesses are in the dark about pen testing. Who are these guys? How do they work? Is there a standard approach? And what does a pen test really tell you?

The first thing to know is that pen testers use a set of pretty standard tools. Anyone can learn to use them.

"There's Metasploit, which is a framework used to exploit vulnerabilities and deliver payloads," says Christian Espinosa, MD of cybersecurity consultancy Cerberus Sentinel. "Burp Suite is used for web application hacking; Wifite is used for Wi-Fi hacking; sqlmap is used to probe and attack SQL databases; Nmap is used for network discovery of open ports; and Hashcat is used to crack passwords."

Overall, there are about two dozen mainstream tools for pen testing. They are freely available, so there's no need to rummage around the dark web for them. Most are open source and cost nothing. Metasploit, for example, is downloadable from GitHub.

There are even operating systems that are designed for the job. Louise Barber, senior consultant at risk management consultancy Turnkey Consulting, says: "Where they are legally able to do so, testers will try to use the same tools as the criminals. Platforms such as Kali Linux incorporate many such tools, including Nmap and Metasploit, as well as Wireshark, Netcat and Burp Suite for full end-to-end testing of applications and analysing network traffic."

These standard tools are augmented by the pen tester's homebrew scripts. Liam Follin, senior service development consultant at Pentest People, for instance, wrote the Athena script, which can show whether the passwords of users associated with a domain have been leaked online. It's a fast-moving trade, so the best pen testers will improvise in this way when necessary.

Again, many of these tools are shared with the community on GitHub.

Software tools are only phase one. Pen testers will also use information gleaned from internet searches, and even visits to the target's premises, to gain an edge.

"According to Proofpoint's 2019 *The Human Factor Report*, 99% of cyber attacks apply social engineering techniques to trick users into installing malware," says Leon Teale, senior penetration tester at IT Governance. "The most common form of social engineering attack is phishing. These attacks exploit human error to harvest login credentials or spread malware, usually via infected email attachments or links to malicious websites."

There is a long list of techniques, says Teale, who cites incursion methods such as offering giveaways that turn out to be an infected device. There's tailgating, when a hacker physically follows the target into a restricted area while claiming to have mislaid their security pass.

And then there's waterholing, which infects websites that a target group is known to frequent. This is what happened with 2017's NotPetya infection. Believed to be a politically motivated attack against Ukraine, NotPetya infected a government website and then spread through the country's infrastructure.

The image of pen testers conjures up maverick hackers, working in a basement surrounded by screens. In fact, many learn their trade simply by going on courses. One former Pen Tester of the Year used to be a roadie until he became bored with stacking boxes for touring musicians. So he took the cyber exams and became an ethical hacker at KPMG.

> **As the malicious hackers get smarter, it's critical for ethical hackers to stay on top of the latest vulnerabilities and threats to keep one step ahead**

"Numerous certifications are available," says Jonathan Wood, founder and CEO of C2 Cyber. "The most prestigious of these is known as the offensive cyber security professional. It features a 24-hour exam that requires you to identify various vulnerabilities and break into a network. It's offered by the organisation Offensive Security and is intended for cybersecurity professionals who want to step into the world of professional penetration testing."

He adds: "As the malicious hackers get smarter, it's critical for ethical hackers to stay on top of the latest vulnerabilities and threats to keep one step ahead. The only way to achieve this is by studying."

A popular place to learn is Hack The Box. Founded in 2017, this resource now has 670,000 active users. It offers tuition for cyber experts of all standards and runs 'capture the flag' competitions – in which teams of pen testers tackle a series of challenges, such as website hacks, forensic examinations and blockchain tasks. Such exercises give students of the art an effective way to put their skills to the test.

Do pen testers always succeed? The truth is that there are almost no systems without some sort of weakness. Nate Drier, managing principal consultant at Secureworks, puts it this way: "Good teams have a very high level of success in penetration testing but they usually have to deal with time and scoping restraints that the real bad guys don't abide by."

Drier points out that well-funded hackers, such as nation states, can take months to achieve their objectives. "The bad guys often have a lot of patience when it comes to achieving their ultimate compromise or pay day," he says.

The best defensive policy is not only to employ pen testers but also to work with cyber consultants. For instance, 22 heads of IT from NHS organisations in Cheshire and Merseyside ran a drill managed by consultancy Gemserv after the WannaCry ransomware attack, which had affected 34% of NHS trusts in 2017.

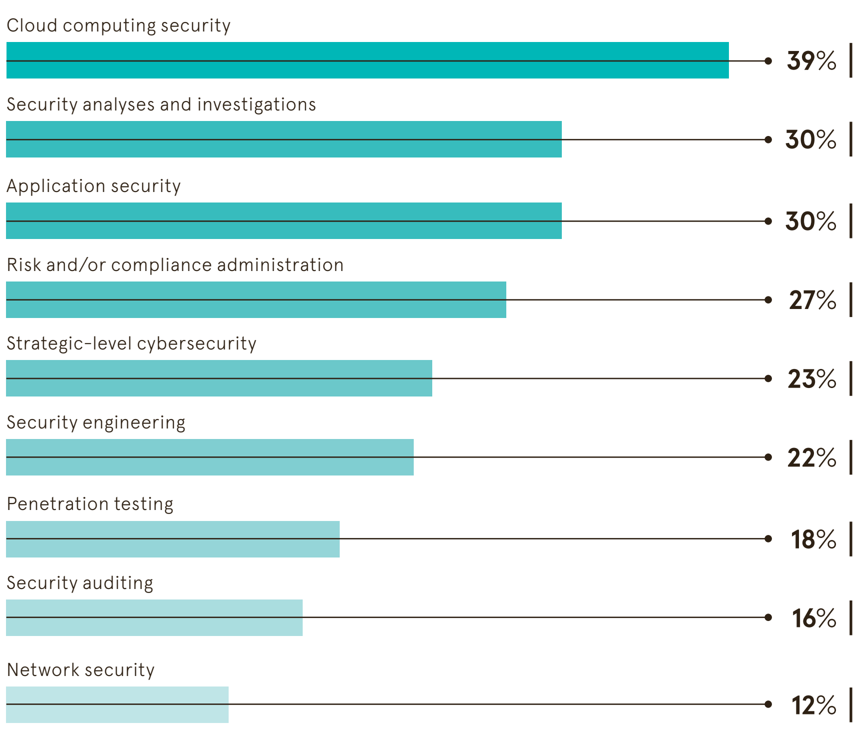
Paul Charnley led the initiative, which tested the participants' security and their ability to restore compromised databases.

"After WannaCry, we swore that we would work more closely together, under the tagline 'we are only as strong as our weakest link'," he says. "I want to do this every six months – certainly once a year – and every integrated care system should be planning to do the same."

It's a strong point. Pen testers are very good at discovering vulnerabilities. What an organisation does with the information they provide is the next big question. ●

CYBERSECURITY SKILLS IN DEMAND

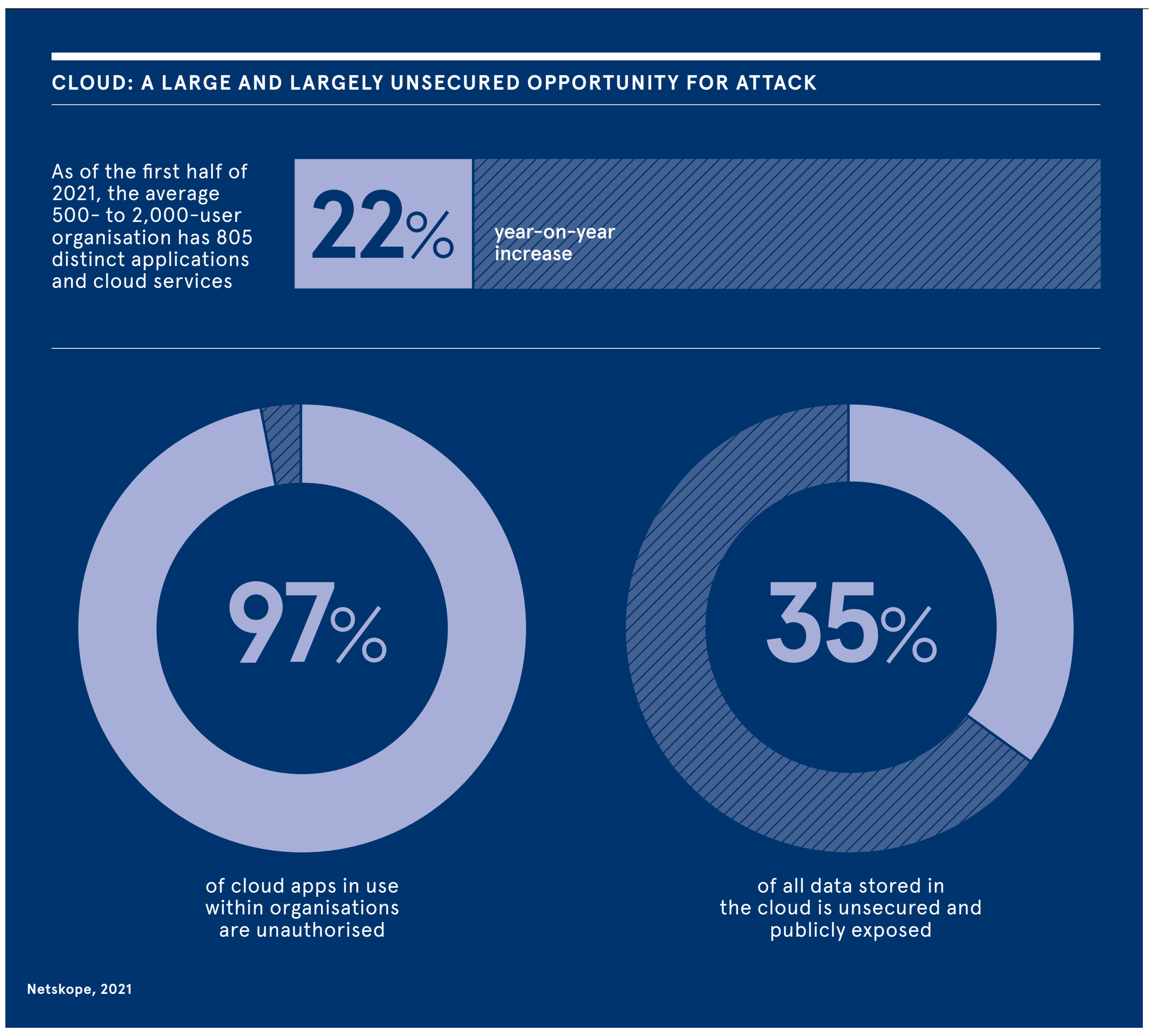
Percentage of cybersecurity professionals who say the following are among the top three areas in which organisations are experiencing a lack of cyber skills



ESG, ISSA, 2021

Commercial feature

CLOUD: A LARGE AND LARGELY UNSECURED OPPORTUNITY FOR ATTACK



Netskope, 2021

Rethinking network and security architectures for cloud

In an evolving cyber threat landscape increasingly shaped by cloud computing and applications, organisations need to rapidly rethink their traditional network and security architecture

The traditional concept of a network security architecture, where teams build secure perimeters around corporate assets and police the traffic that comes in and out, still underpins the security strategy of many organisations. But in the era of cloud, it is no longer fit for purpose.

The growing patchwork of vendors required in a perimeter-based security approach is a source of daily frustration for chief information security officers (CISOs). In a study by Netskope in early 2021, 46% of global IT leaders said they are looking for an opportunity to consolidate network security vendors. This is one of the reasons that, in 2019, Gartner recommended a new approach to security architecture, Secure Access Service Edge (SASE). A software-defined, cloud-delivered architecture, SASE protects anywhere-anytime access to digital services.

Just months after Gartner presented the SASE approach, the arrival of the Covid-19 pandemic vastly accelerated its urgency, as organisations rapidly adopted remote working to survive. With employees having now spent 18 months juggling work, school and life across a mixture of corporate and personal devices, the reliance on cloud applications has exploded. As of the first half of 2021, the average 500-2,000 user organisation has 805 distinct applications and cloud services, a 22% year-on-year increase, according to Netskope.

Every company has become a cloud organisation during the pandemic, and research firm 650 Group forecasts the SASE market to grow by 500% between 2020 and 2025. As teams moved swiftly to select and authorise cloud services as the only way to onboard and upscale essential services, `shadow IT' use among remote workers spiralled. Unauthorised cloud apps in use within organisations is as high as 97%, Netskope's data reveals.

"The impetus for change was already there, but nobody realised what was just around the corner in the form of a global pandemic that further accelerated the need for SASE," says Neil Thacker, chief information security officer EMEA at Netskope, a market leader in SASE.

"We're seeing a lot of requests from organisations to consolidate. They've realised they have too many overlapping legacy network and security controls and instead want to leverage approaches such as zero-trust network access but don't want multiple disparate products to do it. They aren't too concerned around how they connect to key services and data, they just want to connect securely, without any degradation in performance, and to use the same security policies across all traffic and data flows."

Cyber threats, meanwhile, are adapting quickly to this new landscape. More than two-thirds of malware is now delivered via the cloud, predominantly through cloud storage apps. Cybercriminals use the same cloud services in their attack as the enterprises they target, so the URLs that host the nefarious payload are familiar and trusted by their targets. Phishing attacks are also still common, and they are increasingly linking back to a cloud service as threat actors themselves are outsourcing their architecture to help bypass an organisation's security controls.

"There has been an increase in both the prevalence and sophistication of threats," Thacker adds. "Most notably, threat actors not only use cloud services to deliver their malware and payloads but they also target cloud infrastructure and applications looking for misconfigurations. There are now thousands of cloud services and security teams are often asked by the business to enable direct access to them. Of course, when you put in a bypass or allow this type of connectivity without any security controls, threat actors will be ready to actively exploit these gaps."

Organisations that are no longer able to put walls up around their data in private data centres are more at risk of user error when applying security settings to cloud-stored data, leaving over 35% of all data stored in the cloud exposed. By following the data, a SASE approach can spot these security gaps and either automate a remediation, or coach employees when inappropriate high-risk behaviours are identified, making the security team's role less reactionary and more proactive.

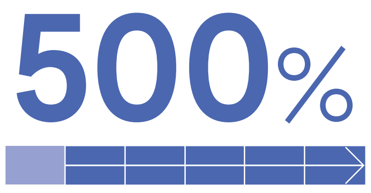
Traditional security products interpret the language of HTTP(S) and so fail to spot issues in trusted cloud services. SASE can do this, but it also interprets the languages of cloud, such as API, and so is able to provide the granular inspection of data needed to protect against cyber risks and threats. After using Netskope to analyse its data traffic, one large manufacturing firm discovered that the organisation had over 800 unique instances of Google Drive. One was the corporate instance, while the rest were personal and third party instances. The only way to accurately identify them was through API decoding.

Large architectural IT redesigns may often come with big price tags, but early SASE adopters are reporting the opposite. As SASE is in the cloud, it is operational rather than capital expenditure, and by replacing traditional appliances it has helped eradicate the need for painful and expensive hairpinning of traffic flows. Crucially, early adopters are reporting cost savings of millions of pounds from removing Secure Web Gateways, VPN and WAN hardware, as well as MPLS bandwidth savings.

> **Organisations are realising cost savings from 15% to 30% by moving away from hardware and adopting a SASE architecture**

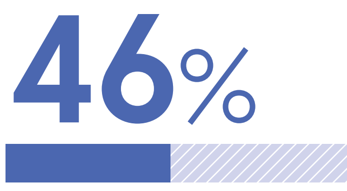
"Organisations are realising cost savings from 15% to 30% by moving away from hardware and adopting a SASE architecture," says Thacker. "But a key benefit, beyond cost and consolidation, is visibility. As enterprises move more and more data to cloud services, these services are becoming the default target. We are also seeing an incredible number of unauthorised or unmanaged cloud applications being used, and all the while there are ongoing challenges around data sovereignty and compliance with data protection laws.

"We urgently need to fix the visibility gap because 97% of cloud services being unauthorised and unmanaged is way too high. Organisations must bring that down to a more manageable level. The CIOs and CISOs we interact with see the need for better visibility of what cloud services are being used as their number one priority. If they don't know what is being used, how can they apply an appropriate form of security control? SASE identifies what cloud services are being used; by whom, for what purpose, exactly what data is going there, and where it is located."



market growth is predicted for SASE between 2020 and 2025

650 Group



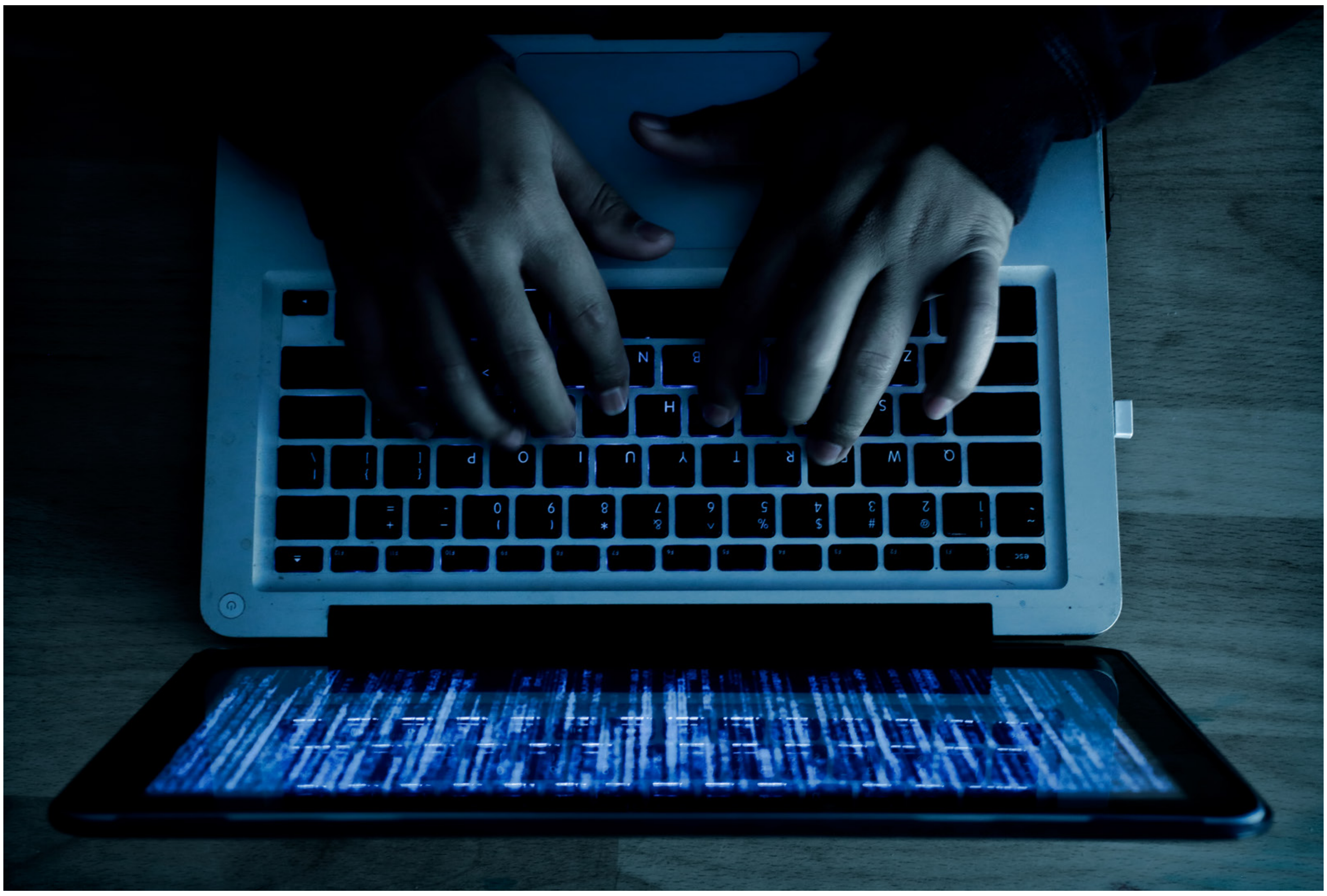
of global IT leaders say they are looking for an opportunity to consolidate network security vendors

Netskope, Censuswide, 2021

For more information about the latest cloud security threats, download Netskope's most recent Cloud and Threat Report at:

https://www.netskope.com/netskope-threat-labs/cloud-threat-report

netskope



GEOPOLITICS

Cold war 2.1

Cheap, low-risk and effective, state-backed cyber attacks are attractive to nations such as Russia and China, particularly while their adversaries' digital security remains so lax

Peter Yeung

> It makes perfect sense – cybertools are excellent weapons. They are efficient, affordable and deniable

For decades, cyber attacks were widely thought to be the preserve of tech-savvy individuals or gangs seeking to steal or extort money. In recent years, it's become clear that nations are using cybercrime as a standard part of their armoury.

Ransomware, phishing and distributed denial-of-service attacks are just a few of the many weapons that states are using in geopolitical conflicts that are increasingly playing out in cyberspace rather than on the battlefield.

Mikko Hyppönen, chief research officer at IT security company F-Secure, has been helping state authorities in North America, Europe and Asia to fight cybercrime for more than 30 years.

"In the 1990s, I wouldn't have believed that national governments, intelligence agencies and the armed forces were developing and deploying malware against other countries. The notion would have sounded like science fiction to me," he admits. "But it's obvious in hindsight. It makes perfect sense – cybertools are excellent weapons. They are efficient, affordable and deniable."

Hyppönen observes that all technically advanced nations are developing both defensive and offensive applications for these weapons as the battle for cyber supremacy escalates around the world.

Although state-backed cyber warfare is no longer novel, a tipping point has been reached as the offensive capabilities of the weaponry have become more sophisticated and the use of digital tech has become more ingrained in society. So says Dr Tim Stevens, senior lecturer in global security at King's College London and head of its Cyber Security Research Group.

"A lot of what we're seeing isn't entirely new, but the scope and scale of it are increasing all the time," he says "What's readily apparent is that this is now an issue of public and global policy. It affects you and me every day."

His point is backed by the most recent figures from the National Cyber Security Centre, which is a part of GCHQ. Last November it reported that it had protected the UK from 723 cyber "incidents" in the 12 months to 31 August 2020. That was a 20% increase on the annual average total over the preceding three years.

There are two main reasons behind this intensification, according to Stevens. First, there has been a significant increase in the size of the "attack surface" provided by the world's most developed economies. Their digital transformation has advanced to the point where they're offering a much bigger choice of potential entry points to target.

"This is unequivocally the risk management problem of the 21st century," he says, adding that the second, related reason has been the rise of low-cost digital tech lacking adequate security features.

"We are producing increasing amounts of data and we're linking up devices that are demonstrably insecure," Stevens says. "When you turn things over to the market, it becomes a case of 'pile 'em high and sell 'em cheap'. Billions of low-cost devices being sold don't have good security."

Alex Rice is the founder and CTO of HackerOne, a company that uses hackers to help organisations detect vulnerabilities in their own systems. He cites another factor behind the upsurge in state-backed cyber warfare.

"The amount of tech being developed that's unique to particular governments is declining rapidly. Today, it is shared more or less across the board. This means that there are few pieces of state tech that can't be attacked," he says. "We improve their defences by focusing on private-sector and open-source technology. For example, there are two major mobile platforms – Apple and Android – in use. We secure government infrastructure by securing all private infrastructure and networks."

Given the complexities of cyber warfare, Stevens believes that no single solution can ever provide an effective defence. "A multi-pronged set of initiatives is needed," he says. "These will range from security standards to education and diplomacy."

While diplomacy has a key role in developing standards of behaviour, Stevens

Commercial feature

The future of security needs to put developers first

Why embedding security throughout the software development lifecycle is crucial

The pressure to be an always-on, ever-evolving business today is enormous. It's not enough to innovate: businesses must be responsive to new market conditions that can change like the wind. But, added to all the disruption and transformation is the question of keeping everything secure. It's a challenge not everyone is prepared for.

Internet-based applications now play a major role in how companies work with customers and deliver services: they're the engine for this new-found agility. Applications can be changed to meet new conditions or customer needs many times a day, if necessary. But this has important implications for how companies approach cybersecurity.

Historically, Security with a capital 'S' has been a separate department to Development. It would wait until code was 'finished', then it would be tested and refined. But in reality, code is never 'finished', and these types of cumbersome, legacy processes slow down innovative businesses, not allowing them to keep pace with their competition.

Today's applications have two major characteristics. First, they're cloud native – built and hosted in the cloud rather than on the business's own servers or data centres. This allows them to scale and change direction in minutes. It's a far cheaper, more flexible way of staying ahead of the curve.

Second, most modern applications are created using the practice of 'DevOps'. Essentially, it means the teams building and running the applications are one and the same. As a result, developers can make a wider range of strategic decisions about the application as well as making changes to it, as and when they need to.

Guy Podjarny, co-founder and president of Snyk

In this fluid world, where fast decision-making is paramount and applications are in a state of constant change, a static 'single point in time' approach to security is simply outdated and inadequate.

Ultimately, security needs to be assimilated into the development process. But finding a way to meet rigorous standards without slowing down product evolution or compromising security can be difficult, particularly if the rest of the business has yet to catch on to this mindset. Snyk has a unique developer-centric approach to cybersecurity and validates its vision for application security for global enterprises currently undergoing digital transformation.

To succeed with a developer-first security approach, businesses need to tackle three key security challenges.

First, there is the curse of the expert. Developers are highly skilled at finding effective solutions to almost any gnarly problem. But they aren't necessarily also aware of current best practice in using code to make sure they avoid security vulnerabilities.

The second challenge is building on the work of a wider community. In part, developers are so fast and efficient at what they do because they can access a vast supply of ready-made resources, many of which have been published as Open Source code. This code rapidly accelerates projects and avoids reinventing the wheel, but it might occasionally have security flaws. Developers have neither the time nor the expertise to 'peel back the layers of the onion' when it comes to making sure there are no unpatched vulnerabilities lurking in the background.

Finally, simple misconfiguration can be a significant source of security woes. Developers can easily create and manipulate large amounts of computing power like virtual servers using software. But making sure they are always set up correctly is a new territory, and not always a familiar one.

For companies already unfamiliar with the need to put security at the heart of a newly tech-driven business, these challenges may seem like a mountain to climb. But, in most cases, it's simply a question of adjusting mindsets and adopting tools that are more appropriate to both today's work and the future. Tools that assist developers as they work, provide solutions at the touch of a button and, crucially, that are themselves constantly updated and enhanced in real-time, just like Snyk, with millions of developers becoming more secure by leveraging our tools in their daily work.

This developer-first approach is essential. Adopting a broader and deeper approach to cybersecurity by embedding security tools and best practices throughout the software development life cycle is the make-or-break factor in achieving cloud native application security success.

For more information please visit snyk.io

snyk

OPINION

'The social networks that bring our industry together are being tainted by the few. The call for respect in security has never been more vital'

Harassment and trolling have, devastatingly, become more endemic in the cybersecurity industry in recent years.

The *Cambridge Dictionary* describes trolling as "the act of leaving an insulting message on the internet in order to annoy someone". The term means different things to different people, but I'd argue that a troll is a variation of the term 'bully'. Perhaps it's better to use that term, because society recognises how damaging bullying is.

I've dedicated considerable time to investigating the scale and severity of harassment in the infosecurity industry. It's jaw-dropping, ranging from insults and slurs to sexual and physical harassment and even death threats.

Social media has long been a haven for the cybersecurity industry, bringing the community together in a way that makes many techies feel at home. This culture of trolling and harassment has ruined that refuge for many.

About a month ago, #infosecbikini began trending. When a member of the infosecurity community experienced a backlash for posting a photograph of herself in a bikini on her personal Twitter account, the industry rallied around her. Men and women alike flooded the network with photographs of themselves in swimwear using the same hashtag, in a display of solidarity and condemnation of the troll. It was a powerful moment in an industry that has grown tired of toxicity.

The recent creation of Respect in Security, an industry-led initiative that aims to support victims and stamp out abuse in cybersecurity, shines a spotlight on the abhorrent behaviour taking place. Its founders' passion is admirable, but the fact such an initiative needs to exist is tragic.

Respect in Security commissioned Sapio Research to poll more than 300 industry professionals (male, female and non-binary) about the extent of harassment in the industry. About one-third of respondents shared their own experiences of harassment online (32%) and in person (35%).

As an industry, we need to be wary of the emphasis we place on social media status. Twitter amplifies the voices of those who seek to be amplified and ought to come with the following warning: 'Danger of unwelcome opinions and comments.'

The tech industry has been guilty of putting its social media personas on a pedestal, acting with outrage and disbelief should anyone try to knock them off. We have placed too much value on social media notoriety. Healthy debate and criticism should be 'verified'. Abuse should not.

Infosecurity is an industry that has historically struggled to attract talent. There remains a substantial skills gap, yet we continue to allow our networks – both online and in the real world – to be afflicted with abuse that may well be deterring potential recruits. The industry must do better.

I have asked some of the industry's finest minds for guidance on what to do if you become a victim of trolling. Their advice is as follows. Publicly engage only if the troll is making an untrue statement about an organisation that you represent. If you need to take a break from social media, come back differently. Build your own resilience. Use your 'tribe' not to shame the troll, but to seek advice and a private confidence boost. Pick your battles. And report harassment to the social network concerned, the police and/or the Internet Crime Complaint Center.

It's a travesty that the online social networks that bring our industry together and offer such a source of community and support to so many can be so tragically tainted by the few. The call for respect in security has never been more vital. ●

Eleanor Dallaway
Editorial director,
Infosecurity Magazine

IS THE NATIONAL CYBER SECURITY CENTRE PROTECTING UK CITIZENS EFFECTIVELY ENOUGH?

723

cybersecurity incidents handled by the NCSC in the 12 months to 31 August 2020

2.3 million

suspicious emails reported using the new suspicious email reporting service

2.7 million

visitors to the NCSC's website

1,200

victims supported

166,710

phishing URLs taken down, more than 65% of which were removed within a day

National Cyber Security Centre, 2020

The cyber risks of the smart city

The 5G-enabled, highly connected smart city has been heralded by some as a utopia, offering seamless functionality between infrastructure systems ranging from power distribution grids to public transport networks and providing the ultimate in digital convenience for its citizens.

Yet security experts are concerned that, while such developments could drastically improve people's quality of life, the smart city is vulnerable to being disrupted like never before.

"There's a lot of talk about smart cities, but not so much talk about *secure* cities," says Tim Stevens of King's College London. "Critical infrastructure must be made absolutely secure. But we're not quite there – criminals are still working their way in."

He cites the ransomware attack in May that successfully took control of the computer systems of Colonial Pipeline, a major US fuel distribution network, forcing the company to spend $4.4m (£3.2m) to pay off the hackers.

"That was a wake-up call for a lot of people," Stevens says. "Energy is one sector that really concerns the public because without it everything grinds to a halt. I find it remarkable that we haven't yet seen many infrastructure disasters on this scale."

The University of York's Vasileios Vasilakis agrees, citing the first known successful cyber attack on an electrical grid in December 2015. Hackers believed to be linked to Russia delivered malware via a phishing email, which cut power to more than 230,000 people in Ukraine, fortunately for no more than six hours.

"Events such as this could become more and more common," he predicts.

Security professionals warn that, as a consequence, there may need to be a trade-off between a modern urban environment, made smarter by data, and a city where everyone's privacy is protected.

"The explosion of the internet of things has made people's lives easier, but few IoT devices have been designed with security in mind," says Jake Moore of ESET. "We have far more IP addresses in our homes than ever. These can be exploited by all sorts of criminals. We need to think carefully about the implications."

This threat is likely to become even more complex as systems become ever more reliant on the internet. Experts fear that, if the appropriate measures aren't taken to agree stricter security protocols, hackers could take control of critical urban infrastructure.

"It's like what we see in the movies, but some of it could actually be done for real," says Mikko Hyppönen of F-Secure. "We're becoming more and more efficient, but more and more vulnerable. Just imagine how much more reliant we will be in 10 or 20 years' time."

acknowledges that it would be hard to come up with a framework that's acceptable to all – and, even then, some states could sign up to it and then renege.

"Russia, for instance, allows cybercriminals in the country to act as long as they don't interfere with the state's activities," he notes. "But this is something that Biden and Putin could agree to prevent."

Dr Vasileios Vasilakis, a lecturer in network security at the University of York, agrees with Stevens that "advanced persistent threats" – hacking groups affiliated with national governments – could be prevented through diplomacy.

"It would be much more difficult for them to operate if Russia were to crack down on them," he says.

Hyppönen suggests that another response to the cyber threat at the political level would be the establishment of a dedicated ministerial portfolio.

"This issue needs to be taken seriously and have the proper levels of leadership behind it," he says. "Eventually, all countries will have ministerial or cabinet-level representation for cyberspace. It's going to become the norm."

Rice believes that a more effective political response, which could help to protect critical infrastructure, would be the creation of a cyber warfare equivalent of the Geneva convention.

"It's in our mutual interest to not attack each other's power grids," he says. "So we need to establish what's allowed and what is not, so that governments can be held accountable for their actions."

Many analysts think that governments should also regulate any technology being sold in their countries to ensure that it meets minimum cyber security standards.

For Hyppönen, an international certification scheme for security akin to the CE system for manufacturers selling goods in the European Economic Area could work. "We need to verify that the devices we are using are as safe as possible," he says.

Others point to the support that governments could be offering SMEs in a capacity such as that of the UK Centre for the Protection of National Infrastructure. While "large corporations can hire their own teams to defend their networks, it is harder for small businesses to do" Vasilakis notes.

It's not up to governments alone to deal with the problem, says Jake Moore, a cybersecurity specialist at firewall provider ESET. The onus, he argues, is also on individuals and enterprises to support the effort by protecting themselves with proven measures such as encryption.

"Serious players are involved in this, including Russia, China and North Korea," Moore stresses. "They are throwing huge amounts of money at it. That is why we desperately need a collaborative approach. We need the public to get involved and play their part, because governments aren't always the quickest at seeing this issue."

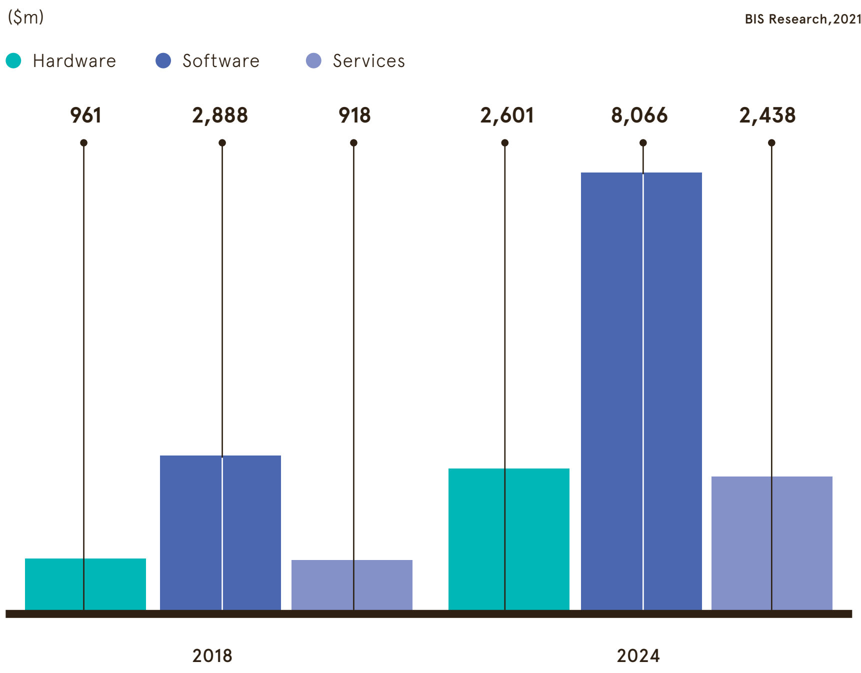
> **All countries will have ministerial or cabinet-level representation for cyberspace. It's going to become the norm**

Nonetheless, experts are keen to stress that most cyber attacks are still committed by criminals rather than governments, which tend to use hacking as a tool for espionage and sabotage rather than theft. This means that any defensive measures should account for these varying contexts.

"Who is your enemy – what threat will you need to defend yourself against? The answer could be so different depending on your enterprise," Hyppönen says. "Pizza restaurant owners, unlike state agencies, don't need to worry about foreign governments, for instance. But they do need to worry about ransomware attacks designed to gain access to payment systems." ●

MILITARY ARTIFICIAL INTELLIGENCE AND CYBERNETICS MARKET REVENUE WORLDWIDE IN 2018 AND 2024, BY SERVICE

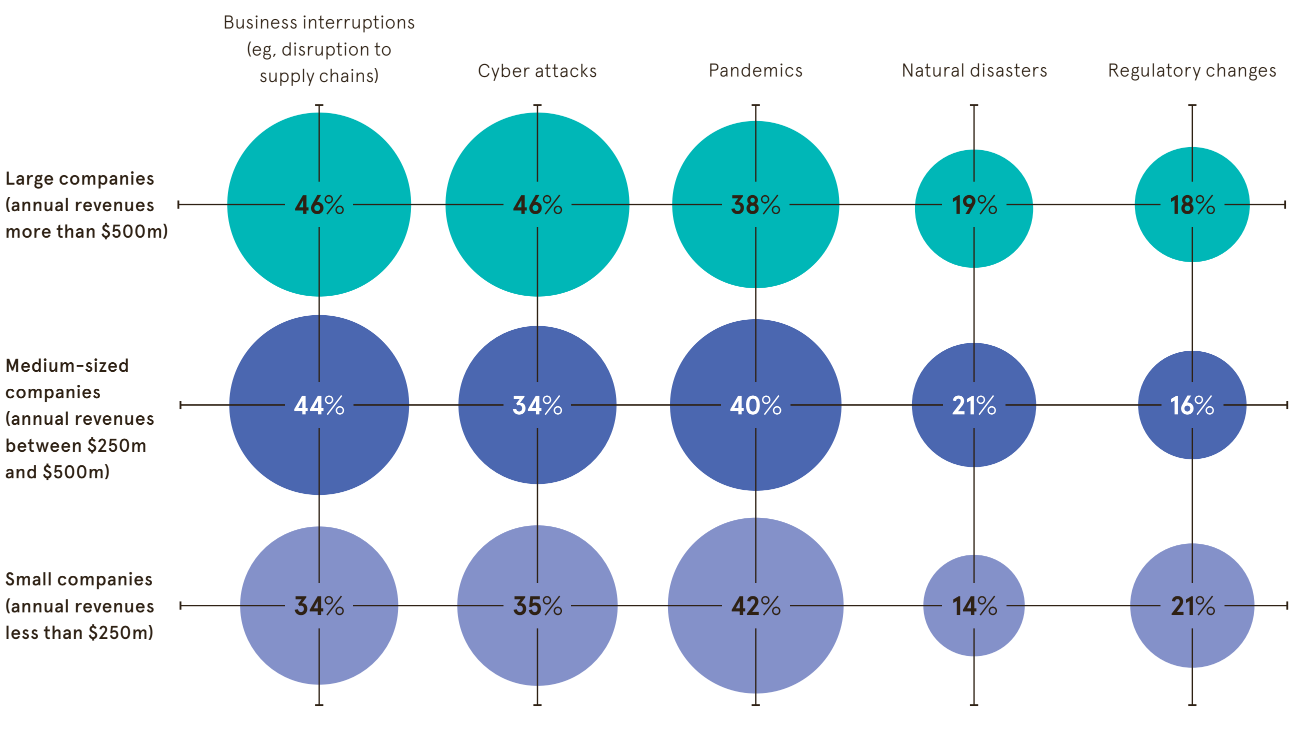
BIS Research,2021



CYBER ATTACKS RANK HIGHLY ON THE LIST OF MAJOR THREATS TO BUSINESS

Leading risks to companies worldwide, by business size

Allianz, 2021



Commercial feature

SMEs overwhelmed and unprepared in the cyber abyss

Small and medium-sized businesses are lacking the time, expertise and capability to deal with an ever-evolving threat landscape, which threatens to bring down their operations at any time

The democratisation of sophisticated cloud and collaboration tools has meant SMEs can compete globally with major enterprises which have much bigger budgets. Where the large variation in resources does clearly expose itself, however, is in the area of cybersecurity.

If SMEs are competing on an even keel with large enterprises, it means they are also as much of a target to cybercriminals, or at least can be equally affected by vast supply chain attacks, such as last year's devastating SolarWinds hack. Yet they are nowhere near as able to commit the big sums required for the cutting-edge cyber tools that the vendor ecosystem claims they need.

This has left three-quarters of SMEs feeling they lack the capability and expertise to withstand a cybersecurity attack, a recent study by Arctic Wolf found. The report underlines the extent of the challenge facing SMEs, with 39% overwhelmed by the sheer volume of security alerts they receive. Many get up to 75 alerts a day, according to the research, leading to 'alert fatigue'.

"SMEs are in an uneven playing field," says Ian McShane, field CTO at Arctic Wolf, a leader in security operations. "Not everyone has the multi-million-pound budget to afford all of the latest cybersecurity technology. But these smaller organisations are too often used as the embarrassing case studies by vendors. It's frustrating when so called 'lessons to be learned' boil down to 'don't be like these idiots who couldn't afford it'. Vendors have a lot to answer for here.

> **The human element is critical to getting cybersecurity right. If you don't measure it, it's not managed.. Nobody wants to experience the huge cost and inconvenience of a ransomware attack**

"There has been this massive explosion in recent years in the sheer number of buzzwords, tools, products, platforms and security vendors. The number of solutions that companies are being convinced they need to invest in is pretty incredible. If organisations are using 10, 20, even 30 security products on average then there are a whole lot of things that can go wrong."

In the hype-fuelled cyber industry, it can often be forgotten that the threat landscape cannot be dealt with by technology alone. People and process are just as important, but this is also where the resource gap is exposed. Simply finding time to manage cybersecurity is a key problem for many SMEs, the Arctic Wolf research discovered, leaving them even more vulnerable to attack.

Over half of the business leaders surveyed by Arctic Wolf admitted cybersecurity issues are regularly deprioritised in favour of other business activity, while 34% said they don't have time to keep across every threat or alert. Those that fall victim to cyber attacks not only suffer short-term financial and operational impacts, but also long-term impacts on trust and reputation.

Even when companies do have the resources to invest in people, they are met by a cybersecurity skills shortage. There were 3.12 million unfilled cybersecurity-related roles globally last year, according to research by (ISC)^2. The shortage only exacerbates the resource gap even further, pushing up the expected salaries demanded by highly in-demand cyber talent.

"This isn't an industry that will be replaced by AI. People and process play a huge role" says McShane. "The human element is critical to getting cybersecurity right. If you don't measure it, it's not managed. If you lack the talent, whether through lack of investment or availability, ultimately you're playing security by chance instead of security by choice. You're hoping luck will prevail. Nobody wants to experience the huge cost and inconvenience of a ransomware attack."

Through outsourced security operations, Arctic Wolf helps thousands of companies end cyber risk by identifying, responding to and recovering from threats. The Arctic Wolf cloud-native platform is the industry's only solution that spans the complete security operations framework, including managed detection and response (MDR), managed risk, managed cloud monitoring and managed security awareness, delivered by the industry's original Concierge Security Team.

Arctic Wolf is now expanding its operations into the EMEA market, establishing a European headquarters in the UK with further plans to open a European Security Operations Center in Germany later this year while growing its presence in the Nordics and the Benelux regions. The global expansion comes after the company doubled its North American sales for an eighth consecutive year and secured a further $150m Series F financing round, valuing the business at $4.3bn.

"We're bringing the expertise, knowledge and context to help organisations do more with the people they have," says McShane. "Importantly, we're not trying to replace people – we augment what they do. And similarly, we're not trying to tell companies they need to buy more tools, platforms or products. All organisations have, at their disposal right now, enough security tools to improve their security posture, but they just need the assistance to be able to operationalise it. Arctic Wolf does that operationalisation at scale, and at a speed which is orders of magnitude faster than companies can do on their own, if indeed they can do it at all."

73%

of small and medium-sized businesses feel they lack the capability and expertise to withstand a cyberattack

39%

of businesses in the survey claim they are overwhelmed by the sheer volume of security alerts they receive, with the data revealing companies receive up to 75 alerts a day

55%+

of respondents admit they have ignored a known cybersecurity issue to prioritise another business activity

Arctic Wolf, 2021

That scale is partly delivered via Arctic Wolf's cloud-hosted platform, which does most of the heavy-lifting analysis. But there is also the human element, removing the worst elements of cybersecurity from the company's ownership into Arctic Wolf's ownership. By embedding their expertise within businesses on a day-to-day basis, Arctic Wolf's team understands not just the IT infrastructure of its customers but exactly how their company works, giving SMEs both the time and peace of mind to get on with running their business. This eliminates the burden of alert fatigue as well as drastically reducing the impact of a cybersecurity incident when it does occur.

"Ransomware is just going to get worse, and over the next year or so it's going to be a real wake-up call for almost every organisation," McShane adds. "Even if they are doing something now, every company needs to do more. Security isn't something that has a silver bullet. It's not something you can buy away. It's an ongoing journey; something that needs continual investment, measurement and management. We want to be that security partner for as many customers as possible and remove that unfair advantage that large organisations with big budgets and 24/7 IT staff have. We want to bring those advanced capabilities to everyone."

For more information, visit www.arcticwolf.com/uk

ARCTIC WOLF

DIVERSITY

Rainbow alliances

Some LGBT cybersecurity workers feel that they need to hide their sexuality and/or gender identity at work. What can their employers do to make them feel more comfortable and supported?

Finbarr Toesland

For people from many traditionally under-represented backgrounds, discrimination and lack of inclusion can make working in the cybersecurity industry difficult. This is reflected in the relatively low percentage of women and ethnic minority workers in the sector. Yet a recent report from KPMG and the National Cyber Security Centre has revealed that 10% of cybersecurity professionals identify as lesbian, gay or bisexual – significantly higher than the national average of 2.2% reported in 2018.

There is no simple explanation for this, but Berkeley Wilde, executive director of diversity and inclusion consultancy The Diversity Trust, believes that LGBT people are drawn to the cyber industry “because they know other members of their community work in the sector. The disconnect is in knowing that the sector attracts other LGBT people, yet discrimination still occurs.”

Diversity and inclusivity, it seems, do not go hand in hand.

The KPMG report bears this out, with 15% of gay and lesbian and 29% of transgender respondents saying that they have experienced discrimination at work. This can include being subjected to anti-LGBT language, misgendered or even excluded from social events. So what practical steps can organisations take to make their workplaces a safe space to be openly LGBT?

Wilde believes that the first step is to assess organisational policy. “For example, it’s important to ensure that maternity and paternity leave are inclusive of LGBT people. All policies need to be very explicitly inclusive of trans people and cover same-sex relationships,” he adds.

Reassessing recruitment and retention processes is also important. This can entail using representative interview panels that include LGBT staff members wherever possible. Exit interviews with LGBT employees can also provide valuable insights.

Acknowledging and celebrating events such as Pride Month and the International Day Against Homophobia, Biphobia and Transphobia can also make LGBT workers feel more comfortable and supported. But it’s crucial that these initiatives are not consigned to a single month, but instead celebrated throughout the year and accompanied by awareness training.

Recruiting and retaining a highly skilled and diverse workforce is essential in cybersecurity, especially as the industry continues to face a skills gap of about 3 million qualified workers, with 64% of professionals saying that their organisations have been affected by this shortage.

The *2020 (ISC)² Cybersecurity Workforce Study* highlights the business need to ensure that LGBT staff feel comfortable and secure in their jobs. Cybersecurity businesses that fail to address the challenges facing LGBT employees stand to lose out in the competition for talent, as offensive comments and discrimination drive people to more inclusive workplaces.

Rebecca Fox, a founding partner at digital and technology consultancy Gray Blue, has experienced both homophobia and sexism during her career in the technology sector. She can therefore well appreciate the difference that a supportive organisational culture can make.

“I came out in my late 20s in an organisation where it was relatively safe to be open about your sexuality,” she says.

Creating safe spaces at work for LGBT people requires businesses to improve their policies and processes, but this doesn’t need to be complicated. For members of the LGBT community, a safe space can simply mean being treated with respect and feeling comfortable discussing their personal lives without judgment.

The ability of positive representation to empower LGBT staff and attract talent should not be undervalued, Fox argues.

“If you’re working in an organisation where you see a role model like you, you’re inclined to stay. You’re not the token LGBT person or token woman; you’re just included,” she says. “Many firms have a cookie-cutter view of what a person in cybersecurity is – and it isn’t inclusive. It goes without saying that having a diverse workforce can better reflect your customer base.”

A 2020 research report from McKinsey entitled *LGBTQ+ Voices: learning from lived experiences* revealed that, while 80% of senior-level employees were ‘out’ at work, only 32% of junior employees felt comfortable with being open about their sexual orientation and/or gender identity.

“This tells me that the more you progress in your career, the more comfortable and confident you become with being open about your sexuality,” says Belton Flournoy, director at technology consulting practice Protiviti and co-founder of its UK LGBT+ group. “A thing you consistently find in many LGBT people, including me before I came out, is a lack of confidence.”

> **“If you’re working in an organisation where you see a role model like you, you’re inclined to stay. You’re not the token LGBT person or token woman; you’re just included**

Constantly policing your actions to avoid ‘outing’ yourself is common among younger workers, he says. “You devote so much energy to ensuring that you say the right things that you tend to be less real with people. When I stopped having to lie, all of a sudden I formed new relationships with most of the people I worked with.”

From a business perspective, if employees are expending so much effort on hiding elements of their identity, they aren’t working to their full potential.

“When I came out of the closet, my productivity shot through the roof. All my brainpower was focused on helping my clients find the best solution. I wished that I could tell others to try to get there sooner,” recalls Flournoy, who adds that every company should benefit from asking about employees’ confidence levels at work. “If we’re looking to drive meaningful change in our organisations, we need to be tracking the right information.”

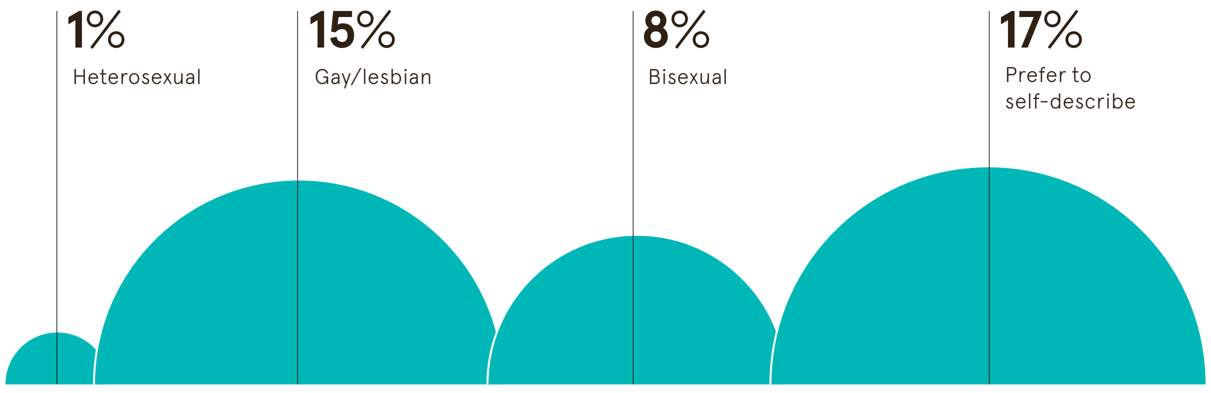
Protiviti analyses levels of diversity across the organisation, including at leadership level, and shares the results at its all-staff meetings. “This continued transparency is what allows our firm to see where we can come together to improve gender and racial diversity at all levels,” Flournoy says.

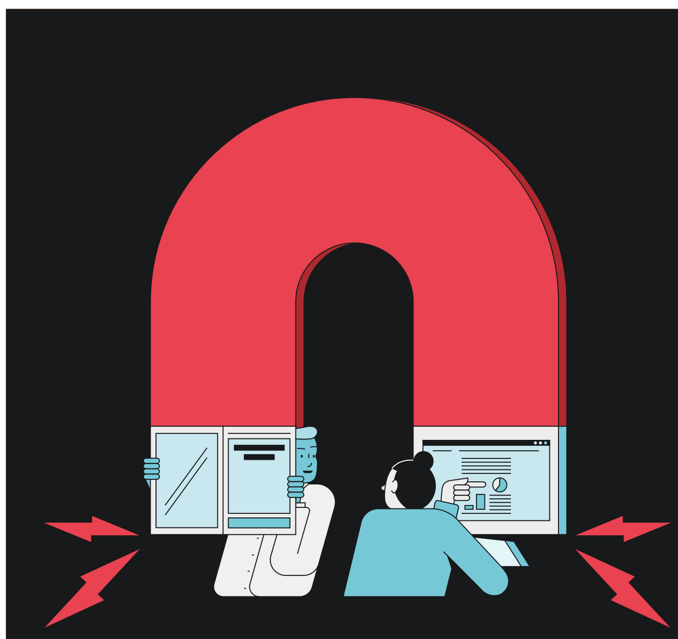
By using such data, organisations can spot where they are succeeding or failing when it comes to making LGBT employees feel a valued part of the company. This is the best possible first step towards building a more inclusive culture that both attracts and retains vital talent. ●

WHAT WORK LIFE IS LIKE FOR LGBT PEOPLE IN THE INDUSTRY

Percentage of cybersecurity professionals who say they have faced discrimination at work, by sexual orientation/gender identity

KPMG, 2020





TRAINING

Meet the ‘people hacker’ with all the tricks

Professed con artist Jenny Radcliffe has a very particular set of skills. Fortunately, she uses them to teach employees how not to invite cybercriminals into their organisations

Jenny Radcliffe: “The return to work is going to be a really challenging time for companies”

Sean Hargrave

The return of many businesses to office-based working is going to keep Jenny Radcliffe busier than normal. She soon expects to be talking her way into senior executives’ offices to remove a computer, photograph a password left on a Post-it note or attach a device that will tell her every word that’s being typed on a keyboard. If she’s lucky, she may even have time to install a ‘pineapple’ – a gadget that can snoop on a Wi-Fi network to steal passwords and other privileged information when users log into their work systems.

Fortunately, for any organisation on the receiving end, Radcliffe will do no harm. Instead, she will tell it where its employees need to be supported with better training. While she spends most of her time educating people in how to spot both online and face-to-face cybersecurity threats, her firm, Human Factor Security, is increasingly being asked to supplement lessons with some real-life testing of how well employees perform face to face.

“Trust me: the return to work is going to be a really challenging time for companies,” she says. “The other day I was sent to an office where the security guy came up and asked me what I was up to. I told him that I was running Covid checks and he should have received an email about it. I said I had to sanitise the equipment and so needed to be left alone. I even put down a yellow ‘cleaning in progress’ cone to make it look official. Sure enough, he left me to it. I was able to send my client photos from inside its offices to show how vulnerable it was.”

Radcliffe predicts that cybercriminals will use this sanitising ruse to get hold of laptops and smartphones, as well as planting listening devices, to gain access to private information or customer details that they can either sell on or, more likely, return to the business if a ransom is paid.

This kind of trickery is not restricted to physical premises. It has been happening online for years and has escalated during the past year or more. Radcliffe describes the pandemic as “the perfect storm”. People have been tired and distracted while using devices and Wi-Fi networks at home that aren’t as secure as those provided at work. It has made them unwittingly compromise their own security and, by default, that of their employer.

“People sometimes let the kids do homework or watch Netflix on their work laptops and have no idea if they have clicked on any pop-ups or links that might contain malware. We’ve all been tempted to ‘do a Hillary’, as it’s called in the business, and answer emails on a phone because it’s easier. The problem is that your phone is not going to be as well protected as your work laptop,” Radcliffe says.

> “We’ve all been tempted to... ‘do a Hillary’ and answer emails on a phone because it’s easier. The problem is, that phone will not be as protected as your workplace laptop is

The other factor making the pandemic the perfect opportunity for cybercriminals is that people are working in isolation at a time when they are emotional and fearful. This means that, unlike in the office, they might not always make the best decisions when an email appears to be from a legitimate company asking them to pass on a password or send money. These phishing attempts are the most common form of an attack on businesses and are now normally referred to as spear-phishing because a criminal will address the email to an individual and claim to be someone the recipient knows in their organisation.

“As part of my training sessions, I show people how simple it is to find out so much about a company and its people that you end up knowing better than they do who is working with whom on what project,” Radcliffe says. “It’s easy to obtain personal information about someone from social media too. You can make it look like you really know them and then refer to something they’re working on and ask them to send you some cash or the log-in details for the company’s network because you don’t have the password with you.”

Staff need to be trained to understand how sophisticated these attacks can be, to the point where a criminal will register a very similar domain name to the company they are attacking, perhaps replacing the letter ‘l’ with a ‘1’ or the letter ‘O’ with a ‘0’. Emails purporting to come from senior executives can look very realistic.

As cybercriminals have been refining their trade, employees have had the problem of working from home, with nobody to share their suspicions with.

“In the office, you can always go and ask a colleague: ‘Did you get this email too? Does it sound like Bob to you?’” Radcliffe says. “There’s almost certainly an IT person you can ask for advice too. But at home people have been distracted and feeling emotional, with no colleagues to talk to – and that’s what cybercriminals prey on.”

To train staff to spot potential cyber attacks, she has some simple questions everyone should ask whenever they receive an email, text, call or chat message asking them to help out a colleague.

“I have four red flags that I train people to look out for. If they spot one or more, they need to stop and check it out with a colleague or call the person who is supposedly asking them to do something,” she says. “Whether it’s a call or a digital message, if someone is using emotional language, asking you to make a snap decision or saying it’s urgent and it involves money, those are all the signs of social engineering. So you should stop and ask for advice.”

Aside from training, there are practical steps that Radcliffe suggests all clients and their employees should take to improve their cybersecurity. These actions may not all be new but they are hugely important, she argues. To start with, every piece of software on every employee’s computer, tablet and smartphone should always be kept up to date.

“People often don’t realise that these updates are security patches. A hacker may have found a way to get into people’s computers through an app and the developer has updated it to keep them safe,” she says. “So, even though it’s a pain, the training is to always update your software. If you can’t be bothered because you don’t use an app anymore, that’s a good reason to delete it. But you have to keep all your programmes updated, as well as your security software.”

Radcliffe knows that people will have heard it all before, but difficult-to-guess passwords are a must – and these shouldn’t be shared across different log-ins. One solution is to accept the strong security password that an app will suggest, which you have no chance of remembering, and then use a password manager to log back in. Using two-factor authentication is another obvious step that she trains people to adopt. Typically, a website or app will let someone log in only if they have both the correct password and a code that it sends to the owner’s mobile phone.

Her courses also come with a stark warning about using public Wi-Fi facilities. This should always be avoided in preference of sticking with a smartphone, which ought to have a sound 4G connection.

“People don’t realise how simple it is for anyone to set up a Wi-Fi hotspot in an area and name it after a local coffee shop to trick its customers into logging in,” Radcliffe says. “There’s software that anyone can install and then set themselves up as a Wi-Fi hotspot. All they need to do is call it ‘X coffee shop free customer Wi-Fi’ to sound convincing. The minute you log into it, everything you do using that connection can be eavesdropped on.”

If cybersecurity during the pandemic has been problematic, Radcliffe predicts that things could get a lot worse. Criminals will undoubtedly use the partial return to office working to target staff with Covid-related ruses, such as the sanitising scam. There is also the issue of devices that may not be working securely, and could have malware installed, being brought back into the office network. Moreover, people are going to be far more mobile, so the temptation to save their mobile data allowances and log into free public Wi-Fi hotspots will be high.

With the right training, though, staff can work far more securely outside the office, as long as they know how to better protect themselves, spot a cyber attack and, just as crucially, know whom they should approach to report their security concerns. ●

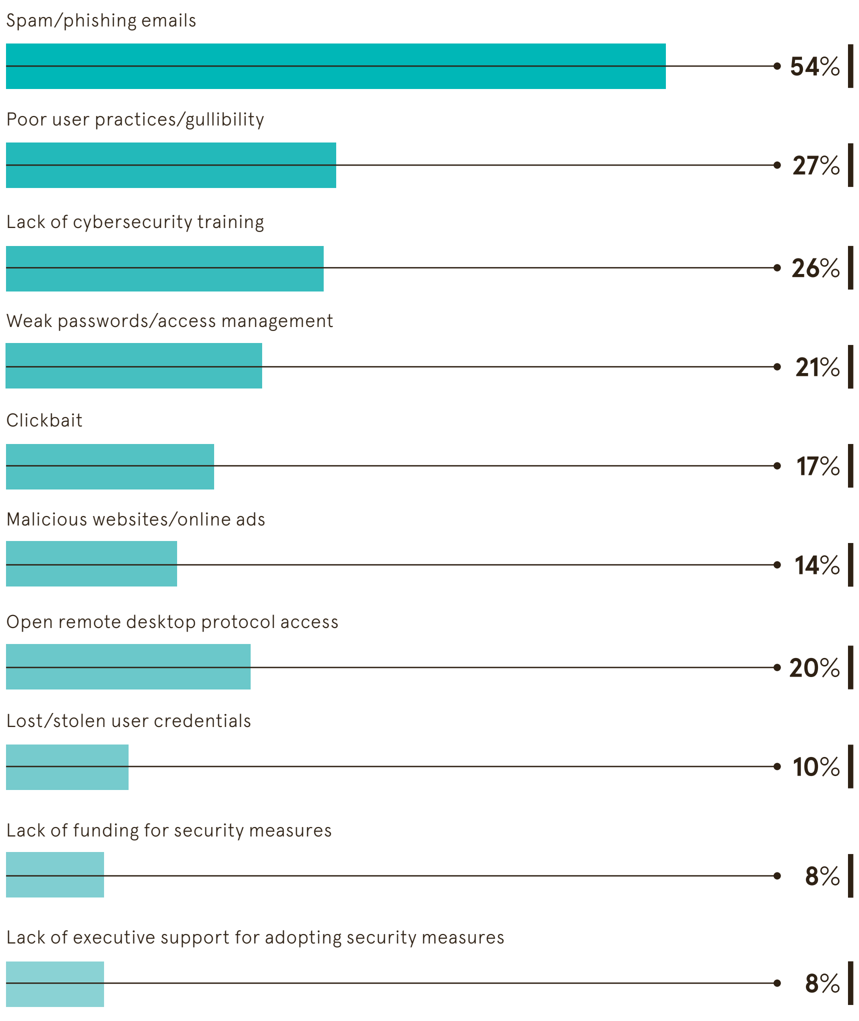
99%

of managed services providers predict that the number of ransomware attacks will increase in the next year

Datto, 2020

HUMAN ERROR TOO OFTEN CONTRIBUTES TO SUCCESSFUL CYBER ATTACKS

Percentage of managed service providers who say the following are the leading causes of ransomware attacks



Datto, 2020

Commercial feature

Keeping secure in the age of anywhere work

Sridhar Iyengar, managing director at Zoho Europe, outlines how cybersecurity practices need to evolve to support the ‘work from anywhere’ approach championed in hybrid working models

Q How has the cyber threat landscape evolved to become more dangerous?

A The average enterprise data breach costs $4.24m (£3.1m) in 2021, according to research by IBM, and that doesn’t account for reputational damage. Cyberattacks have evolved to become far more sophisticated – and lethal. Companies must protect their resources from various types of threats including ransomware, social engineering and distributed denial of service attacks. Bad actors not only prey on system vulnerabilities but human error, with most attacks originating from using weak or stolen passwords or people sending sensitive information to the wrong person.

Q How has the Covid-19 pandemic impacted organisations in a cybersecurity sense?

A Massive workforces had to switch to remote working in a matter of weeks, leaving organisations scrambling to adapt their infrastructure, tools and work culture to support it while ensuring data, device and systems security, and privacy of employee and customer data. Some are still dealing with those challenges, partly because only 56% of companies have changed their security strategy despite remote employees being directly targeted by malicious actors, according to a recent survey we conducted. Higher digital adoption means organisations’ people, assets and apps are more exposed than ever, increasing the overall risk score of businesses, especially those lacking security awareness, training and infrastructure readiness.

Q What are the specific security challenges as companies now embrace hybrid work?

A It all depends on the way you adopt the hybrid model, though all organisations should certainly be prepared for more cyberattacks and data breaches, including phishing and ransomware. There's an ever-growing challenge of monitoring user behaviour and securing endpoints. A data breach is, on average, $1.07m more costly when remote working is a factor causing the breach, IBM’s research found. That's not good news for IT teams, who are constantly on their toes trying to reduce the attack surface, keep compliance in check and systems up to date. Four in five IT leaders lack confidence in their organisation’s cybersecurity capabilities, according to research by IDG, so it is vital to invest in the right technology, hybrid working tools and security training.

Q How is ManageEngine helping organisations enhance their cybersecurity capabilities?

A ManageEngine has been around for close to two decades and it’s also part of Zoho Corporation, a web-based solution provider that uses its IT and security tools to manage its data centre and provide cloud business applications to more than 60 million users globally. Last year, we were given a week to go completely remote with 10,000 employees catering to millions of users worldwide and we pulled it off with ease. We used our own solutions to do that – solutions our customers can take advantage of too, including remote IT support, monitoring cloud infrastructure, managing privileged access and securing data, as well as increasing visibility across the enterprise network, servers and modern endpoints. We have more than 50 IT management and security solutions that are not only perfectly capable of keeping IT on track in a hybrid and remote work environment, but also help comply with major industry standards. We combine dynamic solutions with round-the-clock support.

Q What is the future of cybersecurity in the post-pandemic age?

A There's no such thing as 100% safe in the digital world and no one can predict what future attacks will be like. Organisations can only work on minimising the risks and controlling the attack vectors. They must not shy away from accepting vulnerabilities in their infrastructure. Instead, work towards minimising them, invest in the right solutions and always be prepared with a proactive incident response system. AI and machine learning will also play important roles in cybersecurity applications, improving real-time threat detection and providing automated incident response; that's what we have in our pipeline. ManageEngine will continue striving for agility in our solutions. Even the best cybersecurity solution is of little use if it cannot evolve.

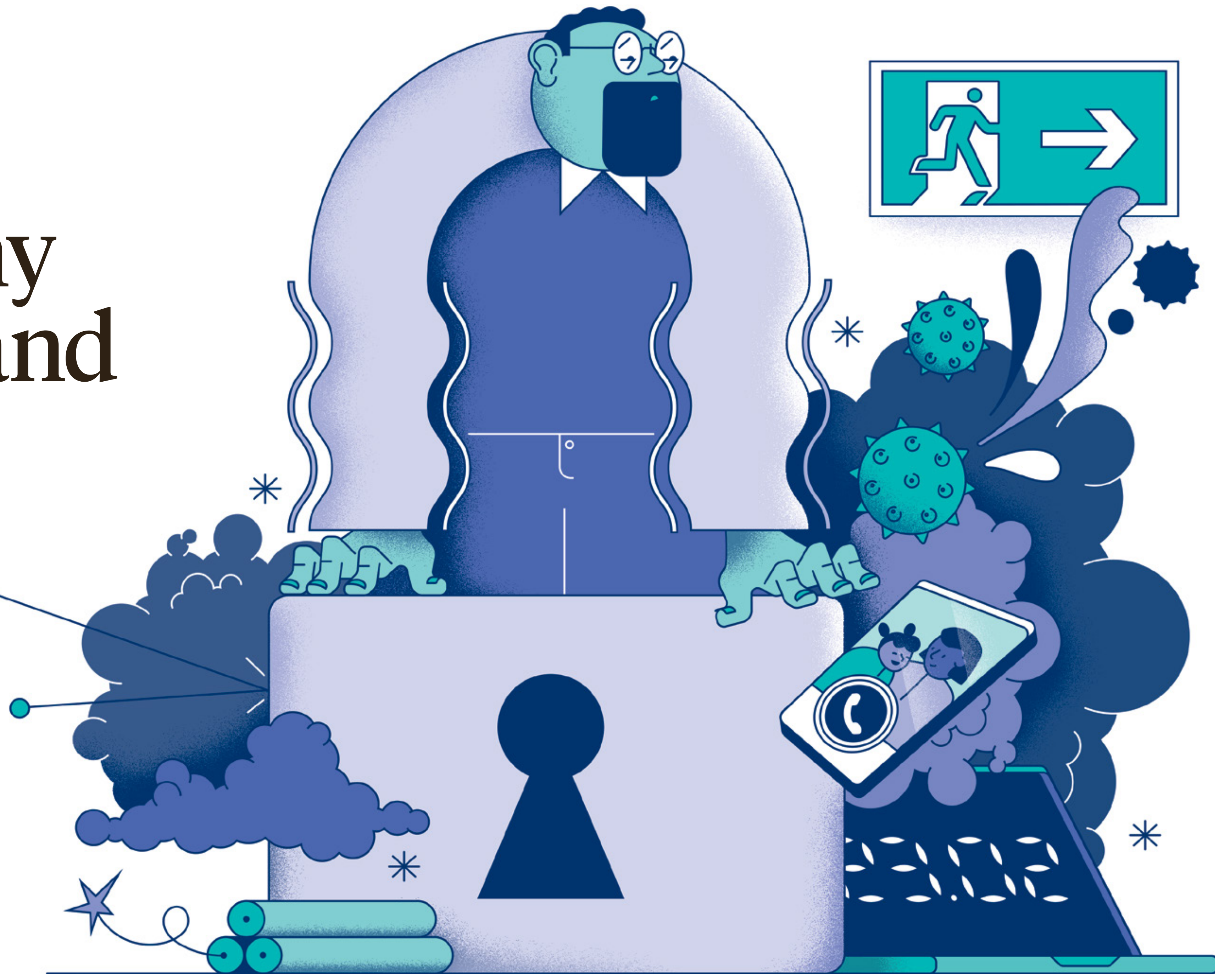
For more information, visit www.manageengine.co.uk

ManageEngine

RETENTION

CISO churn: why it's happening and how to stop it

Only a quarter of chief information security officers last a year in the job. What are the main factors behind this high turnover rate – and what can be done to reduce it?



Christine Horton

Recent research has revealed that 24% of Fortune 500 chief information security officers (CISOs) last only one year in the role, with the average tenure being a mere 26 months. C-level positions necessarily involve higher levels of responsibility and stress than other roles impose, but why is it so much worse for security executives than for their peers in finance, HR and marketing?

The simple answer is that security teams are under an incredible amount of pressure – arguably, more so than any other department. A typical data breach can cost an organisation more than £3m, which could cripple some completely or set them back years in terms of financial performance. That's a lot of weight for CISOs to shoulder, particularly if they're constantly fighting against the rest of the business.

"The high churn among CISOs is no surprise to me," says Anthony Young, co-CEO at security and risk consultancy Bridewell Consulting. "It's a very difficult position, with typical challenges including a lack of authority, budget and support from the executive team, which still sees security as a cost rather than an enabler."

He cites the following main factors behind the high churn rate among CISOs: fear of a breach and inability to do their job successfully; stress and burn-out; and being tempted to move by offers of better money and working conditions elsewhere.

"Many leave an organisation because they feel they don't have the tools or support they need to do their job properly and that a breach is inevitable. They want to leave before this happens and tarnishes their careers," Young says. "It's also quite common for organisations to recruit a CISO and expect that person to solve all their security problems, effectively pitching them as a lone superhero. Such pressure, along with the expectation on them to take responsibility for aspects such as system configurations, risk assessments and vulnerability scanning, can cause high levels of churn among CISOs, who are unable to meet unrealistic expectations."

Young adds that getting boards to understand the return on security investments can also be an uphill struggle.

"This results in stress among CISOs, who are fully aware that their current security measures aren't sufficient and are working all hours to protect their organisation. The weight of this responsibility means that it's not uncommon for CISOs to find their personal lives hugely affected by the stress."

Paul Watts is group CISO at Kantar, a data analytics and brand consultancy. He notes that "hackers don't work fixed hours. This factor tends to ripple into security teams and their leaders. You are never truly off the clock as a CISO. Last year, CISOs were working, on average, 10 hours per week beyond their contracted hours. During the lockdowns, this appears to have increased for a number of CISOs. I was regularly working 12- to 14-hour days, certainly during the first lockdown.

Watts continues: "This puts a strain on personal commitments and family dynamics. I have heard numerous cases of CISOs having relationship problems with their partners and children. This is amplified for CISOs who work for multinational organisations, where there's an expectation that the security chief is always available."

Moreover, Watts says that in terms of rewards and benefits, CISO salaries are low in comparison with those of similar senior roles, especially when the levels of responsibility and stress are taken into account.

"CISOs can feel vulnerable and lonely in their roles – it can be seen as a thankless job. They are also at moderate risk of becoming the immediate scapegoat if a security breach occurs, even though it's highly unlikely that the fault was directly theirs, especially if the root cause was underinvestment or a poor culture."

Regarding responsibility, Watts also points out that there is a noticeable difference between the CISO and CIO (chief information officer) when a security breach occurs. "How many CIOs lose their jobs when an organisation suffers a major outage? The answer is: not many."

Even before Covid-19, the CISO's role was fraught with difficulties, according to clinical psychologist Dr Nick Taylor, CEO and co-founder of workplace mental health platform Unmind. He points to a recent report which shows that 88% of CISOs feel moderately or tremendously stressed dealing with their high-pressure, high-demand and high-stakes job.

"The pandemic has compounded this already high level of stress and the risk of burn-out," Taylor says. "The move from the office to working at home has created uncertainty alongside the constant responsibility of safeguarding their company from security threats. In fact, almost half of CISOs say that work stress has had a detrimental impact on their mental health."

Killian Faughnan has been group CISO at online gambling company William Hill for two years and eight months. He believes that a large part of the high CISO churn rate is frustration at a lack of progress.

Faughnan explains: "Many CISO activities are long-term iterative improvement programmes, solving fundamental problems that were never addressed properly, with some occasional firefighting thrown in for good measure. It can be hard to feel a sense of accomplishment without stopping to deliberately take stock."

The churn becomes a bigger problem when each new CISO demands a reset of strategy, priorities and commitments, with old plans torn up and new ones established.

"While a refresh is often necessary, with CISO churn rates of less than two years, it also means you never get to the bottom of some of the more fundamental security challenges," Faughnan says. "I've found that most roadmaps from the previous CISO's term were not far off the mark, so I prefer to fight to keep those same fundamentals. Then, the CISO after me shouldn't inherit any insurmountable challenges."

Tash Norris has been head of cybersecurity at online greeting card and gifts firm Moonpig for nearly two years. In that time, she has led the security team and wider technology function through a demerger and a stock market flotation.

"Where I've seen CISOs have short tenures, it's often because the business isn't fully committed to security as an ongoing programme of work," Norris says. "A lot of CISOs are really at the mercy of the product and technology teams, which prioritise and implement security fixes and, quite often, the prioritisation of those fixes are neither well understood nor well communicated,"

> “
> **Hackers don't work fixed hours. This factor tends to ripple into security teams and their leaders. You're never truly off the clock as a CISO**

She adds that this can mean that security teams find themselves being held responsible for security events that they not only foresaw but also actively lobbied to fix.

"It is this pressure that causes many CISOs to feel that they don't have the right level of influence in their organisations to be effective and successful in their roles. As a result, they choose to leave. CISOs require both accountability *and* authority to be effective, not just accountability."

Norris notes that security is considered an enabling function at Moonpig. "This helps to ensure not only a secure product but also my enjoyment of the role, which ultimately reflects in my tenure," she says.

24%

of Fortune 500 CISOs have been in their current job for an average of one year

10%

have been in their position for an average of four years

Cybersecurity Ventures, 2020

And, while she agrees that other C-suite positions experience high stress levels resulting from a lack of resources, for the CISO this issue could ultimately lead to negative media coverage of their company, regulatory sanctions and, worse still, ramifications for its customers.

"The success of your CISO very much depends not only on the financial investment in their function but also the support they receive from their peers across the business," Norris says.

So is there anything that organisations can do to help stop the churn? Taylor says that, when it comes to employee retention, there aren't any shortcuts.

"Principled leadership; an inclusive organisation; accessible and empathetic support; and openness about mental ill-health are all fundamental factors in creating an engaged, healthy and happy culture, particularly at C-level," he says. "Employers can take practical steps to support these areas among their workers and provide them with tools to help them nurture their own mental health. But the problem of high churn rates among CISOs won't go away until businesses tackle the root causes of their unhealthy stress levels head on."

Watts believes that company boards should give CISOs impartiality and independence, allow them direct access to the board and audit committees, as well as recognising them as trusted advisers.

"Regulators and governments should continue to reinforce with business leaders that the buck stops with them when it comes to security and risk management," he says. "Ideally, legislation should support the CISO in being fully effective in their role and not the sacrificial lamb."

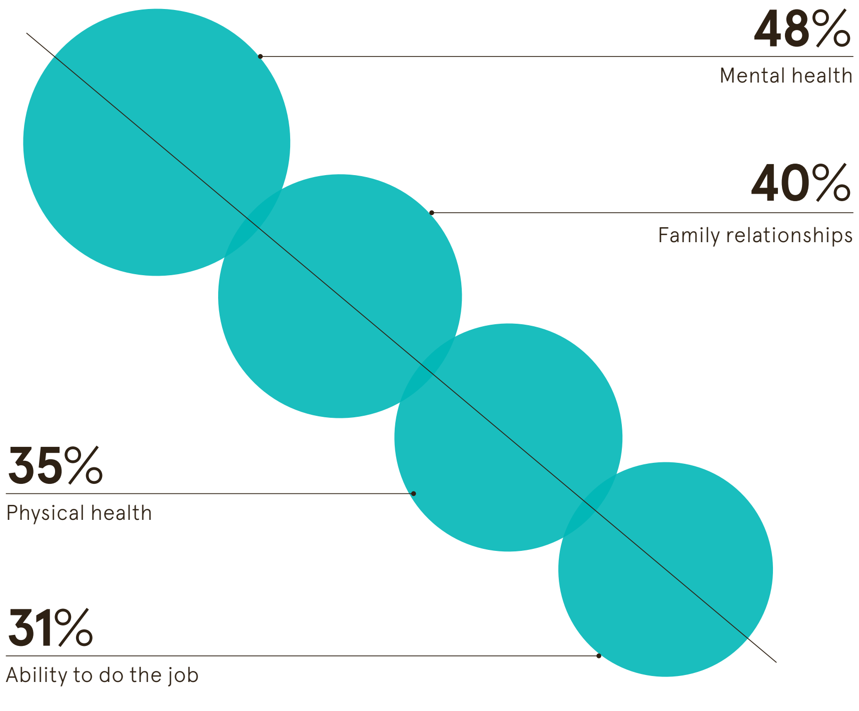
Watts also advocates for CISOs to spend more time connecting with, and getting the support of, the business. Ideally, too, those holding the purse strings should give the CISO the headcount and "bandwidth" they need to do their job effectively, meaning people, money, tools and other resources.

In return, CISOs should be more articulate about their vision statements and be able to express these in a language that resonates with the board. And, if they can, CISOs should recruit skilled people into specific leadership positions in the security team and then trust and empower them.

Embedding continuous improvement requires a consistency that could be lost with a regular changing of the guard. Businesses therefore need to ensure that CISOs have the right authority, budget, talent and technology to do their job effectively – and help to stop the churn.

CISOS ARE FEELING THE PRESSURE

Percentage of chief information security officers in the US and UK who reported that their stress levels had affected the following things



Nominet, 2020

Commercial feature

Why data is safer in the cloud

The expertise, innovation and resources available from cloud providers are hard to match on-premise

Digital transformation and the rapid shift to home working during the pandemic have pushed cybersecurity up the corporate agenda. In fact, it's now rare to find a business that doesn't consider powerful security a top priority. So how can they ensure their data is backed up, protected and only available to the right people?

Here's the short answer: use the cloud. In the age of distributed workforces and ever-increasing cyber threats, it's the best way to ensure that important data is secure and accessible only to those who need it, when they need it.

Because cloud providers continuously update their servers to combat the newest cyber threats, they're able to stay two steps ahead of hackers too. By contrast, on-premises solutions can be harder to protect, straining finances and resources. And don't forget that on-premise servers are more prone to break-ins or natural disasters too.

It's therefore hardly surprising that almost nine in 10 businesses surveyed for Epicor's recent Industry Insights Report believe their data is safer in cloud-based solutions. So have fears that migrating to the cloud involved a loss of control over your data finally faded away?

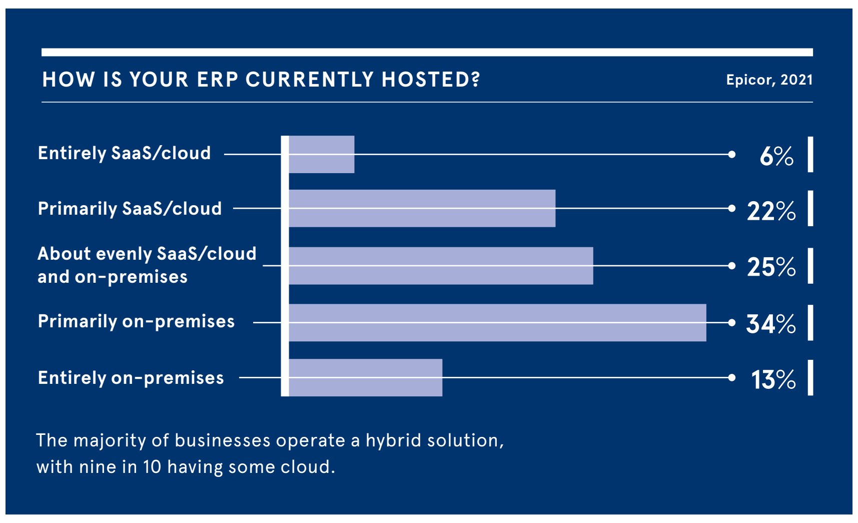
"Cloud usage continues to grow at a rapid clip in virtually every vertical and across all geographies, a very good indication that many of the myths about cloud security risks have been successfully dispelled," says Rich Murr, chief information officer at Epicor, which provides cloud ERP and business management solutions to the world's most essential businesses. "Where they do persist, it's often a reflection of an outdated understanding of cloud providers' security capabilities."

Cloud providers know that earning their customers' trust and business means their security offering must withstand intense scrutiny, and have invested large sums to ensure that it does.

"While the same robust security capabilities that cloud providers offer can also be implemented and operated on-premise, the cost and level-of-effort to do so is highly prohibitive. Whether it's encryption, multi-factor-authentication, web-filtering, intrusion detection and prevention, or the dozens of other security technologies needed for a layered defence, cloud providers offer a level of technical prowess and scale that is increasingly difficulty for all but the largest of enterprises to duplicate," says Murr.

HOW IS YOUR ERP CURRENTLY HOSTED?

Epicor, 2021



The majority of businesses operate a hybrid solution, with nine in 10 having some cloud.

Epicor's report revealed that businesses consider encryption and multi-factor authentication to be the cloud's two most useful security features, with monitoring a close third. When you consider that cloud security patches and management tools are constantly being updated too, it's easy to see why businesses that want to protect themselves from security issues know that a cloud solution is the way to go.

With the cloud, data is consistently backed up in separate servers that are often thousands of miles apart. By contrast, backups and redundancy are often found to be lacking with on-premise solutions at the worst possible moment – for example, when they're needed to recover from a hardware failure, ransomware attack, data corruption, or another event that renders a system unusable.

"SaaS providers design a level of data protection into their solutions that is highly reliable, and IaaS providers offer numerous data protection options that can be leveraged to virtually guarantee your data can be retrieved and restored in the event data is compromised," says Murr.

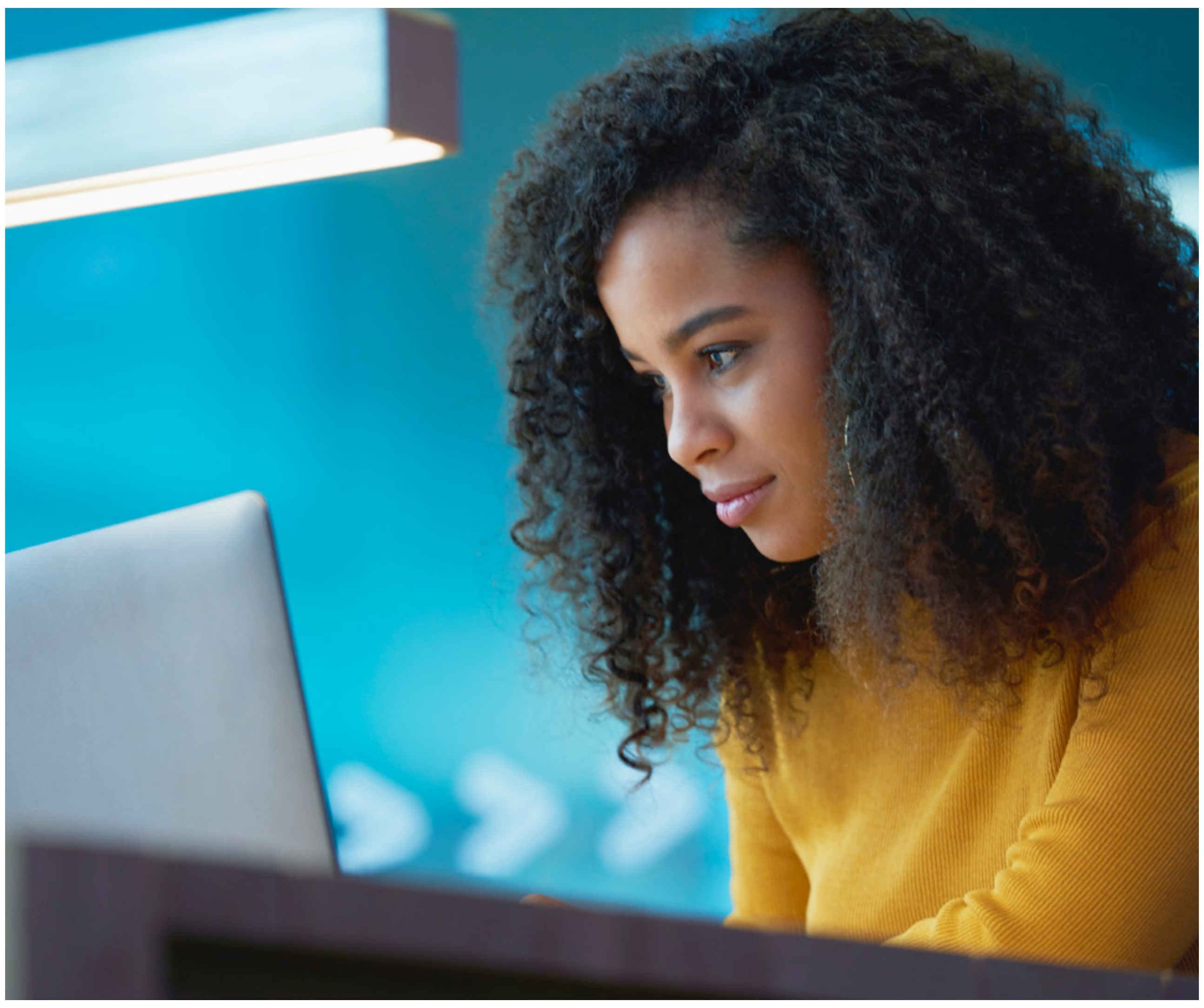
Migrating to the cloud can streamline compliance with data security regulations too. "Most enterprise-class cloud providers insulate customers from the underlying technical complexity associated with designing, delivering, and operating compliant solutions, allowing customers to more easily and cost-effectively achieve compliance than attempting to do the same with on-premise solutions," says Murr.

Ultimately, no business can afford to cut corners when it comes to the security of their data and systems: the cost of regulatory fines and risk of reputational damage is simply too high. But thanks to the cloud, they can rest assured that their data is secure, easily recoverable and protected against the latest threats.

Please contact us at www.epicor.com

EPICOR

Commercial feature



RETENTION

How CISOs can steel themselves for short tenure

Considering the often limited time spent in the job, do chief information security officers need to approach the role differently from the rest of the C-suite?

Christine Horton

Given that short tenures have become common among chief information security officers, incoming CISOs may need to adopt a different approach to their role compared with the rest of their C-suite colleagues. For example, they may feel that it will affect how quickly they need to implement their plans, as well as the impact these can make on their organisation's security strategy. Yet problems can result if a CISO becomes too preoccupied with making a near-instant impact because they don't expect to stick around for long.

"Those who are concerned with making a big impact in a short time will often use a cookie-cutter approach by recycling strategies implemented in previous roles," says Paul Baird, chief technology security officer UK at Qualys, a cloud software vendor. "Problems will occur in such cases, because each business is different, with its own unique set of priorities and challenges. An approach that worked for one company therefore won't necessarily work for another. Good CISOs use their experience to inform the approach they take in their new role while recognising the differences and catering to those accordingly."

If a CISO enters a new role already convinced that they will be out of the door in a year or so, it can be difficult for them to form an effective rapport with members of their team and other colleagues. Here, emotional intelligence is key. But it's a skill rarely considered in the hiring process.

"If CISOs operate on a short-term mindset, they're likely to enter the organisation hard and fast, upsetting the status quo of the security team and other business units. A skilled CISO will instead strike the right balance, understanding what motivates their team and colleagues, and using this insight to drive change," Baird says.

To prepare themselves for a short tenure, CISOs need to fully understand the company's culture, structure and goals from the outset. First, this means ensuring that expectations are well communicated and understood at the interview stage, says Anthony Young, co-CEO at security and risk consultancy Bridewell Consulting.

"Second, CISOs need to establish a comprehensive plan of action very quickly, agreeing with the board what is realistic within a set timeframe," he says. "This also has to include any crucial resources that they will need to achieve their goals, as well as the budget required."

Third, a new CISO needs to prioritise demonstrating the potential return on their firm's cybersecurity investment.

"Having good security credentials and robust processes can open up markets and revenue streams that were previously impossible for the business to attain," Young says. "CISOs must ensure that this is at the forefront of the board's mind by putting in place the right strategy, clear communication channels and using the right technology to optimise investments."

THE AVERAGE CISO IN THE UK...

... earns

£88,324

a year

... gives back their employer

£19,873

in unpaid work a year

... would sacrifice

£7,509

a year for a better work/life balance

Nominet, 2020

> If CISOs operate on a short-term mindset, they're likely to enter the organisation hard and fast, upsetting the status quo of the security team

But CISOs might be better served by adopting a different approach. It's one that acknowledges the strategic importance of their role in the organisation – and their need to spend a reasonable time there to make any positive and lasting impact on the business and its people.

It's also worth noting that cybercriminals are only too happy to play the long game and wait for gaps to appear as new CISOs implement their changes.

So instead of thinking about how they can prepare themselves for a short stint, there are some ways CISOs can dig in for the long haul. The first is to conduct an IT and security due-diligence exercise during the interview process.

"Ask for things such as the organisation chart; the IT strategy; the main technologies being used; the governance model in place; details of team members and their profiles; the delegation of authorities that would follow; and the CISO's budget." So says José María Labernia, head of IT security and internal control at building materials manufacturer Holcim, who adds: "This will help the CISO understand the state-of-the-art situation and so avoid unpleasant surprises once it's too late."

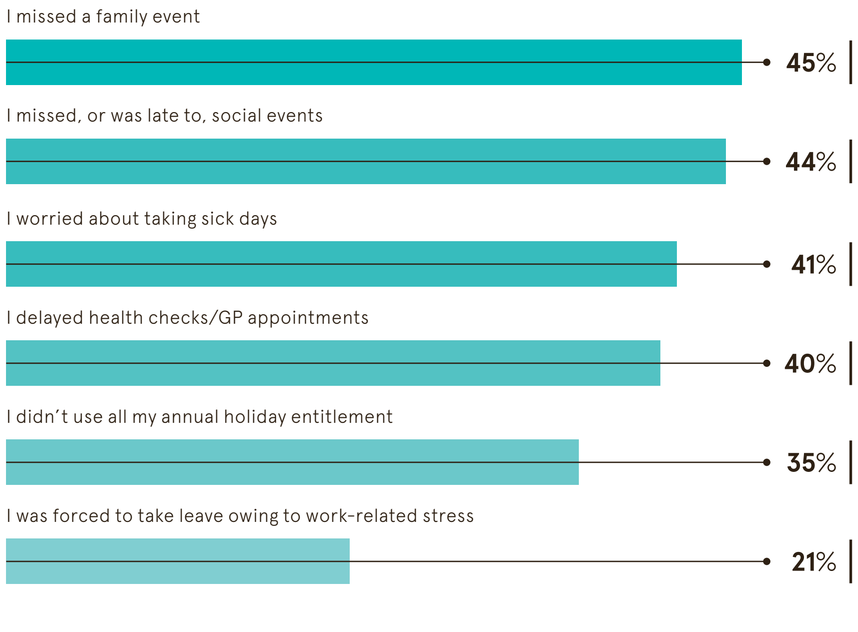
The second task is to establish sound mid- and long-term incentive plans during the negotiation phase, which should help, over time, the CISO to ignore competitive offers from the employment market.

The third, Labernia says, is "to meet the CEO and/or the executive member in charge of IT during the selection process. Try to understand their real concerns and commitment to IT security, then work with them to define some key metrics and milestones to focus on during the first six, 18 and 36 months in the job."

High churn has become the norm in cybersecurity. And, although it is possible for a CISO to make a positive impact on an organisation relatively quickly, it's important for both the business and the CISO to recognise the potential limitations that come with short tenures. ●

THE CISO'S LACK OF WORK/LIFE BALANCE

Percentage of chief information security officers in the US and UK who said they had or hadn't done the following things as a result of work commitments in the preceding 12 months



Nominet, 2020

Tackling tech abuse: protecting people from 'stalkerware' and cyberfraud

Access to the right tools and information can empower people online to protect themselves from tech threats and enjoy true digital freedom

Technology is a powerful tool and the online world served as a real lifeline for many in the pandemic. However, it also provides some people with a new way to stalk, isolate and control women, as well as target and take advantage of some of the most vulnerable people in society.

Research by Avast, a global provider of digital security and privacy products, revealed a huge increase in the use of stalkerware and spyware apps in the UK since lockdown measures were first introduced. The volume of stalkerware and spyware apps in January and February of this year increased 93% on the same period in 2020 before Covid restrictions came into force.

"Depending on which country you look at, sometimes it's a 300% rise, sometimes it's a 100% rise," says Jaya Baloo, chief information security officer at Avast. "It's a dramatic difference from the year before, and we think it's been brought about by the pandemic."

Alarmingly, the growth in stalkerware seems to echo the increase in domestic abuse cases across the UK since lockdown measures came into force. Refuge, which provides specialist support for women and children experiencing domestic abuse, reported that between April 2020 and February 2021 calls and contacts logged on Refuge's National Domestic Abuse Helpline (NDAH) were up by an average of 61%.

Stalkerware apps give abusers another way to exert control over their victims. Often advertised for monitoring children, employees or loved ones, they are generally installed on the victim's phone by jealous spouses, abusive ex-partners, or so-called friends. The perpetrator can potentially gain access to a victim's photos, videos, emails, texts and WhatsApp and Facebook messages, as well as eavesdrop on phone calls and make covert recordings of online conversations.

"These apps act as a trusted party on the device, like any app that would have full permission, and therefore they can do multiple things," says Baloo. "So it's not just about tracking the victim's physical location." Once installed on the victim's device, stalkerware is also incredibly hard to detect. "You don't receive any alerts. It's surreptitiously running in the background, so it requires some significant skills [to discover and remove]."

As well as partnering with Refuge to support its Tech Abuse support line, the company is also a member of the Coalition Against Stalkerware, a cross-industry organisation committed to raising public awareness about the issue. Avast continuously monitors and reports stalkerware apps. For example in 2019, Avast mobile threat researchers identified and worked to remove several stalkerware apps from the Google Play Store.

"We want to be on both sides of the timeline, making sure that appropriate protections are employed before there's ever a victim, trying to get rid of the companies that make this [stalkerware] possible in the first place, and educating victims about what you can do to make sure you don't get revictimised," says Baloo.

Protecting the most vulnerable in society

As well as the growth of tech abuse within relationships, cybercriminals are also actively targeting the more vulnerable in society. Romance fraud, government and bank impersonation schemes and tech support scams all aim to exploit a group that are online more than ever before, but which sometimes lack the knowledge, skills and confidence of younger generations or those who are more digitally savvy.

To tackle the issue, Avast teamed up with Neighbourhood Watch to create a joint Cyberhood Watch initiative. Together, it helps members and volunteers learn more about the cybersecurity risks that exist online, and provides clear, simple tips on the steps they can take to protect themselves.

> Over a third of Neighbourhood Watch members are now more concerned about cybercrime than physical crime

93%

increase in the volume of stalkerware and spyware apps in January and February of this year, versus the same period in 2020, before Covid restrictions came into force

Research by Avast and Neighbourhood Watch found that over a third of Neighbourhood Watch members are now more concerned about cybercrime than physical crime. "We knew there was a concern, but we were quite surprised at the level of it," says John Hayward-Cripps, CEO of the Neighbourhood Watch.

According to a survey of 28,000 Neighbourhood Watch members, 18% have been victims of cybercrime in the past year, while 33% know someone else who has. In terms of financial impact, over a third of victims (36%) lost money and of them, 23% lost more than £1000. A further 39% of the 28,000 members polled had experienced an increase in the number of targeted phishing attempts. The majority of these crimes were kept secret by the victims, with only 27% reporting the incident to the police.

This seems to indicate a general lack of confidence in talking about cybercrime experiences within the community, as well as a gap in understanding the best methods for protecting yourself online. "None of us want to admit we've been daft, even though the reality is that scammers are really good at what they do," says Hayward-Cripps. "If it wasn't successful, they wouldn't do it."

One of the unique features of the Cyberhood Watch initiative is its network of community ambassadors, who help to initiate conversations about cybersecurity. "These are ordinary people that have been trained to act as a kind of hub, talking about these issues to local groups or answering questions that people have got locally," says Hayward-Cripps.

Examples of what people can do to protect themselves online include not opening links or downloading items from unknown senders, as well as installing a solution like Avast Mobile Security. Similarly, there are steps women can take to detect and protect themselves against stalkerware, including protecting their phones with biometric logins, unique pins or passwords, and installing antivirus software that will alert them to any attempt to install stalkerware and help them remove it.

"The most vulnerable part of the population can actually protect themselves relatively easily. But they just don't realise that they need to deploy some basic mechanisms to do so," says Baloo, who feels that many digital security firms have "cultivated an environment of fear around technology without cultivating equal transparency in terms of what you can do to reduce that fear."

In other words, while stalkerware and scams pose a very real threat to vulnerable people, with the right information and tools anyone can become a confident and empowered digital citizen, and enjoy all the benefits that technology has to offer.

For more information please visit:
www.avast.com
For further information on Avast's Cyberhood Watch programme please visit:
www.avast.com/uk-cyberhood

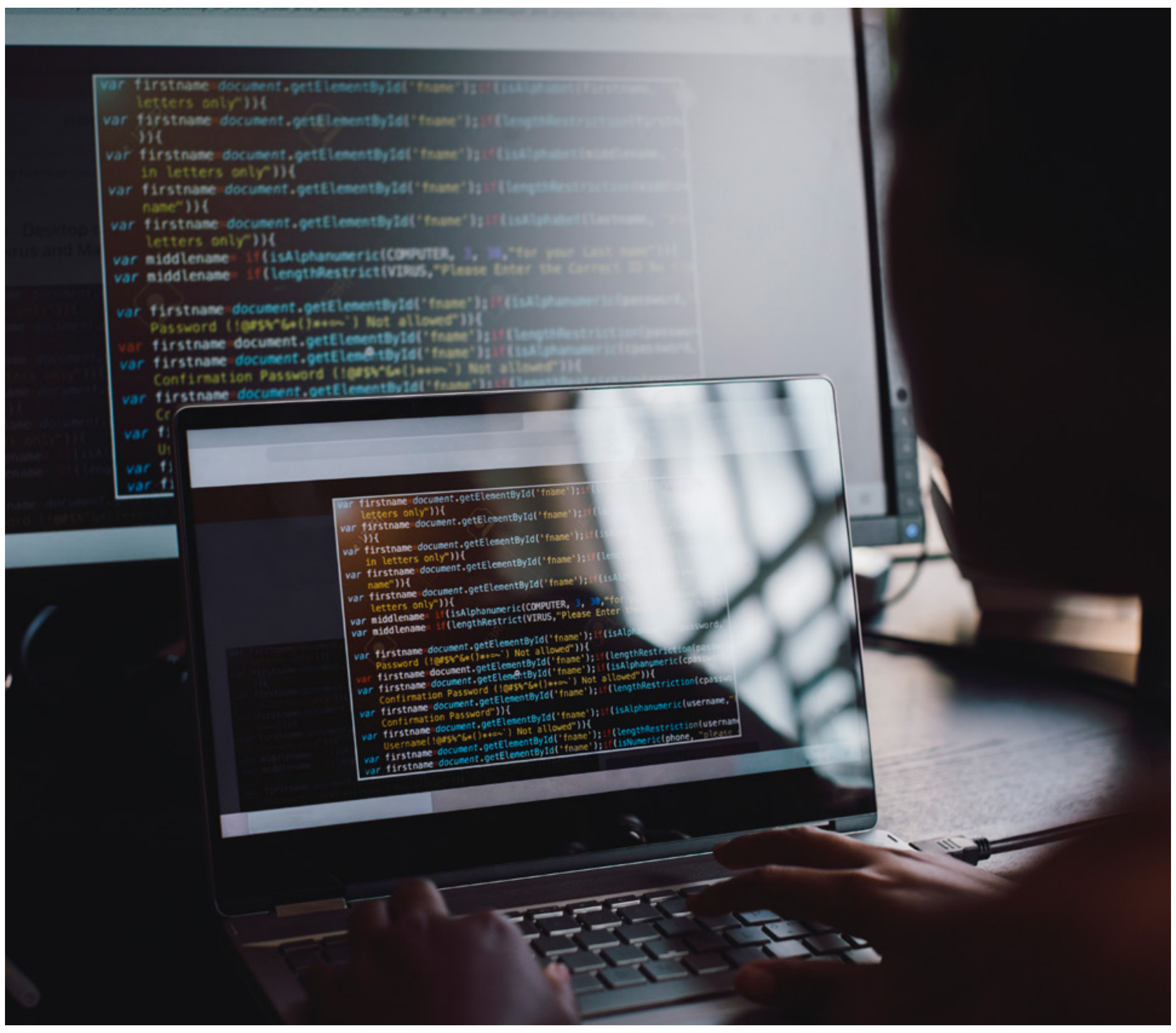
avast

ENCRYPTION

The solution to the locked-room mystery

How can companies analyse data in the cloud without compromising security and privacy? Homomorphic encryption makes it possible

Ouida Taaffe



In a 'locked room' mystery, a crime has been committed in a room that no one could have entered and the reader has to work out what happened. Spoiler: the room was never as secure as it seemed. Unfortunately, real-life data crime has much the same plot. Unencrypted data is never really secure, no matter how good the locks on the perimeter may appear.

The obvious solution to that, of course, is to keep data encrypted. But what happens when you need to use it? Until recently, the need to have data in plain text to be able to analyse it was an insurmountable security problem – particularly on the cloud and when data was being shared. But now firms say that there is a way to have secure data-sharing and collaboration. It's called homomorphic encryption.

This has long been the holy grail of cybersecurity. IBM's cryptography expert, Craig Gentry, has defined it as how a "third party can perform the complicated processing of data without being able to see it".

He gives the analogy of a jewellery workshop with a locked box of precious materials that only the owner can open. His employees can access the box using gloves to assemble the jewellery but cannot take anything out, leaving the completed piece safe.

Homomorphic encryption is similar in that it lets data processors manipulate selected 'raw materials' such as sales figures or medical data, but keeps the plaintext data private. That is because the data doesn't have to be decrypted to be used. Only the end result of the computation is presented in plain text. Because homomorphic encryption is mathematically and computationally very challenging, it was an intriguing theoretical discussion long before it became a practical option. And it is still in development.

> “Unencrypted data is never really secure, no matter how good the locks on the perimeter may appear

"There are no theoretical limits to the computations that can be carried out using homomorphic encryption," says Ellison Anne Williams, the founder and CEO of Enveil, a firm that specialises in privacy-enhancing technologies. "But there are some practical constraints."

In particular, homomorphic encryption is still limited in the functions it can perform and needs a lot of processing power to work.

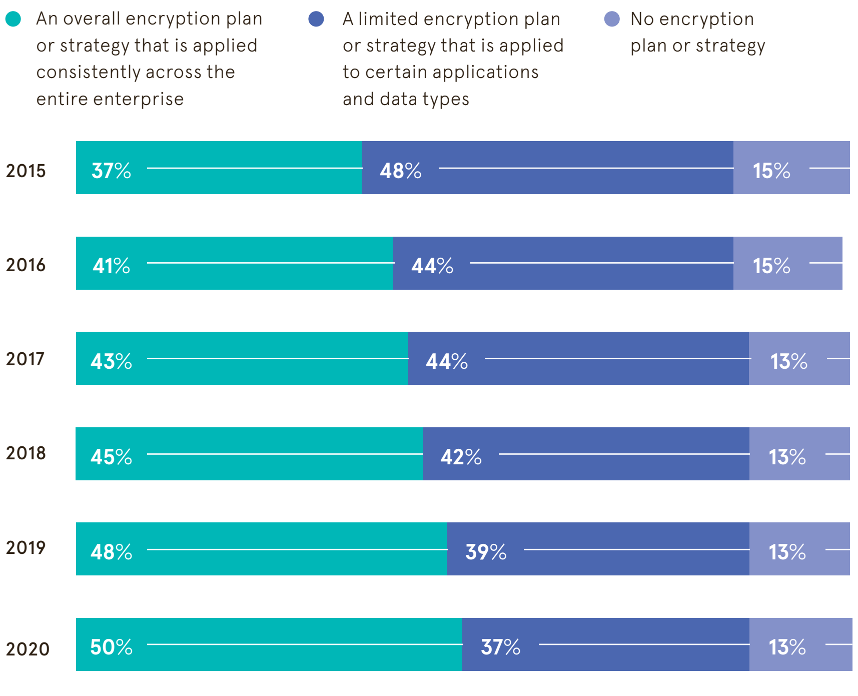
Given that analysing data you can't see seems to require both a leap of faith (at least for non-mathematicians) and significant resources, why use it? Williams says that Enveil "doesn't ask clients to press the 'I believe' button". Instead, it provides frameworks and tools to verify the analysis and to help people understand what's going on.

Use cases are also becoming increasingly evident. Robert Schukai, executive vice-president of technology development, fintech and new infrastructure at Mastercard (an investor in Enveil), said in his keynote speech at the 2021 Secure and Private Compute Summit: "Homomorphic encryption is a phenomenally exciting technology. We see great value in querying data where it lives… It is an ideal technology when you are dealing with sensitive data that you don't want to sling around but would prefer to leave in its location."

Companies will often need to interrogate information that is not stored on their own systems. Big multinationals, for example, share information across borders. Homomorphic encryption allows them to do that while still complying with local regulatory requirements because what is moved around is the analysis of the data. The data itself stays put and remains encrypted.

THE IMPORTANCE OF ENCRYPTION IS GETTING THROUGH TO BUSINESSES

Percentage of global IT providers that say their company has an encryption strategy



	An overall encryption plan or strategy that is applied consistently across the entire enterprise	A limited encryption plan or strategy that is applied to certain applications and data types	No encryption plan or strategy
2015	37%	48%	15%
2016	41%	44%	15%
2017	43%	44%	13%
2018	45%	42%	13%
2019	48%	39%	13%
2020	50%	37%	13%

Ponemon Institute, 2021

Homomorphic encryption is already being used by those large companies that can afford to pay for, and value, the use cases. Williams points out, for example, that ransomware goes after data at rest, so firms would be well advised to keep data permanently encrypted if they can.

Homomorphic encryption promises that data never has to be moved or presented in plain text. Even if there is a perimeter breach, the data is safe. But is homomorphic encryption itself a securely locked room? What about quantum computing, which is powerful enough to break many of the cyphers now in use? Williams says that even quantum computing won't be able to crack homomorphic encryption because it doesn't rely on factoring huge numbers.

Unsurprisingly, given the technology's potential, the big cloud players are all active in homomorphic encryption. Microsoft, for example, offers Microsoft SEAL (which stands for simple encrypted arithmetic library and does what it says on the tin). It is a set of 'encryption libraries' designed to help software engineers build end-to-end encrypted services. The open-source technology aims to make homomorphic encryption easy to use and available to everyone, not only people with a deep understanding of the complex maths.

Google opened its fully homomorphic encryption library in June this year. Again, the aim is to bring everyone on board with open-source software. Google's solution is a transpiler that turns code for "any type of basic computation… into a version that can run on encrypted data".

Miguel Guevara, a product manager in Google's team, says: "Up to our release, you needed to be expert to produce things on top of encrypted data. This tool lets any developer do it. You no longer need a PhD in the field." But there may still be a big gap between a library that developers use and a solution that businesses can implement.

Guevara adds that, while Google's offer is "very good for basic things such as verifying an age in a database, or updating and changing records. We're still far away from being able to convert all applications to fully homomorphic encryption".

It's also still cloud-based and not for edge devices such as mobile phones. "That is mostly because the technology is very new," he says. "Over time, there will be a mix. For instance, homomorphic encryption could be used to hold the keys to data on a phone."

Still, even now, homomorphic encryption promises to solve some big privacy problems as well as easing security headaches. For example, Guevara says that a database of smart devices in a home could be interrogated to produce a video snippet that provides data about the property's structure without exposing images of the home.

If companies (and governments) really only have access to anonymised data that is essential to a particular – and necessary – query, it won't be only big cloud-based enterprises that take comfort from homomorphic encryption. ●

Commercial feature

Hybrid working: six steps to managing cybersecurity and data privacy risks

As pandemic restrictions are eased and staff head back to the office, many will want to continue working from home for part of the week, raising cybersecurity concerns for employers

Hybrid working is set to become standard practice for most organisations as we slowly begin to emerge from the coronavirus pandemic. According to a May 2021 McKinsey survey, 90% of organisations intend to shift to a hybrid-working model, a combination of onsite and remote working.

Whether your staff are working in the office, at home, in shared working spaces, or anywhere else, you face numerous additional risks to the confidentiality, integrity and availability of your corporate information.

Many organisations that quickly moved to a remote-working model in early 2020 found there was simply not enough time to carry out suitable risk assessments before making such sweeping changes to their working practices.

The focus was on ensuring their services were able to continue, rather than considering the risks associated with the change. In particular, those that had little or no existing infrastructure to support home working found the situation challenging as they were exposed to cybersecurity risks they were unprepared for and often didn't even understand.

Cybercriminals inevitably took advantage, launching phishing campaigns exploiting fear and uncertainty about the pandemic, and targeting vulnerabilities in popular software.

65%

year-on-year global increase in ransomware attacks

SonicWall, 2021

Perhaps most disruptively of all, there was a huge increase in ransomware attacks. According to SonicWall's 2021 Cyber Threat Report, there was a 65% year-on-year increase globally.

Implementing suitable technical and organisational security measures is especially important when it comes to maintaining your compliance with data protection law. If you breach the UK Data Protection Act 2018 or the European Union General Data Protection Regulation, you could face fines of up to £17.5m (€20m) or 4% of your annual global turnover, whichever is greater.

UK regulators such as the Information Commissioner's Office made allowances for the pressure the pandemic put organisations under. Now that restrictions are being lifted, however, they will be less lenient, so it is essential to act without delay if you are making hybrid working permanent.

"The pandemic has shown organisations they can operate with staff working from home," says Alan Calder, founder and executive chairman of IT Governance, a leading global provider of IT governance, risk management and compliance solutions. "Indeed, there are many benefits. Staff are more productive, overheads are reduced, it's easier to recruit from a wider talent pool and there is less impact on the environment.

"However, remote working is not without its challenges – one of the biggest is information security."

So how can an organisation successfully implement a hybrid working model? Here is a six-step guide:

- **Step 1** Assess your current organisational state to pinpoint any gaps and give you a starting point on what needs to be completed.
- **Step 2** Prepare to put your new policies in place, which will provide a roadmap for day-to-day operations and ensure compliance with laws and regulations, give guidance for decision-making and streamline internal processes.
- **Step 3** Train your staff, as they can often be your weakest link in the security chain, and implement an ongoing training programme to ensure they are aware of the emerging risks of working remotely.
- **Step 4** Put cyber basics in place to stop the most common forms of cyber attack.
- **Step 5** Implement privacy basics to ensure your organisation continues to be compliant with international regulations.
- **Step 6** Think ahead and implement an ongoing, long-term security strategy so your organisation remains secure and compliant, even with the rising level of cyber attacks and data breaches.

If your organisation is yet to consider fully the security practicalities of mixing onsite and remote working, IT Governance can provide you with all the support you need, every step of the way, with its cost-effective cybersecurity-as-a-service and privacy-as-a-service solutions.

IT Governance's cybersecurity consultants, legal experts and incident responders will become an extension of your organisation's in-house IT department. They are your pre-packaged and comprehensive cybersecurity and privacy teams who come without the price tag and work 24/7 to make sure you are, and continue to remain, cybersecure and compliant – in the office, at home, wherever in the world you work.

Please contact us at www.itgovernance.co.uk/hybrid-working-solutions

it governance Our Expertise, Your Peace of Mind