INDEPENDENT PUBLICATION BY

RACONTEUR

RACONTEUR.NET | #0805 | 08/05/2022

CYBERSECURITY & IT GOVERNANCE

STRATEGY

Shields up as new cybersecurity strategy looks to the future

Are the UK's latest plans to develop the country's cyber capabilities sufficient to deal with the latest digital threats?

Sam Forsdick

An imminent cyber attack is an inevitability. Research by cybersecurity firm Trend Micro shows that more than three-quarters of global organisations expect to be successfully hacked in the next 12 months.

Changes to the way we work have increased the likelihood of cybersecurity breaches. Remote working and cloud computing are highlighted as two of the most high-risk factors. The current geopolitical climate is another significant factor. The Five Eyes intelligence alliance warned recently of increased malicious cyber activity from Russia, since the invasion of Ukraine.

The revelation that details of UK government employees appeared on Russian sites makes the success of the UK government's recently revised cybersecurity strategy even more crucial to secure the country and businesses within it.

In January, the UK government's National Cyber Strategy set out its three-year vision to improve the country's digital resilience. It focuses on five pillars: strengthening the cyber ecosystem; improving resilience; developing new technologies; international influence, and countering threats. It lays out plans to expand the existing approach of 2016 to 2021, with the ambition of making the UK a global leader in cyber.

> **Although it is a government-led strategy, there is a much greater emphasis on the responsibility of the private sector and citizens to manage cyber risks**

Dan Patefield is head of the cyber and national security programme at TechUK. He believes the National Cyber Strategy continues "the robust leadership" the UK government has taken across the cyber domain over the past decade. "The UK has built strong foundations, enabling the industry to strengthen its cyber resilience in the face of the ever-growing threat landscape," he says.

One of the key differences between the previous strategy and the revised one is the onus it places on the whole of society to improve the country's cyber capabilities. Although it is a government-led strategy, there is a much greater emphasis on the responsibility of the private sector and citizens to manage cyber risks.

As Chancellor of the Duchy of Lancaster, Steve Barclay's responsibilities include oversight of the Cabinet Office's cybersecurity remit. Speaking at the strategy's launch, he said: "The new National Cyber Strategy sets out a clear vision for building cyber expertise in all parts of the country, strengthening our offensive and defensive capabilities and ensuring the whole of society plays its part in the UK's cyber future."

This change in tack is one that David Woodfine, managing director of Cyber Security Associates, welcomes. "People think cyber is all about technology," he says. "But cybersecurity involves people, processes, culture and society. By focusing on the cyber ecosystem of the UK, we're not relying on the big technology companies to protect us. We're encouraging everyone to be cybersecure and to improve awareness."

Ransomware is malware which targets individuals. In its 2021 review, the National Cyber Security Centre warns that it is "the most significant cyber threat" facing the UK. Similarly, Verizon's 2021 *Data Breach Investigations Report* showed that 85% of attacks involved a human element, highlighting the need for greater education in cybersecurity and justifying the National Cyber Strategy's society-wide approach.

Woodfine was involved in the development of earlier iterations of the UK's national cybersecurity strategies, when he was at the Ministry of Defence. "In some regards, people are our weakest points in cyber defence. But if we get it right, people can equally be our strongest defence mechanism," he says.

The new strategy also emphasises the importance of resilience, something that Dayne Turbitt think is "critical". Turbitt is senior vice president and UK general manager of Dell Technologies, a company that has worked closely with the UK government to help devise its cyber strategy.

The foreword of the strategy references the importance of using technology suppliers that share the UK's values. This provides an opening for UK-based technology companies to work across the country's critical national infrastructure. "It gives a great opportunity for us here in the UK to serve our customers and help them through their cyber strategy," he says.

The new strategy also recognises the need for a more "diverse and technically skilled workforce" to create a more internationally competitive sector. Currently, more than half (53%) of the UK's 1,838 cybersecurity firms are registered in London and the South East, employ 45% of the country's cyber professionals and account for 91% of external investment.

Steps are underway to address this regional imbalance. The 12 government-funded cyber clusters, which are located across the length and breadth of the UK, are being instructed to strengthen their links between local business and academia and to encourage greater collaboration across the UK.

As chair of Gloucester's Cyber Tech group, Woodfine has seen how closer interactions between schools, universities and businesses can improve pathways for people to get into the cyber industry.

"The strategy provides a good building block but I would like to see a concrete plan," he says. "We can see the strategies and the plan for the next 36 months. But as a business owner, I'd like to know how I can influence it and understand how we're going to protect the UK digital infrastructure of the future."

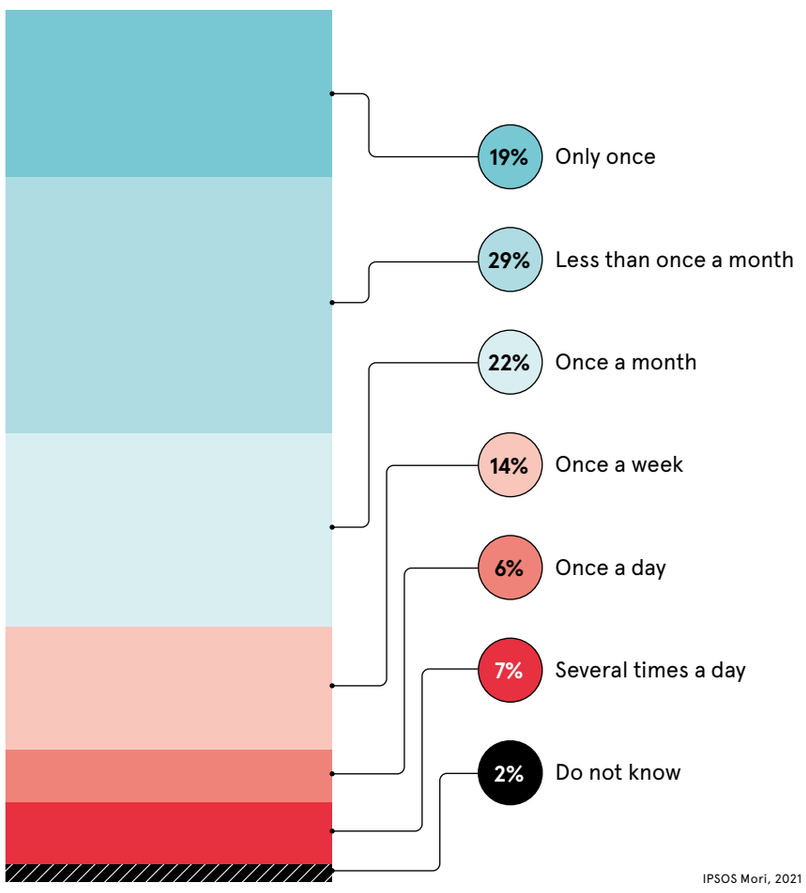
There is also an emphasis on improving education and skills in this area. There has long been a digital skills gap in the UK; Turbitt describes cyber talent as being as "rare as hen's teeth". The strategy document addresses this with the promise to "expand the nation's cyber skills at every level". But there are few details on how this can be achieved, beyond upskilling teachers and encouraging more young people to take up cyber. "Arguably, the government hasn't done enough to increase the take-up of STEM subjects," he says. "But it isn't just the responsibility of the government. It's the responsibility of industry, in partnership with the government, to figure out how we address this and any spotlight on this topic is a great thing."

As an initial document, there seems to be wide agreement that the National Cyber Strategy addresses many of the key challenges currently facing the sector. Turbitt believes that it's now up to the private sector to "step into the breach".

"What will follow from this is investment of public money in these areas. And it will then be beholden to UK industry to work within that framework to go and execute it," he says.

HOW OFTEN ARE UK BUSINESSES ATTACKED?

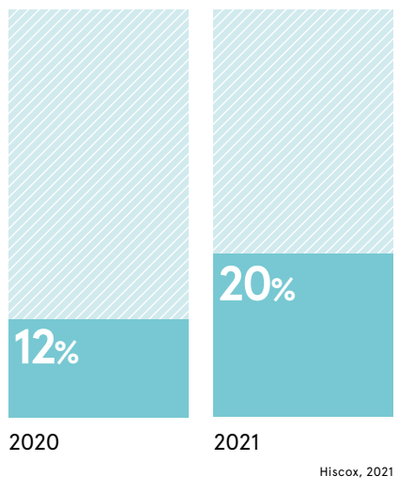
Frequency of cyber breaches experienced by UK businesses



IPSOS Mori, 2021

A SPIKE IN CYBER SPENDING

Cybersecurity as a percentage of IT spend in the UK



Hiscox, 2021

Distributed in
THE SUNDAY TIMES
Published in association with
infosecurity

Contributors

Alison Coleman
Writer and editor, senior contributor at *Forbes*, with articles published in *The Guardian*, *Quarterly* and others.

Jonathan Evans
Journalist, specialising in HR, the future of work and leadership, with work published in *The Independent*, *Metro* and PA.

Sam Forsdick
Raconteur's staff writer, specialising in technology and the future of work. He has written for I-CIO, NS Business, *Press Gazette* and *New Statesman*.

Tamlin Magee
A London-based freelance journalist specialising in technology and culture for a range of publications.

Kate O'Flaherty
An award-winning cybersecurity and privacy journalist, writing on issues that matter to users, businesses and governments.

Charles Orton-Jones
PPA Business Journalist of the Year, former editor of *EuroBusiness*, specialising in fintech and startups.

David Stirling
A freelance journalist specialising in news and features for national newspapers and business magazines.

Chris Stokel-Walker
Technology and culture journalist and author, with bylines in *The New York Times*, *The Guardian* and *Wired*.

Emma Woollacott
Journalist writing about business, technology and science, and a regular contributor to the BBC News website and *Forbes*.

raconteur reports

Lead publisher
Sophie Freeman
Managing editor
Sarah Vizard
Deputy editor
Francesca Cassidy
Reports editor
Ian Deering
Sub-editors
Neil Cole
Gerrard Cowan
Christina Ryder
Commercial content editors
Laura Bithell
Brittany Golob
Head of production
Justyna O'Connell
Design and production assistant
Louis Nassé
Design
Celina Lucey
Colm McDermott
Sean Wyatt-Livesley
Illustration
Kellie Jerrard
Samuele Motta
Design director
Tim Whitlock

/raconteur.net
@raconteur
@raconteur_london

raconteur.net /cybersecurity-2022

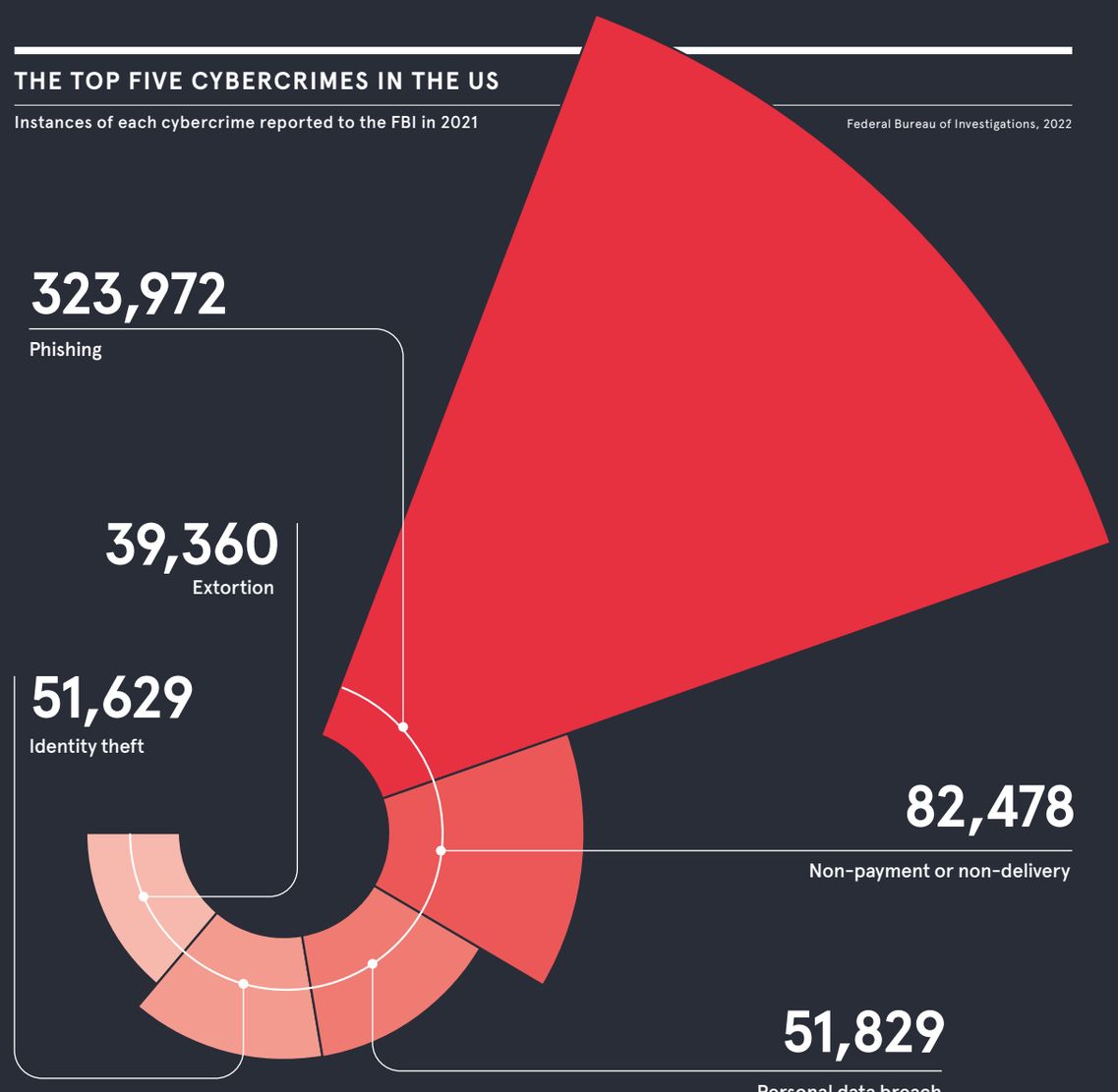
THE RISE OF PHISHING

More than 320,000 people reported being a victim of phishing in the US in 2021 according to the FBI, up by a third compared to the previous year. It is by far the biggest cause of cybercrime and can have devastating consequences on people and businesses. Yet organisations continue to be caught out as hackers take advantage of the Covid pandemic and the ability to be more personal in their attacks.

THE TOP FIVE CYBERCRIMES IN THE US

Instances of each cybercrime reported to the FBI in 2021

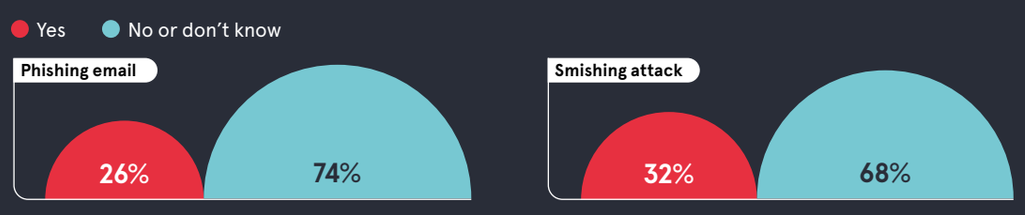
Federal Bureau of Investigations, 2022



PEOPLE ARE FALLING FOR PHISHING ATTACKS

Percentage of employees who say they fell for a phishing scam at work in the past 12 months

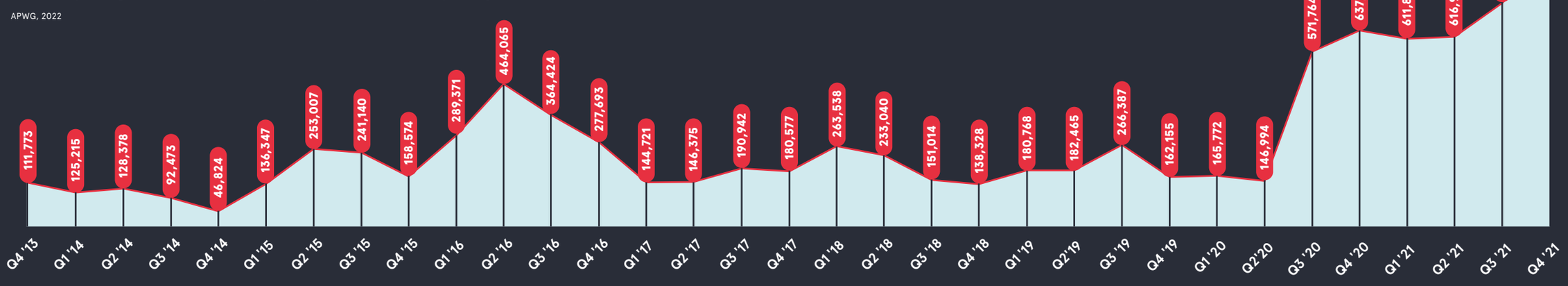
Tessian, 2022



PHISHING ATTACKS ARE ON THE RISE

Number of phishing websites, determined by the unique base URL found in phishing emails

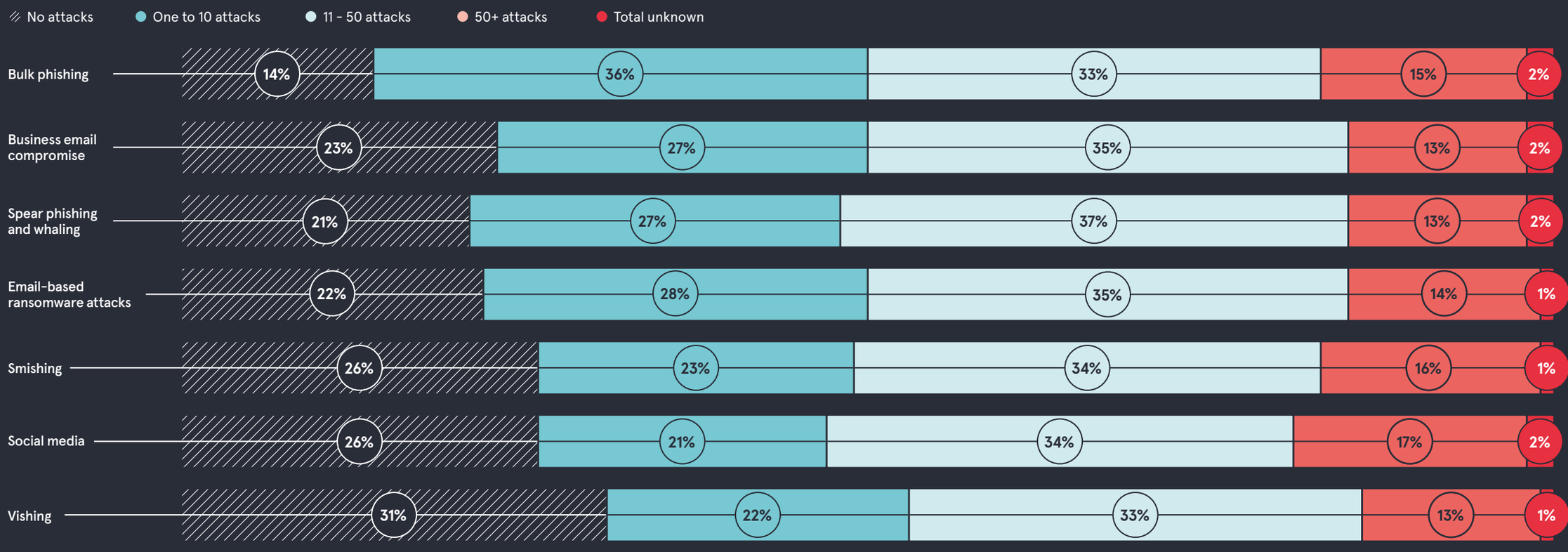
APWG, 2022



THE MAJORITY OF ORGANISATIONS HAVE FALLEN VICTIM TO PHISHING ATTACKS

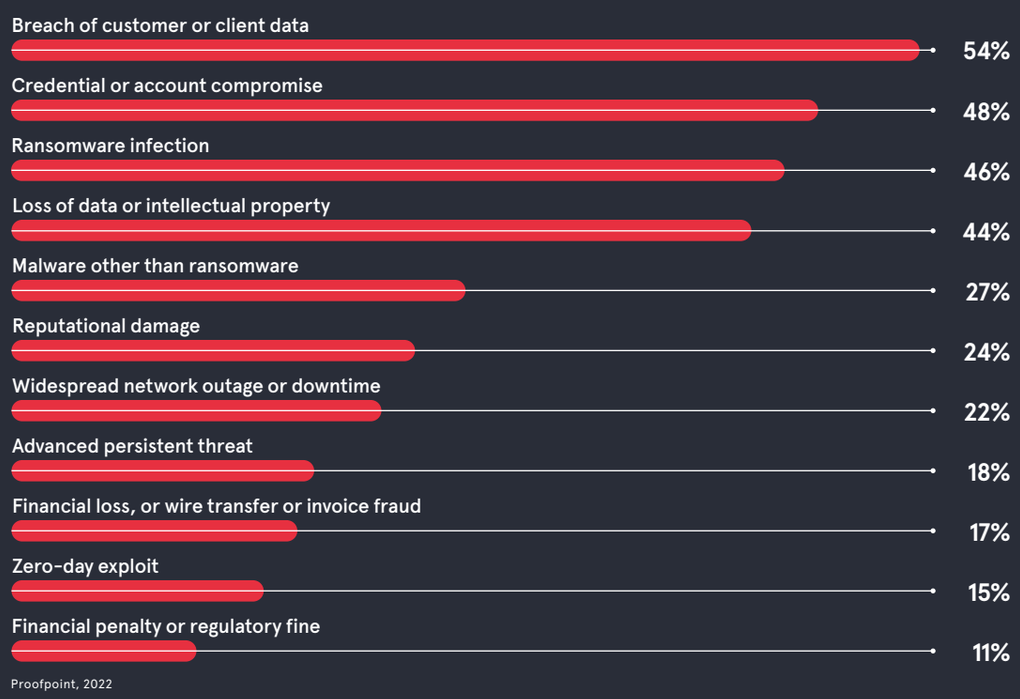
Percentage of global IT workers who say their company was the target of a phishing attack, both successful and unsuccessful

Proofpoint, 2022



PHISHING ATTACKS HAVE REAL-WORLD CONSEQUENCES

Percentage of global IT workers reporting the following as results of successful phishing attacks

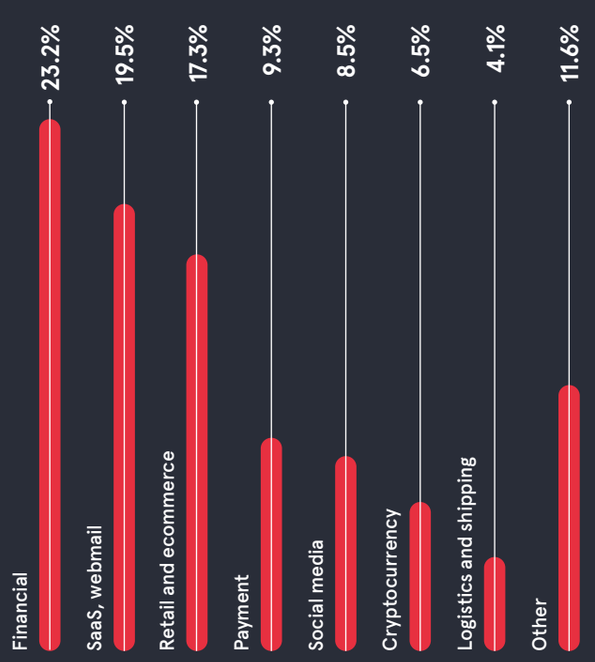


Proofpoint, 2022

FINANCIAL SERVICES IS THE MOST TARGETED INDUSTRY FOR PHISHING ATTACKS

The most targeted industries in the fourth quarter of 2021

APWG, 2022



The different types of phishing

Bulk phishing: indiscriminate attacks sent to many people in an organisation

Speak phishing: targeted attacks on specific people in an organisation

Whaling: attacks against high-value targets in an organisation

Smishing: using text messages as the source of the attack

Vishing: using phone calls or voice messages as the source of the attack

Why do we have such a hard time with passwords? Here's the answer

Passwords have been with us in some form or another since the dawn of computing. Yet we're only marginally better with them today

Memory remains something of a mystery. Neuroscientists everywhere are working to unlock the secrets of human memory, many of which continue to elude us. But one theory posits that we don't usually remember our original memories – we remember the last time that we remembered them, like copies of copies of copies.

The nature of our digital lives necessitates that we create more complicated, unique combinations of letters, spaces, phrases, upper-case, lower-case, signs and symbols in order to access the services we rely on at home and at work. These are only growing: a recent study from LastPass shows 90% of people have as many as 50 online accounts. Given our time-pressed lives, is it any wonder that, even in 2022, the top five most common passwords leaked to the dark web were '123456', '12345678', 'Qwerty', 'Password', and '12345'?

While 90% of internet users are worried about having their credentials stolen, a staggering 83% wouldn't know if their passwords had been leaked to the dark web. The majority of people reuse passwords across accounts, and 45% don't change passwords even after a known breach – leaving personal accounts and organisations wide open to attack. In terms of user safety, there's clearly a mismatch at play here: while users correctly perceive the danger of credentials theft, they're not doing anything about it.

Today, a single compromised account can easily create a disastrous domino effect where not only the original target suffers, but so do their contacts, suppliers, and everyone else in their wider network – in fact, recycled passwords are often the first point of entry into conducting a successful supply-chain attack. Financial and reputational damage can easily spiral out of control, and one stolen credential is all it might take.

Six tips to guard your 'digital doors'

There's no fool-proof way to protect any organisation, but keeping some principles in mind – from culture through to technology, implementation, and ongoing maintenance – can go a long way to help.

1 Embed security in your culture. Create a culture where all levels of the organisation understand and value security, and where staff feel comfortable reporting mistakes. However, accept that raising awareness is not always enough to change behaviour, advises Bournemouth University's John McAlaney. Businesses can hit a wall if they think security culture ends at training.

2 Be cyber smart. Phishing, smishing (text or SMS), and vishing (voice call) attacks are on the rise. Carefully review any messages you receive by double-checking the sender's email address. Be on the lookout for poorly written email copy, and don't blindly accept any MFA requests.

3 Set up your cybersecurity tools. Technology makes securing you and your data a lot easier. Implementing solutions like a password manager and multi-factor authentication (MFA) will secure your data and bolster best practices.

4 Update your software. Cyberattacks often target vulnerabilities in older applications. If you receive an alert from Apple, Microsoft, or Google about an urgent security update, install it right away. The same applies to smart home devices or other Internet of Things (IoT) gadgets.

5 Conduct an audit. Do you know where your data is? Is every piece of information protected? Have you shared any sensitive credentials? Try to map out where your data is, who might have access to your information, and take a digital headcount.

6 Trust your gut. If money or highly sensitive information (like your National Insurance number) is requested – and the sender needs it quickly – take a moment to assess the situation. Don't be afraid to ask questions and get all the facts before pressing send.

In spite of their ubiquity – the password has, after all, been with us since the earliest days of computing – passwords remain a fundamental weak spot. Ultimately, they rely on end-user choice. Security teams can implement some measures, but they are limited in the guidance they can really enforce, or the technical guardrails they can install. Weak or recycled passwords are a case of human fallibility, and that's unlikely to change provided humans remain fallible. Which we will.

Attackers are all too aware of these vulnerabilities in human psychology and so security teams need to be too. People haven't evolved to memorise frequently changing generated passwords – it's just not something that's been a part of our evolutionary history.

So while it's true that every user has a role to play in the safety of their organisation, it's not possible or even desirable that everyone becomes a security-obsessed password expert. It's up to organisations to implement safeguards, maintaining a balance between usability, security, and keeping the onus of responsibility away from weighing too heavily on the user.

But the idea that people are a 'weak link' in security is perhaps an unfair misnomer. People are people, and as such, systems should be built around their blind spots, patterns, or bad habits to help guard against them. That's why it's so important to understand the psychology at play.

"As humans, we have finite cognitive resources that we use to navigate our everyday lives," explains chartered psychologist and professor of psychology at Bournemouth University, John McAlaney. "Workplaces can be very intense, requiring us to pay attention to multiple things at once – we are continually in a state of having to prioritise."

Picture being on a drive and spotting flashing lights in your rearview mirror. It's an emergency vehicle, and you reflexively prepare to move aside – a quick, impulsive decision, but the correct one. These intuitive reflexes are often a strength, but they can be a weakness too: "Sometimes making a quick decision based on limited information will result in an incorrect decision," says McAlaney, "and this could be the case with password safety."

> **You need to understand what barriers are preventing the employees from changing their behaviour, such as the conflict between the need for security versus the pressure to be productive**

If an individual is juggling a lot of tasks, they may not prioritise security. This "doesn't mean they don't understand its importance or are being lazy," McAlaney adds, "it's often just the case people feel they have many other tasks that need to be done with limited resources."

Bolting the 'digital doors'

Fortunately, there are both technical and cultural initiatives that organisations can take to make our digital lives a little more secure. In our homes, it only takes an intruder one entry point to pry open access everywhere. In the digital world, the same is true, but at a far larger scale: one set of stolen credentials could leave your whole organisation's network open for attack.

With good reason, it's socialised into us to lock the doors and windows when we leave our homes. A single pin tumbler lock is worryingly simple for any would-be intruders to pick, and that's why most homes reinforce front and back doors with more secure systems like deadbolts. A simple plaintext password is the digital equivalent of that pin tumbler. It's a deterrent, but easily cracked.

But deadlier still are default passwords. Internet-connected devices on your network, including routers or CCTV systems, will often ship with default passwords enabled. Leaving these in place means you're "basically leaving your keys in the door," says professor of cyber security at Ulster University, Kevin Curran. "There are search engines like Shodan which crawl the web for connected Internet of Things devices, and hackers will try defaults on all of them."

The number one rule, then, is to use different passwords – all the time, everywhere. "One should have a reputable password manager which will create complex, strong passwords," Curran comments. These are then stored in an encrypted vault. "You then only need to remember one master password, and the password manager will automatically take care of logging you into different sites with secure passwords."

However, password managers only work if individuals fully trust them to generate and safely store passwords – and users need to have them installed on every device they use to access their accounts, points out CIO of Endava, Helena Nimmo. LastPass's business password manager, for example, protects all endpoints across the organisation, wherever employees work, with full control for IT over deployment and policies. Suggesting and managing unique, strong passwords, the secure manager reduces the number of passwords employees have to remember and, as such, helps mitigate poor password hygiene.

Organisations can improve password security by combining multiple approaches. Encouraging employees not to share passwords across personal and company accounts, and suggesting employees use sentences, for lengthier passwords, is a good start.

"Securing the password management process with multi-factor authentication, which relies on a PIN or biometrics, and making sure that passwords are changed regularly by everyone within the organisation, without exception, are also good practice," says Nimmo.

Measures like these can fit into a 'cybersecurity by design' framework, says Curran, where security staff help to craft a set of pragmatic guidelines so that organisations can more completely consider the full remit of protections and processes that should be in place.

Businesses need to have a holistic understanding of cybersecurity as an organisation-wide risk, along with all their legal and regulatory implications, and password awareness is part of this. Organisations should train staff, identify which risks to avoid, accept, and mitigate, and communicate business-wide policy to senior management.

However, even with training, it can often take people to make a mistake themselves before they learn. Security teams could consider sending phishing emails containing fake malware to employees, which, when activated, educate them on their mistakes.

Culturally, employees take their cues from leadership, adds McAlaney, so if they feel senior management are only paying lip service to security, staff are less likely to invest in the topic themselves. Leadership need to practice what they preach as well as training staff.

Increasing knowledge doesn't necessarily lead to behaviour change, and this is where a lot of education initiatives fall down: merely having employees sit through a seminar or online course is not necessarily going to make anyone behave more securely. Knowledge helps, but it doesn't definitively translate into action.

"Instead, you need to understand what barriers are preventing the employees from changing their behaviour, such as the conflict between the need for security versus the pressure to be productive," says McAlaney.

"If an organisation finds half their staff did not change passwords after a breach, then the first step should be to open a genuine, non-judgemental, dialogue with employees to find out what's stopping them from making these changes – then finding a way forward taking these issues into account."

For more information, visit lastpass.com

LastPass

PASSWORD PSYCHOLOGY

How good are people's password knowledge and habits?

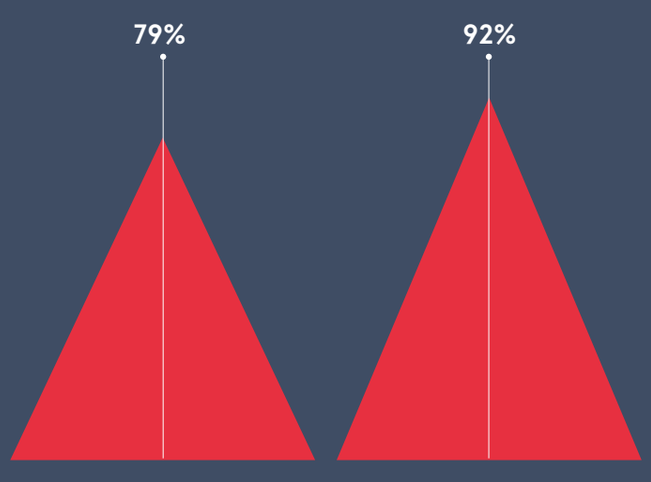
83%

of people would not know if their information was on the dark web

90%

of people have up to 50 digital accounts to protect

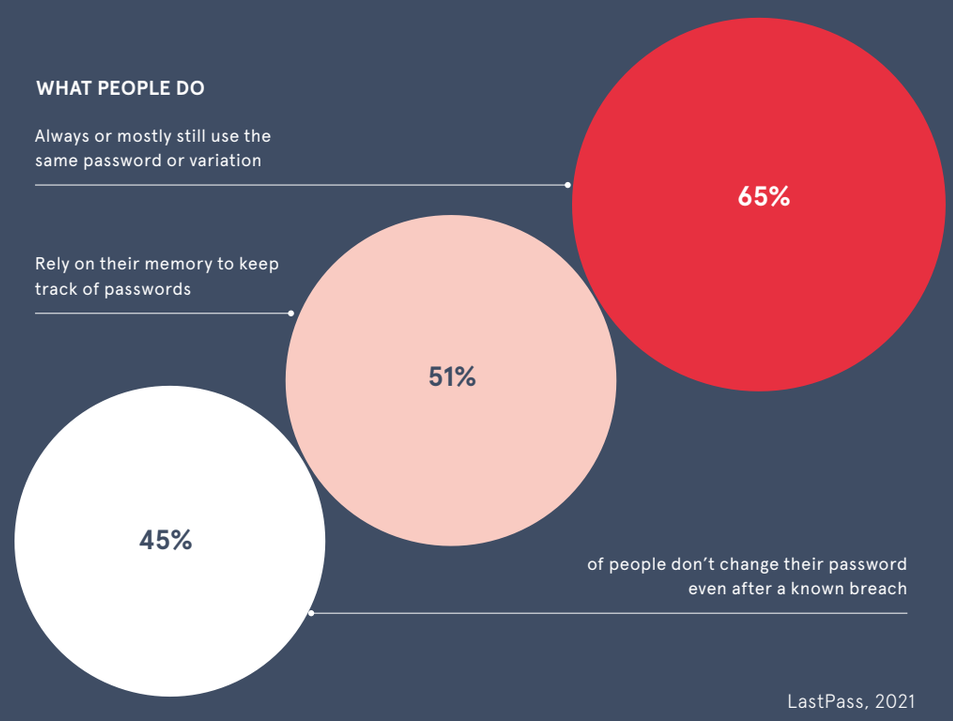
WHAT PEOPLE SAY



agree that compromised passwords are concerning

know that using the same password or a variation is a risk

WHAT PEOPLE DO



LastPass, 2021

CYBER WARFARE

Crossfire-proofing for British firms

Ukraine's cyber conflict with Russia has intensified, increasing the risks of collateral damage far beyond their borders. SMEs in particular need to reinforce their digital defences

Chris Stokel-Walker

Alongside the carnage that's taking place on the ground in Ukraine, a there's a parallel war being waged in cyberspace. Ukraine and Russia are highly IT-literate societies with infrastructure that relies on digital technology, which is why they've been going to great lengths to try to bring down each other's systems.

In fact, Russia has been mounting cyber attacks for decades, with hostilities intensifying significantly after it seized the Crimean peninsula from Ukraine in 2014.

Electricity supplies have been a prime target for disruption since then, for instance. Such attacks have been reasonably focused so far, reports Alan Woodward, visiting professor of cybersecurity at the University of Surrey.

But, just as so-called guided missiles can wreak havoc on innocent civilians, a misfiring cyber attack can cause collateral damage beyond its intended target. For this reason, businesses far from the physical battleground – especially SMEs, whose cyber defences are generally likely to be relatively basic – need to be wary of Russia's online war with Ukraine.

"Effective cyber attacks will quite often use a vector in the supply chain," Woodward says. This makes it possible for a business with no connection to Ukraine or Russia to be caught up in an attack, simply because it shares a software provider with a company that does have such links.

In 2017, for instance, the NotPetya ransomware strain (widely viewed as the handiwork of Russian military intelligence agency the GRU) was launched through a tax preparation app used by many firms in Ukraine – and plenty outside the country too.

"The next time that everyone updated their software – bang, they'd taken in this massive piece of ransomware," Woodward says.

Some of the companies whose systems were infected had to write down billions of pounds from their balance sheets in the process of fixing the problem. "A number of small and medium-sized businesses were practically wiped out," he adds.

This is why the UK's National Cyber Security Centre (NCSC) has advised British businesses to remain alert for such attacks and bolster their defences accordingly. The NCSC doesn't believe that Moscow is deliberately seeking to target British enterprises. Rather, it's concerned that an assault targeting organisations in Ukraine could easily affect enterprises in other countries.

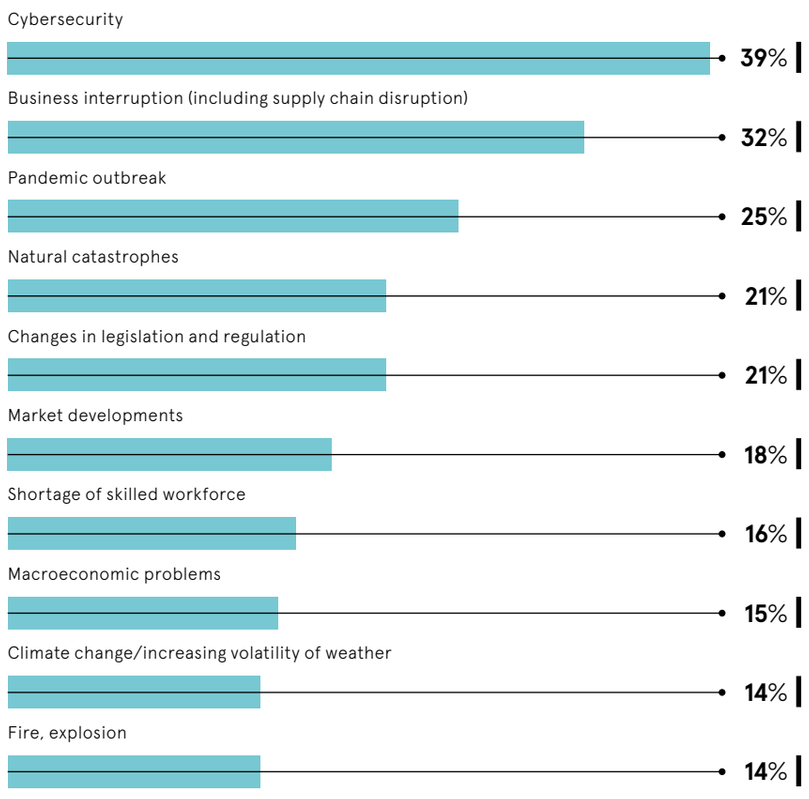
And British firms have more to fear from Russia than a less-than-discriminate cyber strike mounted by the GRU. Dr Victoria Baines is a senior researcher, author and speaker who's worked with bodies such as Europol's European Cybercrime Centre in The Hague. She says: "The line between state-sponsored and profit-driven cyber threats has become very blurred."

> **The line between state-sponsored and profit-driven cyber threats has become very blurred**

JGI/Tom Grill via GettyImages

CYBERSECURITY IS THE NUMBER-ONE RISK FOR SMALL BUSINESSES

Leading risks for small enterprises worldwide — Allianz, 2022



Baines cites the WannaCry ransomware attack in 2017 as a case in point. This spread far beyond its original target, causing chaos for the National Health Service, as well as Renault, FedEx and Deutsche Bahn. Europol estimated that more than 200,000 computers in 150 countries – and especially Russia – were disabled.

WannaCry was eventually traced back to a gang with ties to Kim Jong-un's regime in North Korea. But the link between private criminal enterprise and national governments goes further than that, according to Baines, who points out that the Conti Team – a prolific ransomware gang thought to be based in St Petersburg – "has recently declared its support for Putin".

This means that its members could act as 'hired guns', aiming to cause chaos for any organisation around the world that speaks out against Russia's actions.

Before the invasion, Russia had actually gained some good publicity for starting to round up some of the country's more notorious cybercriminals. Their arrests, some of which were filmed and broadcast worldwide, had indicated a shift in approach from the Kremlin that many countries welcomed.

But, now that Russia has become an outcast, the Putin regime has far less incentive to clamp down on domestic cybercriminals. This means that we're all more at risk, according to Baines, who adds: "It's become increasingly clear that some states are also using ransomware and cryptocurrency scams to generate revenue."

It's another reason why the debate about whether to pay ransoms or not has become so heated. "Ultimately, we can't rule out the possibility that ransoms paid by SMEs in the UK and elsewhere are supplementing the Kremlin's war coffers – a sobering thought," she says, but stresses that the threat is also "largely preventable".

Woodward agrees that there are several straightforward and effective steps that firms can take to protect themselves from the GRU – and from Russian cybercriminals who've been let off the hook.

"This may sound like a broken record, but look at the NCSC's guidance," he says.

The centre has plenty of advice on matters such as how to manage passwords; handle emails to avoid downloading malicious attachments; and set up corporate networks so that they're more resistant to attack and less likely to spread malware onwards if they do get infected.

"One of the most common vectors for ransomware is an emailed Excel spreadsheet that has a macro in it. If people open it and the right network policies aren't in place, there's nothing to prevent that macro from dialling home and pulling in some malware," Woodward warns.

> **We can't rule out the possibility that ransoms paid by SMEs in the UK and elsewhere are supplementing the Kremlin's war coffers**

While it may seem costly, commissioning external expertise to satisfy yourself that your firm's networks are as secure as they can be is likely to be a sound investment. If you want to do it in house, be sure to cover all the simple aspects that can easily be overlooked, Baines stresses.

"Basic digital hygiene – for instance, keeping software up to date, running a security program that scans for known threats and staying alert to the latest phishing scams – is an effective way to counter many of the cyber threats facing SMEs," she says. "There really is no excuse not to do these things. They aren't rocket science and they'll help you to avoid so much pain in the long run."

dowell via GettyImages

BIOMETRICS

Fingerprints crossed: are biometrics secure?

Fingerprints, voice, and facial recognition have all been touted as the next step in the evolution of online security. But should we hand over our unique physical traits so readily?

Tamlin Magee

An intelligence agent stalks a corridor, landing on an imposing security door. Leaning into a panel that brushes its frame, they put their face into position and, with a satisfying series of computerised bleeps and boops, their identity is confirmed – the portal opens.

These body-powered gateways were once firmly part of science fiction. But today, most of our devices feature fingerprint scanners and facial recognition software.

Our unique biological traits make biometrics a secure and convenient means to authenticate our identity. Given the alarming frequency that plain-text passwords are leaked online, it's little surprise that consumer technology companies and enterprises are using biometric information such as voice, face or fingerprints to authenticate a user's identity.

"Increasing the length and complexity of passwords increases their resilience to a so-called brute-force attack, which attempts to try all the possible combinations of characters," says Steven Furnell, IEEE senior member and professor of cybersecurity at the University of Nottingham. "Advice from the National Cyber Security Centre is to build longer passwords by combining three random words. But, unfortunately, that isn't always guaranteed to work, as some systems and services still insist on checking composition and demand a mix of character types."

No matter the complexity of a passphrase, it can't compete with the robustness of biological information for identity authentication. While a single password could leak onto the web and cause all kinds of chaos, flesh and blood are much trickier to copy.

So, biometrics would seem to be an appropriate alternative. Indeed, Furnell says they're the "key to non-intrusive, frictionless security".

But there may be hidden dangers in relinquishing our biological information to the digital sphere, and what feels frictionless today could come at a cost in future.

Take the US's withdrawal from Afghanistan in 2021. Not only did it leave citizens at the mercy of the Taliban, it also left their biometric data up for grabs. In 2007, the US trialled Handheld Interagency Identity Detection Equipment in Afghanistan, which recorded fingerprint, iris, and facial data. The technology was developed to locate insurgents, then US forces subsequently extended their use to those who cooperated. Ultimately, the personal data of more than 1.5 million Afghans was matched against a database of biometric data and stored in a centralised repository. When this fell into the wrong hands, it revealed information about individuals who had worked with the US, placing them at risk.

These databases, whether created intentionally or as accidental by-products, are one of the chief issues of biometric security, says Britain's Biometrics and Surveillance Camera Commissioner, Fraser Sampson.

"At a simplistic level, biometrics is about measuring and matching. And for matching, a biometric needs a comparator," Sampson explains. "A collection of comparators is a database. And if you retain biometric material, you've created a database."

There are many issues with centralised databases; one is, that they're prone to leaking. When you throw biometric data into the mix, complications that are reminiscent of humanity's darkest moments come to the fore. In the field of biometric surveillance, says Sampson, one person's idea of protection may be someone else's idea of oppression.

"While humanitarian uses of biometric identity can save lives, the same biometric data can be used for domination and exploitation," warns Sampson. "It can be used to marginalise and persecute people on grounds of race, ethnicity and religion."

The benefits of biometrics – their uniqueness, their incontestable ties to real humans – are exploitable as their weaknesses, too.

The abilities of determined, capable hackers with resources should never be underestimated. While biometrics are generally difficult to spoof right now – especially as, for many hackers, lower-effort attacks are more fruitful – what is true today may not be the case tomorrow, as attackers leverage better computing and become more sophisticated.

"Nobody I'm aware of has yet been able to demonstrate an unhackable system," Sampson says, "or an unreachable database. The stakes make it worth it, whether that's hostile state activity or reconnaissance, or commercial hacking. If there's a commercial value to crack something, you can sell that."

45%

of companies worldwide were using biometric authentication in 2021

Okta, 2021

> **At a simplistic level, biometrics is about measuring and matching. And for matching, a biometric needs a comparator**

As the use of biometrics increases and converges, there will likely be fewer, but bigger, databases if these trends continue. While this would reduce the likelihood of breaches and errors, it would increase the impact of compromised security.

That said, it's "not impossible, but it is very hard for someone to spoof a biometric". So says Heather Vescent, futurist and co-author of *Six Principles for Self-Sovereign Biometrics*. It's unlikely, then, that cyber researchers and attackers will arrive at an impasse soon – locked in an endless game of Whac-A-Mole, as is the Sisyphean case with traditional perimeter defence.

But, Vescent adds, the best security on the planet can be useless if stored incorrectly.

"Any data is only as secure as the system in which it is stored," Vescent says. "Sometimes these systems can be easily penetrated due to poor identity and access management protocols. This has nothing to do with the security of biometrics. It's to do with the security of stored data.

"This means the real concern about using biometrics is about how data is stored, how secure the system is, and how much control the owner of the biometric has over it."

In *Six Principles*, Vescent and her co-authors advise that to reduce these risks, biometrics should not be stored in centralised databases.

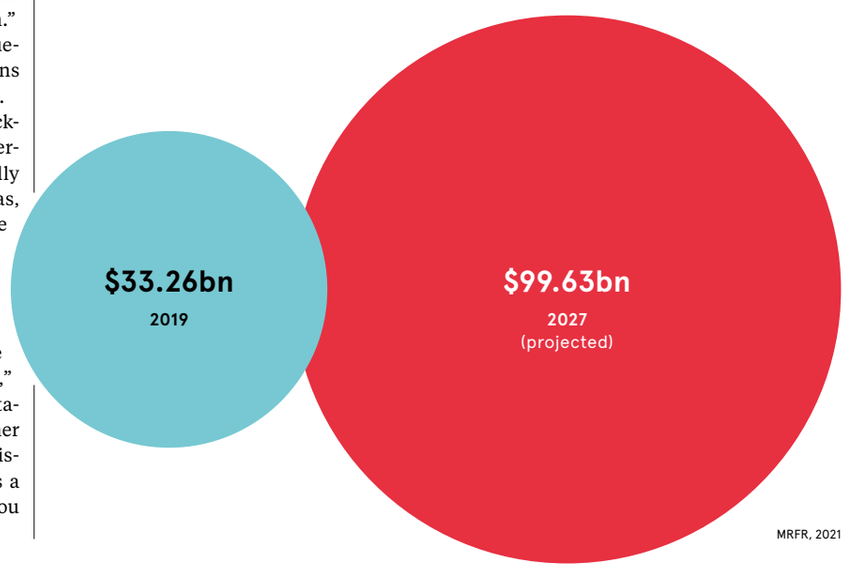
Crucially, users should own and be able to control their biometric data. This data should also be just one component in a wider security landscape – for example, as a supplementary measure, used to provide confidence ratings, or in tandem with other proven techniques such as passphrases.

For Sampson, one of the main questions is avoiding the potential for state overreach. To prevent this, biometrics-based initiatives should be conducted in partnership with trusted private sector providers; these should be auditable, transparent, and conducted under agreed governance arrangements and standards.

But before we race towards using our faces, fingerprints and voices as a salve for all our security woes, perhaps it's worth properly considering the potential for undesirable, second-order consequences. After all, if we waive over all that makes us uniquely human in the name of security – what do we have left?

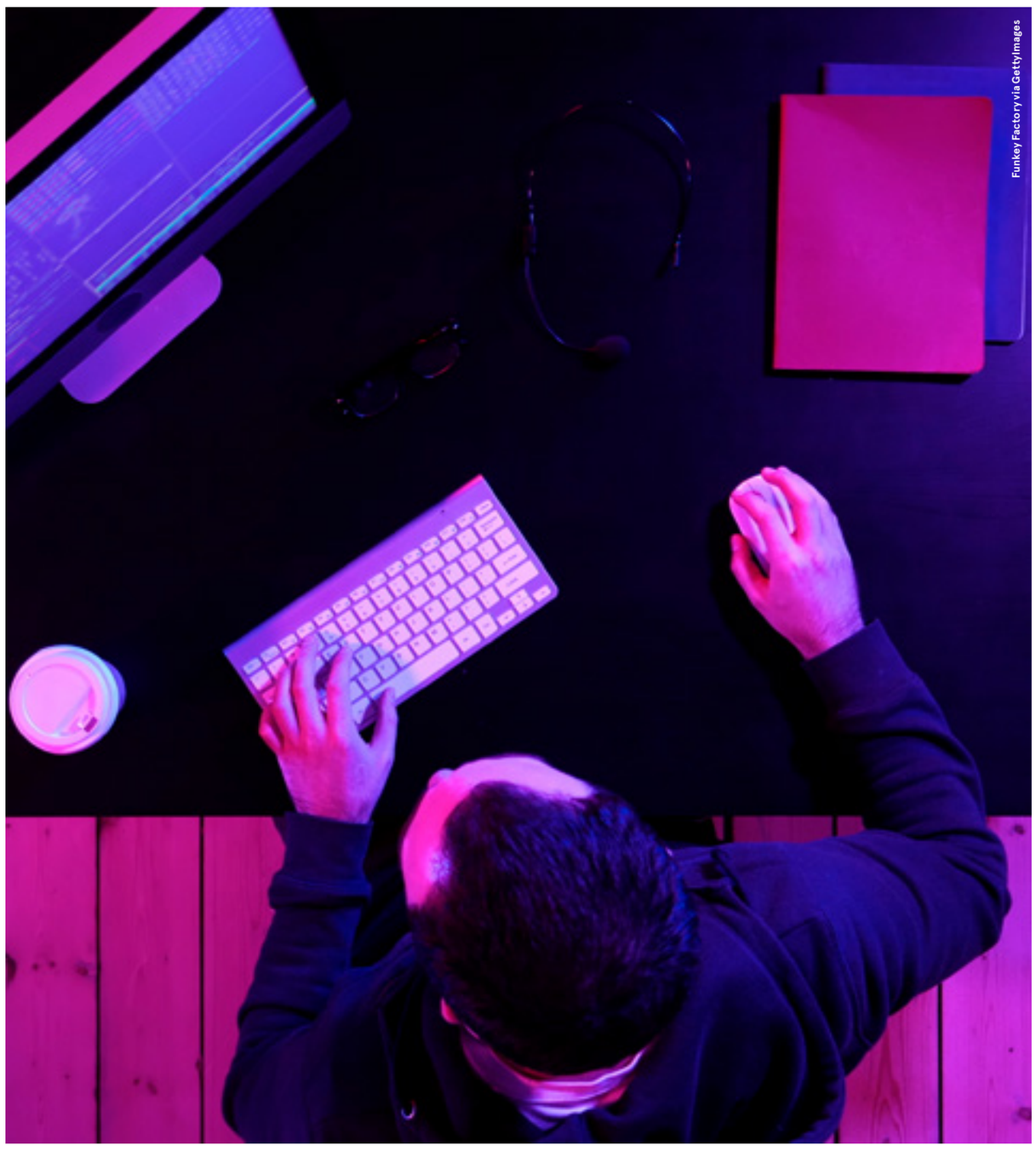
BIOMETRICS ON THE RISE

Biometric authentication and identification market value worldwide



MRFR, 2021

Commercial feature


Funkey Factory via GettyImages

PEN TESTING

The breach and the observance: pen test essentials

The penetration test is a vital protective measure, but there are some important caveats to consider when commissioning a white-hat hacker to probe around your systems

Charles Orton-Jones

In the 2003 version of *The Italian Job*, Charlize Theron plays an ethical safe-cracker who pits her wits against the latest models to tell the manufacturers whether their products are any good. Naturally, she can crack the lot. And pretty soon she's lured into an ingenious gold heist involving Mini Coopers, but, alas, no Sir Michael Caine.

A more imaginative remake might have cast Theron as a penetration tester. These skilled professionals hack into IT systems to pinpoint their weaknesses for their owners. A company needs to know whether its valuable data is secure. But, as per the film, it also needs to know that its pen testers are elite white-hat hackers who aren't going to cause mayhem in the course of their work.

So how do you go about finding a reliable pen tester?

Will North is a good person to ask. He used to run a consultancy running pen tests for clients but now sits on the other side of the fence, hiring them to hack the products of MHR International, a developer of HR and payroll software where he's chief security officer. In the past few years he's commissioned almost 30 tests.

Hiring is no easy task, according to North. "The repercussions of employing an under-skilled tester can be severe. You'll get a false sense of security that your systems are protected," he says. "Unfortunately, it can be very difficult to evaluate the competence of an ethical hacker."

He recommends two places to find candidates: large consultancies and specialist boutiques. The consultancies come with a caveat. "These organisations are often expensive. They can charge nearly £2,000 a day," North says. "Their operating model also means that they often use relatively inexperienced staff to do most of the work."

He believes that boutiques are likely to offer a more cost-effective service. The downside is variability – the chances of hiring a dud are greater. The solution? "You need to rely more on word of mouth."

As for testers' qualifications, the ones to look out for are Crest, GIAC or Check certification. But beware: even the most impressive-looking CV may not be a reliable indicator. So says Hugo van den Toorn, manager of offensive security at Outpost24, a boutique specialist in risk assessment.

"Don't treat certifications as a gold standard," he warns. "The reason is simple: anyone can learn, but this is about understanding and bringing knowledge into practice. Unfortunately, not everyone can pay to take these qualifications or sacrifice sufficient personal time to obtain them. Cheating is a prevalent issue as well."

Look for a "core hacker mindset", van den Toorn advises. For instance, does the candidate blog about cybersecurity matters? Do they have a career showcasing their expertise? How do they perform on external validation platforms such as Hack the Box? Strong candidates may write their own applications to enhance the off-the-shelf products that pen testers commonly use.

Once you've chosen your candidate, it's vital to know how to brief them. What exactly do you want them to prove? Equally important, what are the parameters of the test?

"There should always be a limit of exploitation set, which describes how far into production systems that ethical hackers can go," explains James Griffiths, a former GCHQ cyber expert and co-founder of Cyber Security Associates. "If the client has a huge ecommerce site, for instance, you wouldn't want an ethical hacker changing live data. But there may be cases where you'd want to prove that it could be done. Normally, this can be replicated in a development environment to ensure that availability is not affected."

Griffiths says that a pen test can last from two days to three weeks, with a week being the norm. A key decision is whether to include social engineering hacks. These may involve the pen tester visiting the client's premises incognito to gain physical access to systems or drop infected USB flash drives to see if anyone picks them up and uses them out of curiosity. Other acts of skulduggery could include swiping the pass of an employee or even stealing a laptop.

> **The repercussions of employing an under-skilled tester can be severe. You'll get a false sense of security**

He says that an under-used tactic is to commission a so-called purple team operation. In a normal test assault, attackers (known as the red team) take on defenders (the blue team). In a purple team, both sides work together under the guidance of an expert coordinator to share their knowledge. Reds attack, blues defend and then both parties disclose their thoughts to iterate the security improvements. Griffiths believes that it's a richer process than the standard exercise.

And then there's the question of what to do with the results. Bizarrely, many companies fail to act even when they've been alerted to serious chinks in their armour.

"It's a big frustration to testers when they see the same vulnerabilities cropping up time and time again," reports Gyles Saunders, ethical hacker at NormCyber.

He adds that a common problem is that clients leave an easy route open, making the pen tester's job simple. "When we see such vulnerabilities, we must exploit them, because a cybercriminal would do the same. While that's a valuable exercise, if the client doesn't then act on our recommendations, we're back to square one come the next test."

Pen testing is a vital element of ensuring cybersecurity, yet companies too often fail to instruct their white-hat hackers adequately. At worst, a poorly briefed hacker could bring down vital infrastructure. And the last thing you'd want is to see the smoking ruins of your IT system, recalling Caine's immortal line in the original *Italian Job*: "You're only supposed to blow the bloody doors off!"

247days

the time taken on average to identify and contain a data breach

44%

of data leaks contain personally identifiable information

20%

of cyber attacks are initiated through compromised credentials – the most common attack vector

IBM, 2021

THE GROWING THREAT LANDSCAPE

From ransomware to supply chain attacks, threats are evolving rapidly

11+

cyber threats per device per day are faced by SMEs

85%

of managed service providers reported ransomware attacks against SMEs in 2021

70%

of SMEs have suffered a breach

60%

of those attacked go out of business within six months

BlackBerry, Threat Report, 2022

66%

In 66% of supply chain attacks from January to July 2021, suppliers either did not know or did not report how they were compromised.

50%

Advanced persistent threat (APT) groups were credited with carrying out 50% of supply chain attacks from January to July 2021

62%

Exploiting trust in the supplier accounted for nearly 62% of attacks on customers from January to July 2021.

The European Union Agency for Cybersecurity, 2021

Why you need a prevention-first security strategy

Against a backdrop of growing and evolving threats and skills gaps, organisations of all sizes need to reconsider their cybersecurity strategy

It's not quite Nostradamus, but being able to predict the future using the power of AI and mathematics could be the best way to defeat ever more confident and sophisticated cybercriminals.

Governments and businesses may have raised the white flag in response to the 50% year-over-year increase in weekly attacks across the globe last year – according to Check Point Research figures – but software security giant BlackBerry says they do have the power to fight back.

"If you look across the market at the moment, the most common method of defence against cyber-attack is detect and response," says Keiron Holyome, vice president UKI and emerging markets at BlackBerry. "The industry has given up on trying to prevent attacks happening, but we are putting prevention at the back, centre and front of our strategy. We are using technology in the right place to stop malicious activity getting near to your networks."

Growing threats

Holyome is referring to BlackBerry's AI prevention first approach. Its suite of Cylance AI products includes 'CylancePROTECT', which 'identifies and stops attacks at the door'. It can detect and prevent potentially harmful code in less than 50 milliseconds and can predict malware attacks on an average of 25 months prior to appearing online.

These attacks are increasingly coming from a range of sources such as state actors and are aimed not just at government or big business but also at innovative start-up firms and their lucrative IP (intellectual property).

Indeed, in its 2022 Annual Threat Report, BlackBerry highlighted a 'cybercriminal underground optimised to better target local small businesses'. It said small- and medium-sized businesses were facing upward of 11 cyber threats per device per day. And 2019 research from Ponemon Institute found that over 70% of SMEs had suffered a breach and, such is the financial and reputational impact, that 60% of those attacked go out of business within six months.

Criminals, it added, were also increasingly engaging in their form of a 'shared economy' with groups 'sharing and outsourcing malware allowing for attacks to happen at scale'. Other dangers are coming from public cloud platforms which are unwittingly hosting malware, email and text phishing and 'watering hole' attacks where criminals look for weak-spot websites within a targeted organisation. The increase in hybrid working during the pandemic is also putting extra strain on security with sensitive data being accessed from bedrooms and garages.

Supply chain weakness

Another area of vulnerability is the software supply chain which Holyome says is increasingly being used as an 'attack vector'. There are two elements to this, with the first being weaknesses in the traditional supply chain such as tyre suppliers to a car manufacturer.

"At some point, they will have access to say your e-procurement systems but even if they are not connected to your internal networks then you could be impacted by a ransomware affecting their business," he explains. "What are the implications for your company if you have to close for seven days and you operate a just-in-time system? Ensuring that there is cyber resilience throughout your supply chain is critical."

The software which makes up the supply chain is also crucial. Due diligence needs to be done on all software which suppliers are employing. "There could be issues of software vulnerabilities within software. Don't just allow random installs by ensuring that you have a good corporate policy around deployment," he adds.

> **The industry has given up on trying to prevent attacks happening, but we are putting prevention at the back, centre and front of our strategy**

Prevention first

Detect and response can also be an answer, identifying when employees click on dodgy malware links, but it is not enough, Holyome warns. "It can be both time and cost inefficient. If you rely on it, then you are allowing malicious activity to happen in your environment. That can cause huge financial and reputational issues for your business and loss of critical customer and client data."

It is why BlackBerry has been developing Cylance AI since 2014. It is now on its 7th generation of products. Based on a mathematics model, the AI continuously analyses changes occurring on endpoints in a network, uncovering threats that would be difficult, if not impossible, for a human analyst to find quickly enough to mitigate. When a potential threat is identified, Cylance AI thwarts it in real-time by taking decisive, automated action. But it is also continuously learning.

"It develops and evolves over time. It learns based on the previous bad behaviour data it has seen and adapts its model intuitively," Holyome states. "We have a predictive advantage in securing systems against legacy malware and we can predict what is likely to form the nature of a future attack and again prevent it."

He says Cylance AI also has an advantage over signature-based models which are constantly having to run file updates. There will be a period within that which leaves a network out of data and exposed to attack. "Updates for Cylance AI are much less frequent," he says.

So how predictive is Cylance AI? Mystic Meg or Nostradamus himself? Holyome says his stock position – given the vicissitudes and uncertainty of life – is to say that CylancePROTECT can stop 99% of potential attacks. One example is the Colonial Pipeline ransomware cyber hack last summer where the US energy company was forced to shut down its pipeline system. The group had to pay $5million to the Russian-based cybercriminals DarkSide to restart its operations. "We got hold of that virus after the attack and found that even using our 2015 version of CylancePROTECT it would have been able to predict and prevent it," Holyome says.

Indeed, in a recent test, BlackBerry's suite of Cylance products was, on the independent Mitre ATT&CK testing framework, 100% successful in preventing both the Wizard Spider and Sandworm attack emulations early before any damage occurred. Similarly, its CylancePROTECT solution recently earned the maximum AAA rating from cybersecurity testing organisation SE Labs.

Talent gap

BlackBerry believes that its sophisticated technology can also help lessen the impact of the huge talent gap in the industry. "There is an enormous lack of cybersecurity skills and expertise with SMEs especially struggling to hire cyber security professionals," says Holyome. "Cyber criminals don't switch off at 5pm on a Friday and re-start at 9am on Monday. They are taking advantage of the lack of dedicated employees including increasing attacks on holidays like Christmas when they know nobody is in the office."

He says its products can ease this worry for hard-pressed bosses and staff. "No signature updates reduce an IT manager's workload plus the prevention-first strategy decreases pressure to recruit specialist security skills," he says. "Our AI is very much fire and forget. Just let it do the hard work for you."

And hard work it will be Holyome warns. "Threats are increasing not decreasing. Companies of all sizes can't ignore this and need to reconsider their cybersecurity strategy," he says. "They must understand that security is a journey, not a destination and approaches should continually evolve to meet new threats. Detect and response can leave you vulnerable. Prevention first is the answer. Who wouldn't want to know the future and stay safe?"

For more information and to download the BlackBerry 2022 Threat Report, visit blackberry.com/threat-report-2022

BlackBerry Cybersecurity

BREACH

Employee or employer: who's to blame for a cyber breach?

Many businesses dismiss employees who enable a cyber attack. But is this a fair reaction? And what responsibility does the employer bear?

Jonathan Evans

Imagine your football team has just narrowly lost a game. Who's responsible for the defeat? Is it the goalkeeper, who let the ball slip through their fingers, or the striker who missed a sitter? Maybe it's the manager's fault, for failing to devise and implement a successful game plan?

> **It's like being accused of stealing when you don't even know you've taken something**

Now take this analogy and apply it to a business trying to assign blame in the aftermath of a cyber attack. Does the blame lie with the IT department for failing to put effective cyber defences in place? Or is it perhaps the fault of the CEO for not implementing a culture of cyber awareness? Perhaps the employee who clicked the link that contained malicious software should take responsibility?

Many businesses opt for the latter choice. Research from security company Tessian found that 21% of the 2,000 US and UK workers they surveyed have lost their job in the past year after making a mistake that compromised their company's security.

Irina Brass is associate professor in regulation, innovation and public policy at University College London. She says the figures show "a knee-jerk reaction. There is a lot more that organisations can do to become more resilient before placing the blame on their employees."

One option is a refreshed cybersecurity training programme that reflects post-pandemic working patterns. While many businesses provide such training to their employees, often these overlook the new vulnerabilities exposed by the technologies that facilitate widespread remote working.

The cloud is one example. Nearly four out of ten businesses have accelerated their migration to cloud technologies during the pandemic, according to McKinsey, with 86% expecting this acceleration to persist post-pandemic.

But as Brass points out, the cloud creates more routes for cybercriminals to hack a business, undermining perceptions of the technology as a completely secure option.

"It makes the attack surface larger and more homogenous because you have these cloud-based work packages that are the same being deployed to large numbers of people, meaning that once a hacker figures out a particular compromise, they can apply it to all sorts of replicas."

With more applications and tools being stored in the cloud, more people require access to it. This means the amount of data the average employee can access has grown exponentially in a short period of time.

Cybercriminals are exploiting this. They're using the primary benefit of the cloud – its ability to connect workers to essential company documents regardless of their location – to access large amounts of data through a single breach.

This is part of a broader set of challenges, which stem from the fact that our home environments are fundamentally not as secure as offices.

The immediate shift to home working exposed our work laptops – and businesses' data – to an array of consumer-connected Internet of Things (IoT) devices. According to Which?, smart products in the home – from light switches to speakers – experience an estimated 12,000 hacking attempts each week. Smaller, cheaper products often lack many of the security features of traditional computers, making them easier for cybercriminals to hack.

The threat posed by lax security systems for some IoT devices would ordinarily be isolated to consumer data. But with widespread remote working, these devices now act as a gateway for hackers looking to access a company's data.

"Most consumer devices have dubious security specifications," Brass says. "They have default passwords and really short software update periods, if at all. And if a hacker compromises them, they scan a work device that is on the home network for vulnerabilities and an employee won't even be aware it's happening."

The correlation between the shift to remote working and rising cyber attacks suggests it's the unique working environment caused by the pandemic, rather than employees themselves, that's driving the spike in breaches. The solution may be further training for employees on the importance of cyber hygiene both in and out of working hours.

The legality of dismissing an employee after they make a cybersecurity mistake also warrants consideration. According to Monica Atwal, managing partner and employment law specialist at Clarkslegal, an employer's reasoning for dismissing an employee usually falls into two categories: gross negligence or gross misconduct.

These reasons require an employer to prove that on the balance of probabilities the employee is either culpable of serious carelessness or they engaged in a clear and serious violation of the company's rules.

The lack of regular training offered to employees on cybersecurity undermines the validity of these reasons, Atwal adds. A study from Software Advice, earlier this year, found that 44% of SMEs have not trained their team on cybersecurity since 2020. This is despite 62% of them experiencing an increase in cyber attacks in the same period.

The absence of a "systematic approach to cybersecurity" weakens an employer's argument for dismissal by gross negligence, in Atwal's opinion, because of the need to demonstrate that an employee received "intensive training" on a "regular basis" and still acted carelessly.

"An employee would clearly have an unfair dismissal claim and you would get short, sharp shrift from an employment judge if you said you received one training session on something that is so complicated and nuanced," she says. "It's like being accused of stealing when you don't even know you've taken something."

Despite the risk of being sued for unfair dismissal, Tessian's research shows that many employers believe employees should shoulder the blame for any cyber incidents that happen on their watch.

The same research found that 29% of businesses have lost a client because of a cyber mistake in the past year. Jeff Hancock, is founding director of the Stanford Social Media Lab. He notes that many employers are trying to "pin the blame" by dismissing employees after a breach.

"Businesses want to provide a reason for why it happened to their clients," Hancock adds, "but this comes at a long-term cost because employees are going to be less likely to report attacks in the future."

A policy of dismissing any employee who makes a cyber mistake risks instilling a culture of fear around reporting such incidents. In time, this would leave a business more vulnerable to hackers, as employees become unwilling to report any breaches or vulnerabilities they've noticed in the company's cyber defences.

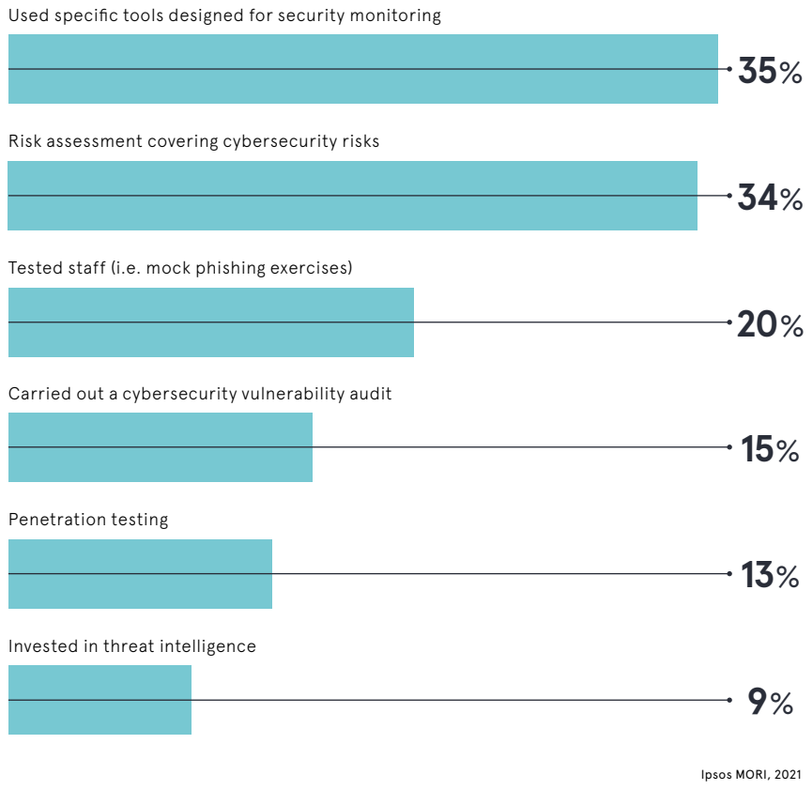
The solution, in Hancock's opinion, is a company culture where cybersecurity is at the forefront of every employee's mind, regardless of their position. This would involve regular training sessions on the latest hacks cybercriminals are using. It would be underpinned by an understanding between employers and employers that cyber breaches are inevitable and not the responsibility of any one person.

In a similar way that a football team deals with a match loss, a breach is rarely the fault of just a single individual.

Good cybersecurity requires input from every employee at a business – whether they're the CEO or an intern.

DEFENSIVE COORDINATION

Which of the following have you done over the past 12 months to identify cybersecurity risks in your organisation?



Ipsos MORI, 2021

33%

of UK businesses had formal policies covering cybersecurity risks as of 2021

Ipsos MORI, 2021

84%

of cyber attacks rely on social engineering

ENISA, 2020

How human psychology causes cyber attacks

Many high-profile cybersecurity incidents paint a misleading picture of the type of attack businesses should expect. Most breaches don't result from a hacker circumventing an organisation's cyber defences. Instead, cybercriminals are increasingly incorporating social engineering techniques into their scams, relying on psychological manipulation, rather than technology, for success.

Phishing emails are one example of a social engineering scam. These employ a wide range of psychological manipulation techniques to fool the recipient of the email to open a link or attachment that contains malicious software.

Some prey on people's fears, anxieties, or emotions, causing them to lower their defences and let a hacker into their system. Others invoke a sense of scarcity or urgency to goad a victim into acting quickly without thinking.

Jeff Hancock, founding director of the Stanford Social Media Lab, regards cybercriminals as "good psychologists", given the wide range of manipulation techniques they use. But, as Hancock points out, there are cognitive vulnerabilities unique to the workplace, making businesses particularly vulnerable to these types of scams.

"With businesses, the hackers will know about social relationships. You can easily see who someone's boss is, and because many people are deferential to authority, this creates a good attack for hackers looking to get employees to share confidential information."

Widespread home working has exacerbated this issue, with many employees losing the face-to-face time with their managers that's essential for trust building. Cybercriminals exploit this by creating scams that prey on an employee's desire to impress senior team members and the vulnerabilities unearthed by isolation.

Often these scams lead the victim into a decision-making process that's quick, complex and vulnerable to emotional persuasion. This combination is highly effective when the victim is unable to speak to colleagues and get a second opinion on a suspicious-looking email.

Such vulnerabilities add to the perception that staff are often the weakest link in an organisation's defence against cybercriminals. However, the vulnerabilities posed by human psychology in cyber attacks are rarely given the same attention as the technological threats from hackers in cybersecurity training.

Good cybersecurity is about more than technology. With social engineering scams on the rise, businesses need to create a training programme that informs employees both what cyber attacks look like and the thinking that underpins them.

Are employees careless or ignorant about cybersecurity?

When an employee enables a breach, employers may need to determine whether it came about through carelessness or ignorance about the threat posed by hackers. The answer could guide any disciplinary action.

But reaching a concrete answer is a complex process, particularly given the number of cyber attacks created on a daily basis. According to the AV-Test Institute, some 450,000 new pieces of malware are detected every day. Hackers send about 3.4 billion phishing emails daily to potential victims.

The range and frequency of attacks on businesses complicates the training process for employees. Team members must be constantly vigilant about a variety of threats that prey on both the technological vulnerabilities of the business and the psychological vulnerabilities of its staff.

Despite the increase in attacks by hackers, Julien Soriano, chief information security officer at Box, believes employees must be aware of the data they have access to.

"You cannot separate ignorance from carelessness in the wake of a cyber attack. Ignorance is carelessness," he says. "It is the employees' responsibility to do the right thing and comply with their employer's policy and understand their role and responsibility in keeping their access safe."

The lockdown-driven surge in remote working dramatically increased the amount of data employees can access. Virtually overnight, businesses shifted to a work from home system, meaning their data was placed into a more vulnerable environment – and at the same time many employees had greater access to critical documents and information than ever before. This increased both the likelihood and repercussions of a cyber attack, meaning employees need to be always aware of the threat posed by hackers.

Yet with remote working here to stay, the only careless or ignorant actor in the aftermath of a cyber incident is the employer that fails to protect their data, says Alex Rice, co-founder and CTO at HackerOne.

"Inevitable human error is never a satisfactory explanation for a cybersecurity incident. If a human caused a breach of your company simply by clicking a single link, your security practices are to blame, not the human," he says.

"If a company acts to its best ability to reduce cyber risk, it is not anyone's `fault' beyond the cybercriminals who chose to commit the crime.

"We need to get out of this toxic blame cycle that discourages transparency and continuous improvement."

The cybersecurity fail-safe

Despite spending £122bn each year on security solutions, organisations are finding it harder than ever to protect their IT infrastructure. Security is changing and it's time for the convergence of security and operations

The huge increase in home and hybrid working over the past two years means that CIOs and CISOs have re-evaluated security policies and are looking to bolster endpoint security. It's little wonder that Gartner Group report that 61% of CIOs of organisations plan to increase spending on cyber and information security this year.

It's turned out to be a bigger project than expected. According to a survey of 750 IT decision makers carried out by Tanium, 82% of CISOs said that they were overhauling endpoint security, but 94% were faced with endpoints that were either unprotected or overloaded with conflicting software agents. As many as one in five endpoints were discovered to be vulnerable to attack.

Organisations are experiencing more attacks than ever before. Cybersecurity Ventures notes that ransomware attacks on businesses occur every 11 seconds. All the while, businesses experienced a 50% increase in weekly cyberattacks in 2021.

> **Unlike traditional, fragmented approaches to endpoint management, XEM maximises visibility, control and trust, and allows teams to interact with all endpoints in seconds, regardless of the scale and complexity of the IT environment**

Cyber criminals are also becoming more targeted in their attacks. Microsoft's recent 'Digital Defence Report' stated that threat actors have rapidly increased in sophistication over the past year, using techniques that make them harder to spot, and which threaten even the most seasoned IT security team. Criminal groups targeting businesses have moved infrastructure to the cloud, where they can hide among legitimate cloud services, and attackers have developed new ways to scan the internet for systems vulnerable to ransomware.

This massive growth in the number and complexity of attacks, combined with a global shortage of IT security professionals, is a big problem for businesses.

Something needs to change

Endpoint security company Tanium says there is a fundamental problem in how most organisations approach endpoint security management. As the number of IT security threats increases exponentially, companies often respond by buying another point solution. In the last year, 90% of organisations have bought at least one new IT security point solution, and almost half (45%) have bought at least four new products, according to the Foundry 'Security Priorities Study.' A typical enterprise now has 43 separate IT security and security management tools in its infrastructure.

This approach simply isn't sustainable. When businesses add more tools to their infrastructure, they don't necessarily increase their protection, because the pace with which new threats emerge is faster than most organisations can keep up with. This is especially true in today's highly distributed organisations. There's also some evidence that the effectiveness of some point solutions is falling; according to one recent report in the New York Times, the first detection rates of some antivirus tools has fallen below five percent.

Then there's the issue of keeping up with a proliferation of point solutions, each with its own data, interface and owner. Perhaps one tool is managed by IT operations and reports into one data silo daily, but another is managed by compliance and reports quarterly into another data silo. If that scenario is repeated 40 times, that's an example of the data headache that CIOs and CISOs are facing.

This patchwork approach cannot provide complete protection, and it can be actively harmful to corporate security efforts. If an organisation has multiple security tools sitting in multiple silos, CIOs can't get a clear overview of how many endpoints there are, much less how effectively they are protected, and what changes need to be made.

In many ways, security is a data visibility problem. When an organisation is running dozens of systems, and dozens of IT security solutions, each generating huge volumes of data at different rates, how is that data being integrated and understood? Simply put, companies can't protect what they can't see.

Today's security decision-makers need help. They need a platform that helps them to keep up with a proliferation of endpoints, and to understand exactly how each one is performing, the threats posed to it, and how it can be protected. This information needs to be available in one place, and in real-time. Only then can CIOs create a single view of security that is needed to deliver effective protection and create a strategy that prioritises the right things at the right time.

What's needed is a converged solution.

Just how bad are things out there?

Tanium spoke with hundreds of IT security decision makers who said they want a way to reduce and simplify endpoint security management.

Key challenges that organisations face in managing endpoint security include siloed teams, especially in IT operations and security, that aren't able to share security data quickly or effectively. Despite this, many business leaders feel a false sense of confidence about their protection.

43

The number of separate IT security and security management tools a typical company has in its infrastructure

The Foundry, 2021

82%

of CISOs said they were in the process of overhauling their endpoint security

Tanium, 2021

Second, poor visibility of security data leaves networks vulnerable to attack. Some 64% of businesses expect to experience a cyber attack in the next 12 months.

This lack of visibility and fragmented approach puts companies at risk of financial losses, downtime, damaged brand reputation and potential heavy fines for non-compliance. This is a huge concern given that 20.4% of vulnerabilities that are discovered within businesses are classed as high or critical risk. It also takes an average of 61.4 days to remediate a critical risk, according to Edgescan, presenting a huge security risk to organisations.

Endpoint security management must be a higher priority for business leaders. In a recent Harvard Business Review survey, 70% of business leaders said they thought that leadership should be more concerned about cybersecurity.

A new approach to endpoint security management

"It's crystal clear that businesses need a new approach to endpoint management that helps us to keep pace with tomorrow's threats," says Steve Daheb, CMO at Tanium. The reason why so many enterprises fall victim to ransomware attacks is that the tools they use are no match for the sophistication of attackers: tools are slow, unreliable and lack a common dataset to operate from. And they inherently create silos.

This approach to security isn't working. It's time to unite tools and data with a unified solution: converged endpoint management (XEM).

Introducing converged endpoint management (XEM)

Tanium takes a unified approach to IT security management. Its platform combines multiple endpoint tools and data so that organisations can have visibility and real-time data on all endpoints, through a single interface.

"Unlike traditional, fragmented approaches to endpoint management, XEM maximises visibility, control and trust, and allows teams to interact with all endpoints in seconds, regardless of the scale and complexity of the IT environment," says Daheb.

> **It's crystal clear that businesses need a new approach to endpoint management that helps us to keep pace with tomorrow's threats**

XEM provides accurate, real-time data to support end-to-end automation, so information security teams can align their efforts and protect their organisations against attacks more effectively. With a unified approach, there's no need for staff from IT operations, compliance, security and numerous other siloes to spend hours collating and sharing data. It can be viewed in a single interface, meaning IT security teams can do more with less resources.

Legacy management systems are often at the heart of problems for organisations looking to improve visibility and efficiency. Moving to a converged platform gives back countless hours of management time, allowing companies to allocate headcount elsewhere and address dangerous vulnerabilities more quickly and effectively across the whole organisation.

The case for better data

IT leaders can't make effective decisions about security without the right visibility into data across their infrastructure. XEM provides real-time information from every single endpoint, so that critical information isn't locked in siloes, accessed by different teams using different tools.

By converging tools into a single interface, companies can focus on actually delivering effective security. With XEM, organisations can easily see, assess and manage all their IT security data in a single view. Data can be shared, allowing for more effective collaboration and easier, more cost-effective management. Ultimately, a converged approach provides reliable, timely insight that can be used to drive better, faster decision-making. That's essential in today's fast-moving threat landscape.

Providing effective governance

IT governance is a top priority for many CIOs but when it comes to security, it can be almost impossible to achieve. Organisations have multiple teams with responsibility for IT security, including compliance, governance, IT operations, security and risk. These teams are often working in isolation from each other, so there's no visibility of organisation-wide threats.

"Without collaboration or visibility about organisation-wide risks, enterprises can develop blind spots, making both security and compliance a challenge. If you don't have visibility into all your endpoints, it's almost impossible to enforce access policies and maintain control across your IT infrastructure," Daheb says.

The good news is that fixing these blind spots doesn't need to be a complex, time-consuming process. XEM provides a relatively quick solution to existing challenges, increasing efficiency and effectiveness by reducing unnecessary complexity and improving visibility of your IT assets. Daheb adds: "Tanium's platform approach means that everything you need – from risk and compliance to data monitoring and more – is accomplished in a single solution. We can identify where all your data is in a matter of seconds, meaning that you can deploy security tools across all endpoints, with a single control plane and common data set and taxonomy."

Making a difference

Daheb says: "Tanium's XEM offering is the only solution that allows teams to collectively perform detailed and complete discovery, in-depth assessments, enterprise prioritisation, cross-platform remediation, and continuous vigilance everywhere."

XEM-based approaches to endpoint security allow organisations to deliver convergence of IT operations and security, as well as the security infrastructures that are based on point solutions. The Tanium platform aims to change the market and meet the twin challenges of spiralling cybersecurity threats and rising complexity of endpoint security management.

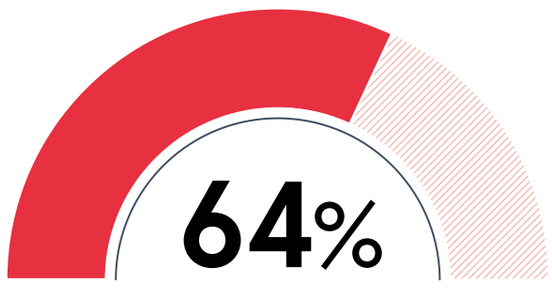
Without XEM, the industry will inevitably see more breaches, more attacks, more data leaks and more problems. It's time to make a change.

Learn more about converged endpoint management (XEM) – visit tanium.com/converged-endpoint-management

TANIUM

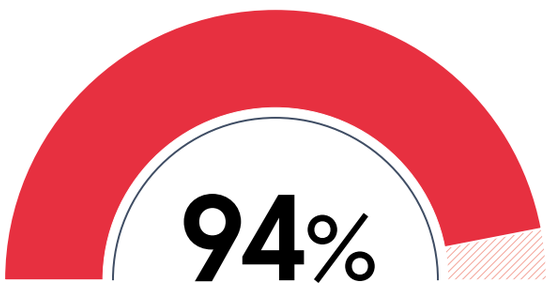
ENDPOINT SECURITY IS CHANGING

How are companies mitigating cyber attacks through XEM technologies?



believe organisations are likely to become compromised by a successful cyberattack in the next 12 months

Tanium 2022



share of enterprises in which up to 20% of endpoints are unknown

Tanium, 2020

20.4% of discovered vulnerabilities were high- or critical-risk

Edgescan, 2021

70% agree leadership should be more concerned about cybersecurity

Harvard Business Review Analytic Services, 2022

11 seconds

frequency of expected ransomeware attacks on businesses by the end of 2021

Cybersecurity Ventures, 2018

61.4 days

mean time taken to remediate a system with critical risk

Edgescan, 2021


Moyo Studio via iStock

ECOMMERCE

The HEAT is on: cybercriminals hunt down web bargains

The rise of ecommerce in the pandemic has opened a lucrative avenue for cybercrime. Now businesses need to wise up to the latest methods of attack and strengthen their defences

David Stirling

Ecommerce came to the rescue of millions of us in the pandemic, be that new iPads to keep the kids busy or a hot tub for stressed adults. But the rush by firms to meet this wave of demand, whether they were a startup, an established ecommerce firm or a bricks and mortar store going online for the first time, left another group of people very happy as well: cybercriminals.

"Many businesses were forced to adopt new selling methods and ways of meeting customer expectations – on the fly," says Yoav Kutner, co-founder and chief executive of ecommerce platform Oro Inc. "At the same time, companies were focused on alleviating supply chain strains and cybersecurity fell a few rungs down the priority ladder. Hackers are now taking advantage because ecommerce sites are a treasure trove of personal data."

This includes online and email addresses when customers sign up to sites, as well as credit card details when they pay for their purchases.

Tom McVey, sales engineer at Menlo Security, says this data means ecommerce firms "have a target on their back". He also fears that many ignored basic security factors as they clamoured to drive sales. "The security maturity of a startup is not that high," he says.

Typical threats to ecommerce operations, he adds, include highly evasive adaptive threats (HEAT), which can bypass traditional security defences that include firewalls and secure web gateways. Menlo saw a 224% increase in HEAT attacks in the second half of 2021.

This can encompass smishing – which is essentially email-style phishing – but this time via text message. The principle is the same in that the hacker is trying to tempt a user to click on a link and unleash malware or ransomware onto a corporate or personal site. Traditional phishing remains a threat, with criminals taking advantage of vulnerabilities in new releases from Firefox or Chrome to launch browser attacks. Again, all you need to do is click on a link in an email for a browser to open and for a malware virus to be launched.

"We're also seeing double-dip ransomware," McVey adds. "Ransomware is where data on your system is encrypted by a criminal, and they refuse to unlock or decrypt it until a ransom is paid. But double-dipping is especially a problem for ecommerce firms because the hacker also steals their customer data, uploads it online outside the company's network and threatens to leak it. If that happened, your entire reputation would be ruined."

Jim Herbert is VP and GM for EMEA for global ecommerce platform BigCommerce. Other exotic sounding threats, he says, include SQL injections (where an ecommerce site insecurely stores data in a SQL database) and cross-site scripting (which involves inserting a piece of malicious code into a webpage). This exposes users to malware and phishing attempts. Another potential means of attack is e-skimming. This is when attackers steal credit card information and personal data by using phishing or XSS to access a site, then they capture a checkout payment in real time.

> **Companies were focused on alleviating supply chain strains and cybersecurity fell a few rungs down the priority ladder**

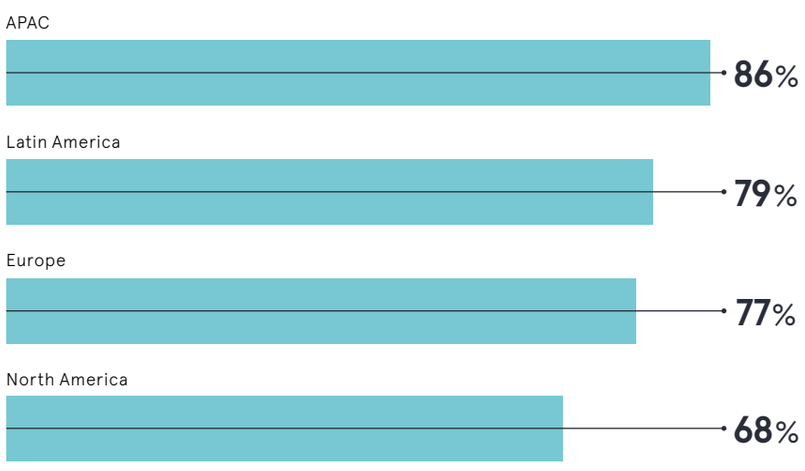
£56bn

Projected size of the ecommerce fraud detection and prevention market by 2025

GlobeNewswire, 2021

CYBER THREATS IN ECOMMERCE

Share of online merchants reporting increased fraud attempts due to the Covid pandemic worldwide in 2021, by region



Cybersource, 2021

Cyber and online payment fraud is a further concern. According to Statista, global ecommerce losses in 2021 reached around $20bn (£16bn), an increase of more than 14% compared with 2020.

Abstract House sells original art and sustainable picture frames to customers via its website and was already established when the pandemic started. But it has seen the scale of threat, including fraud, increase over the past two years.

"We launched in 2017 and saw exponential growth in demand during the pandemic," says co-founder and CFO Summer Obaid. "People began to be comfortable about buying online, including art.

"That's been great for the business, but it has also brought interest from elsewhere. For years, we didn't see any fraudulent sales but now we're experiencing more such as people ordering several £500 gift cards. You may get one order like that but when it is multiple, we try to get more information."

The company, whose original paintings sell for up to £2,000, was aware that dealing with a huge amount of customer data made it vulnerable to attack. Its policy of proactively checking for anything concerning also applies to phishing emails, with employees encouraged not to click on external links and to delete them immediately. But it also has third-party help such as Shopify Plus, which uses machine learning algorithms to flag up orders that could be fraudulent. It also uses Google Business Suite to help protect against spam and secure private data in the cloud. In addition, data can only be seen by employees with privileged access.

McVey advocates web and email gateways to "keep the bad on the outside" and adopting the remote browser isolation model. This means that if an employee does click on a phishing link, there is no direct contact with a company's website and the malware won't run.

Herbert says firms should look at basic protections such as two-step authentication passwords, regularly upgrading software security updates, securing browser connections and ensuring that all connected devices are cyber secure with antivirus software and firewalls.

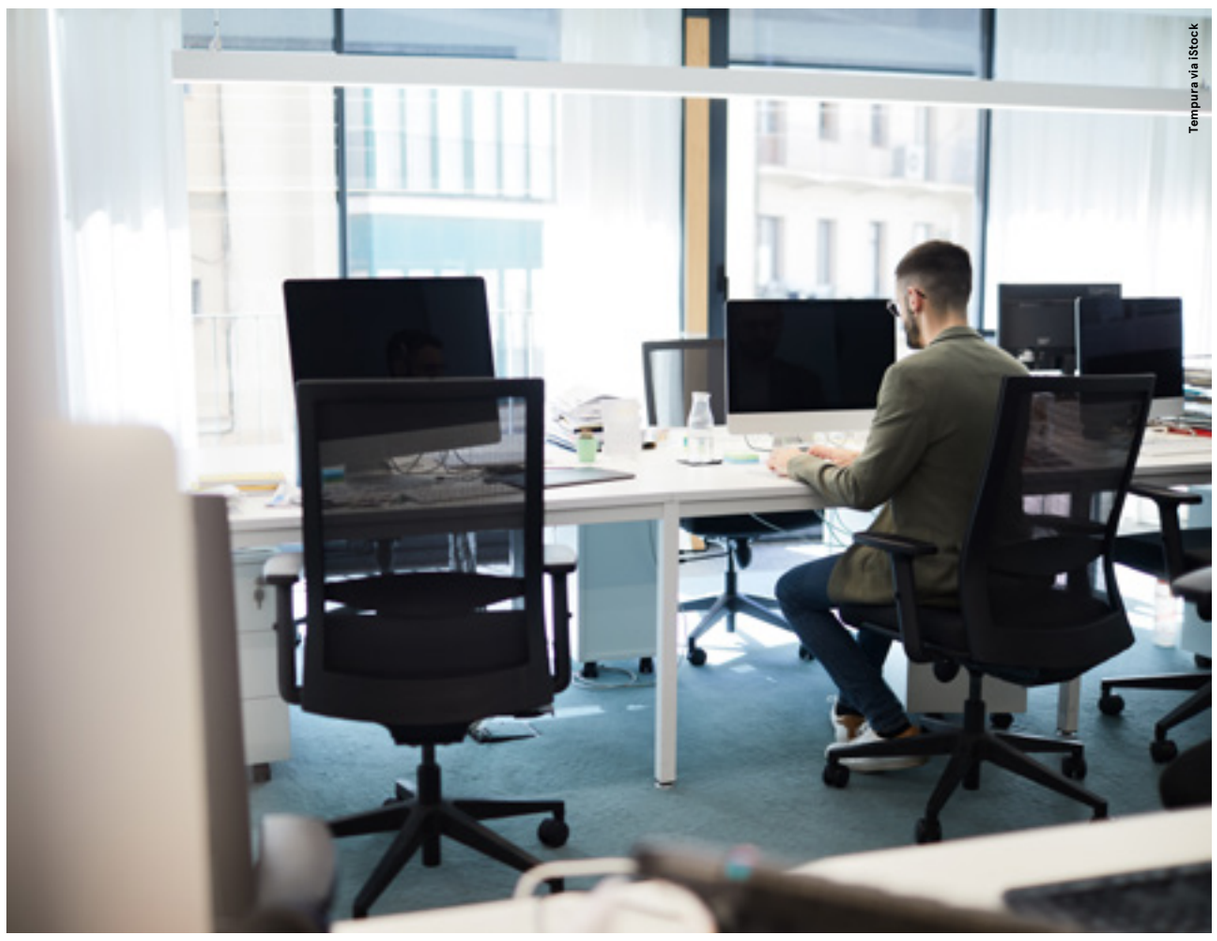
When it comes to payments, Obaid uses an SSL (secure socket layer) certificate on its website, meaning that all data is encrypted at checkout.

For McVey, it is the cloud – including cloud secure web gateways – which not only ecommerce but all businesses should be looking towards for better cybersecurity.

"It is rare for a company to store all its data at its premises nowadays," he says. "All of the documents, applications and emails which we now need to help more people work from home are on the cloud. But most company security strategies remain focused on the office and protecting that. There is a disconnect and little recognition that the world has changed. You can't have an office-based approach for a cloud-based world."

Another impact of hybrid working, McVey argues, and similar to the point Kutner made about the supply chain, is that a lot of IT spend has gone on making the transition as smooth as possible for employees. "Security has taken a bit of a back seat," he says.

Obaid says SMEs especially can't afford to let that happen. "It takes years for a company to build trust with a customer, but one negative experience can be a massive blow to your business. Cybersecurity is a real thing," she says.


Tempura via iStock

SKILLS

Cyberspaced: how to bridge a skills chasm

Attacks are on the increase, but the number of qualified professionals available to repel them is not. How can organisations best deal with this problem?

Emma Woollacott

At the end of March, the Department for Digital, Culture, Media and Sport warned that 39% of businesses had reported experiencing cyber attacks or breaches of data security in the preceding 12 months. In its *Cyber Security Breaches Survey 2022* report, it urged organisations to strengthen their defences.

Yet this is far easier said than done. The number of unfilled cybersecurity jobs worldwide grew from 1 million to 3.5 million in the eight years to 2021, according to research by Cybersecurity Ventures – and this gap is unlikely to close any time soon.

In the UK, the cybersecurity workforce shrank by 65,000 last year, leaving a shortage of 33,000 people, says Clar Rosso, CEO of not-for-profit security training and certification body (ISC)².

The consequences for organisations that have struggled to find sufficiently skilled cybersecurity professionals, she notes, have been alarming.

"What we find is that they are experiencing misconfigured systems. They're not spending enough on risk assessment and management. They're slow to patch critical systems and they're rushing deployments of new tech," Rosso says. "The Russia-Ukraine conflict and the heightened cyber alerts; the zero-day vulnerability in the Log4j Java logging utility that emerged in December; the recent breach at [ID management specialist] Okta – all these are worsening the situation."

Certain roles are proving particularly hard to fill. The US Computing Technology Industry Association (CompTIA) has highlighted specialisms such as penetration testing, auditing, risk management, governance, cryptography, social engineering and the development of defence systems that use artificial intelligence.

"In some cases, the rate of change in these fields is outpacing the speed at which additional cybersecurity professionals can obtain training, certification and sufficient experience," reports CompTIA's chief research officer, Tim Herbert. "Beyond the conventional technical or soft skills gaps, there may be perception gaps whereby employers try to hire a 'unicorn' candidate to fit a very specific mould. There could be location gaps and there could be pay gaps, which tend to be especially challenging for small and medium-sized businesses. And there could be confidence gaps among students or career-changers."

With all these considerations in mind, how can organisations obtain the cybersecurity skills they so sorely need?

The first step is to define the key problems they need to solve, says James Hadley, CEO of Immersive Labs and a former cybersecurity trainer for the government and companies in the defence and finance sectors.

"Companies need to measure where they are with the issues they're facing and, based on that measurement, identify their skills gaps," he advises. "Such gaps could take the form of existing employees who don't understand how their role pertains to cybersecurity, say, but the benchmark assessment could also prove having a deficit of security analysts, for example."

The most obvious way to gain the necessary skills is recruitment, but the scale of the talent shortage is such that organisations may need to cast their net more widely than they're used to.

The cybersecurity profession is notoriously white and male, with new arrivals in the sector generally having a background in IT. Encouraging applications from outside this demographic can give recruiters access to new pools of talent.

"We tend to see women and people from ethnic minorities take an academic route into cybersecurity. So, if you wouldn't normally look to universities when recruiting, seek out people taking degree courses because you tend to find a more diverse set of candidates on these programmes," Rosso says.

Her organisation conducted some research in this field last year. One of its conclusions was that people with more diverse backgrounds are more likely to be attracted to an employer if they can see people who look like them already working in the business. This is because "it leads them to believe they can be successful in your organisation".

Rossi also advocates looking beyond pure technical ability. According to (ISC)²'s *2021 Cybersecurity Workforce Study*, the most important attributes for cybersecurity professionals to have are strong problem-solving and communication skills, plus curiosity and eagerness to learn – all rated as being at least as important as professional certifications and experience.

"I recently spoke with some hiring managers who told me that if they see someone who possesses these skills, they won't even worry about any shortfall on the technical side. That's because they can teach the right candidates those skills in house or send them out for training," she says.

Training up the people you already employ is the other main way to mitigate the cyber skills gap, of course. Indeed, 42% of employers responding to the (ISC)² survey said that they considered this tactic to have the greatest impact.

As with recruitment, there's a strong case for identifying people with the right non-tech skills and then giving them the IT knowledge they need.

"We can help to close the skills gap if we work to increase the cyber literacy of employees across the organisation – people who aren't specifically working in cyber roles but individuals in finance, the legal team and other parts of the business," Rosso suggests. "If we can increase everyone's awareness, that will reduce the need for as many cybersecurity professionals."

Achieving this will entail tailoring people's training carefully, Hadley stresses.

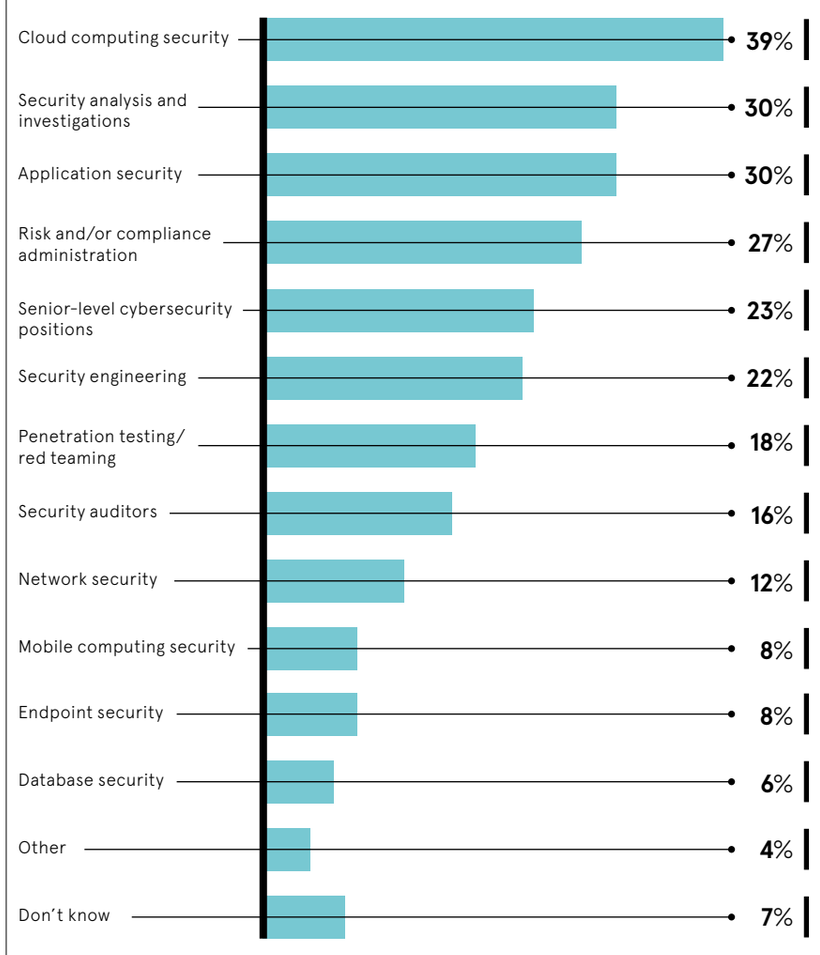
"This is about ensuring the right knowledge and skills are aimed at the right people in the right roles," he says. "Non-technical employees need something that measures what decisions they would make in a given situation and how much confidence they would have in doing so. It should help them to understand the risks better. For members of the board, I might want to run a half-day facilitating session around a simulation."

All these strategies will be necessary, given that the cybersecurity skills gap is expected to widen even further.

"Organisations need to start talking about the fact that this is a long game," Rosso warns. "There isn't going to be a magic pill."

CYBER SKILLS SHORTAGES

Areas with biggest shortage of cybersecurity skills in organisations worldwide



ESG, ISSA, 2021

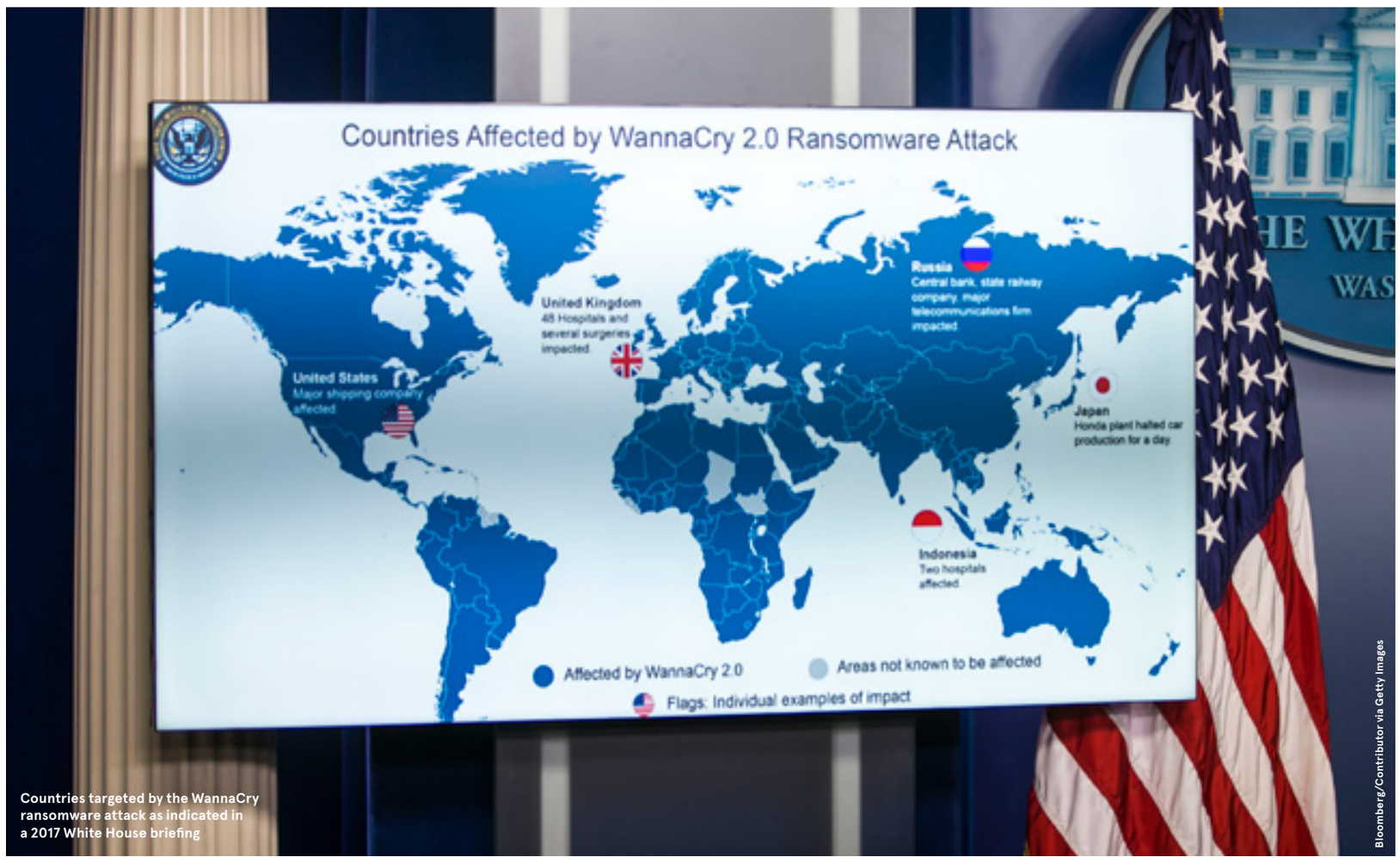
> **We can help to close the skills gap if we work to increase the cyber literacy of employees across the organisation**

THREATS

The new nation-state adversaries

The Russia-Ukraine war has heightened awareness of potential cyber attacks from all nation-state adversaries. Who are the main antagonists and how can businesses and governments protect themselves?

Kate O'Flaherty



Countries targeted by the WannaCry ransomware attack as indicated in a 2017 White House briefing

Bloomberg/Contributor via Getty Images

Attacks in cyberspace can have grave physical consequences, as the 2010 Stuxnet cyber attack showed. Believed to have been jointly carried out by the US and Israel, the infamous cyber assault crippled Iran's nuclear programme after taking over systems and causing centrifuges to tear themselves apart.

More than a decade later, there has been a surge in warnings of a similar attack targeting critical infrastructures such as utilities and water, following Russia's invasion of Ukraine. Alerts from officials in the US and UK describe how Russia is constantly scanning business systems, looking for weaknesses through which to attack.

Growing sanctions imposed on Russia make the country a significant cyber threat to the West. So far, Russian cyber attacks have remained basic, consisting mainly of basic distributed denial of service (DDoS) – flooding websites with traffic to make them unusable – although Ukraine says attempts to hit its electric grid have taken place.

But more broadly, the war has heightened governments' and businesses' awareness of the threat posed by all nation-state adversaries. Aside from Russia, several other major nation-state players are actively perpetrating attacks on the West, each with differing aims.

The main hostile nations are China and Russia, with Iran and North Korea "a close second", says Philip Ingram, MBE, a former colonel in British military intelligence. "They use a mix of state and criminal capabilities, many of which are state-sponsored."

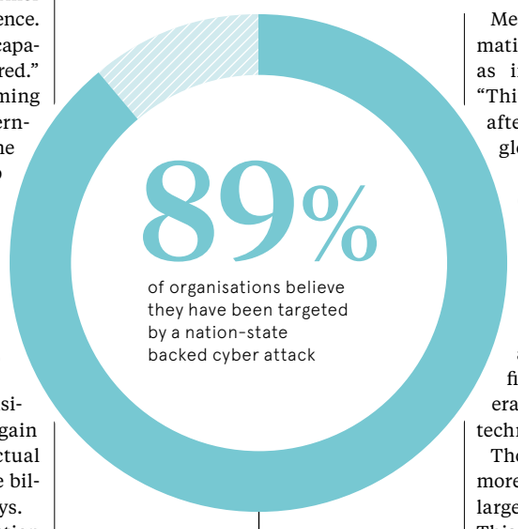
Some nation-state attackers are aiming for financial gain through government-sanctioned organised crime. One example is the North Korean group Lazarus, which was recently linked to a $625m (£492m) cryptocurrency heist. "Economic constraints limit North Korea's efforts to bitcoin heists and ransomware attacks – something the West is getting slightly better at thwarting," says Ian Thornton-Trump, CISO at threat intelligence firm Cyjax.

Other nations are looking to steal business and state secrets. China wants to gain economic advantage through intellectual property, which helps the nation "save billions in development costs", Ingram says.

China has a "very capable" cyber section within its military, says Jamal Elmellas, chief operating officer at security consultancy Focus on Security. "They see cyber as an additional weapon in their arsenal."

Following the Stuxnet attack, Iran's cyber strategy is regional- and defence-focused. Thornton-Trump thinks the country is in watch and learn mode as events in Ukraine unfold. "They desperately want sanctions removed and conducting a major Iranian cyber campaign would be counterproductive to facilitating those discussions."

> **The most successful nation-state attacks are those we don't see or know about**



Trellix, 2022

Meanwhile, Russia is focused on diplomatic and military targets – as well as influencing through disinformation. "This has been evident in Ukraine, and after interference in elections across the globe," says Ingram.

At the same time, the Russian threat comes from organised crime. This is not necessarily sanctioned by the government but is "very capable", says Elmellas.

Hostile nation states are a threat to all businesses, especially if they operate in critical sectors such as utilities, financial services or healthcare. In general, firms developing and fielding new technology should be on alert, Ingram says.

Those involved in a supply chain are also more likely to be attacked as a route into large organisations such as governments. This happened during the 2020 SolarWinds breach, which saw Russian adversaries gain access to US government departments after attacking an IT software provider.

It's a growing risk for businesses to become part of the fallout of a global major cyber attack, even if they are not themselves a target. "The SolarWinds attack provided adversaries with incidental access to many other businesses which were not themselves targeted," says Gemma Moore, director at information security consultancy Cyberis.

Other attacks seeing businesses become part of the collateral damage include the 2017 NotPetya incident and WannaCry ransom attacks. Perpetrated by North Korea, WannaCry brought the NHS to a standstill after hitting multiple organisations via out-of-date Windows XP systems.

Addressing the nation-state threat requires a solid cybersecurity strategy. This includes having "a strong foundation" including the basics, says Ian Usher, deputy global practice lead of strategic threat intelligence at cybersecurity consultancy NCC Group. "Patching, access controls, assessing defensive measures, logging, backups and incident planning."

Threat intelligence also plays a vital role. "It helps organisations understand their unique place within the landscape so they can tailor intelligence collection around the threats most relevant to them," he says.

In addition, business culture is integral in protecting from the nation-state threat. Firms need to understand which business data is critical and ensure it is protected from all risks, Ingram advises.

As part of this, cybersecurity should be part of a business risk strategy. "The threats should be properly understood so the risk can be mitigated in an as cost-effective and business-enhancing way as possible," says Ingram, adding that a sound cybersecurity profile is "a real marketing asset".

Investment in technology is also important. Legacy technical debt will overwhelm firms that have underinvested in IT and security controls, says Thornton-Trump. "Some nation states and cybercriminals will no doubt exploit these opportunities, as victim countries struggle to manage the basic necessities of their citizens in an increasingly polarised political climate."

Overarching this, governance is key, says Elmellas. "It is there for a reason: as the organisation scales up, so should its security capability. You need to be aware of where the boundaries are and make sure to secure them. This is even more critical now than ever, as the borders have moved with increased home working. Test your defences; you have to see security as a functional resource."

Nation-state adversaries will continue to respond, especially in light of sanctions such as those imposed on Russia by the UK and the US. For this reason, it's important to be alert – after all, the most damaging attacks are those that go unnoticed.

"The most successful nation-state attacks are those we don't see or know about," Ingram warns. "Adversaries can be quietly sitting in a network, watching, listening and stealing what is wanted, rather than perpetrating attacks designed to cause nuisance or harm."

Commercial feature

Don't be the weak link in the chain

In an increasingly digital and interconnected business landscape, SMEs are becoming a key point of attack for sophisticated cybercriminals seeking to exploit global supply chains

The cyber landscape has evolved dramatically in recent years – not in the form of new threat vectors but rather the sophistication of bad actors. Organised crime has now firmly extended from physical to virtual, and hackers are increasingly astute at adopting modern key technologies, such as adversarial machine learning networks that trick automated defences.

Phishing and ransomware continue to dominate the threat environment, but amidst the rise of cloud and growing layers of software contributing to products, the greater complexity is creating more opportunities for cybercriminals to exploit. Some are even developing their own value chains employing, for instance, professional call centres in ransomware schemes as a means of 'customer care'.

"Cybercriminals love exploiting complexity," says Jochen Haller, head of information security at IONOS, Europe's biggest hosting provider, which also offers an enterprise-level cloud infrastructure platform. "We are essentially now seeing virtualised operating system stacks inside virtual operating system stacks next to containerised operating system stacks on metal."

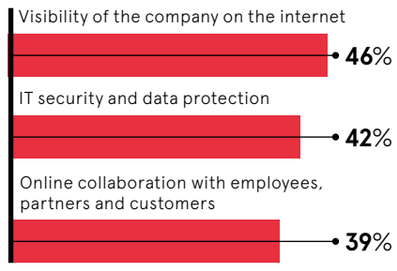
Supply chains have become so global and interconnected that every business is now responsible not only for their own security but also that of their customers and suppliers. This is a particular challenge for SMEs, which typically are not experts in cybersecurity and tend to be further behind larger, better-resourced companies when it comes to digitalisation.

"Organisations have to keep track of each and every piece of software," Haller adds. "And if they lose track of one of them, that's when the bad actors see their advantage. An attacker only has to be lucky once to find an unpatched vulnerability and get in."

A silver lining of the Covid-19 pandemic is that it acted as a powerful accelerant of digital transformation, with businesses forced to adapt to survive. In a research study conducted by YouGov on behalf of IONOS, almost two-thirds of UK SMEs said the crisis positively impacted their digitalisation journey.

FOCUS AREAS OF DIGITALISATION

Which are the areas of focus for your company's digitisation measures



YouGov, 2022

Following the pandemic, digitalisation continues to be central for SME business models, with three-quarters saying it is important to their future viability. Aside from being visible on the internet, security and data protection was noted as the top focus area for SMEs implementing digital measures.

"The biggest challenge for SMEs is coming from the journey into the digital world and facing its security challenges. But if you don't jump on you will be left behind," says Haller. "Companies that fail to digitise will effectively select themselves out of supply chains. If you want to compete in global and even local markets, you just have to do it."

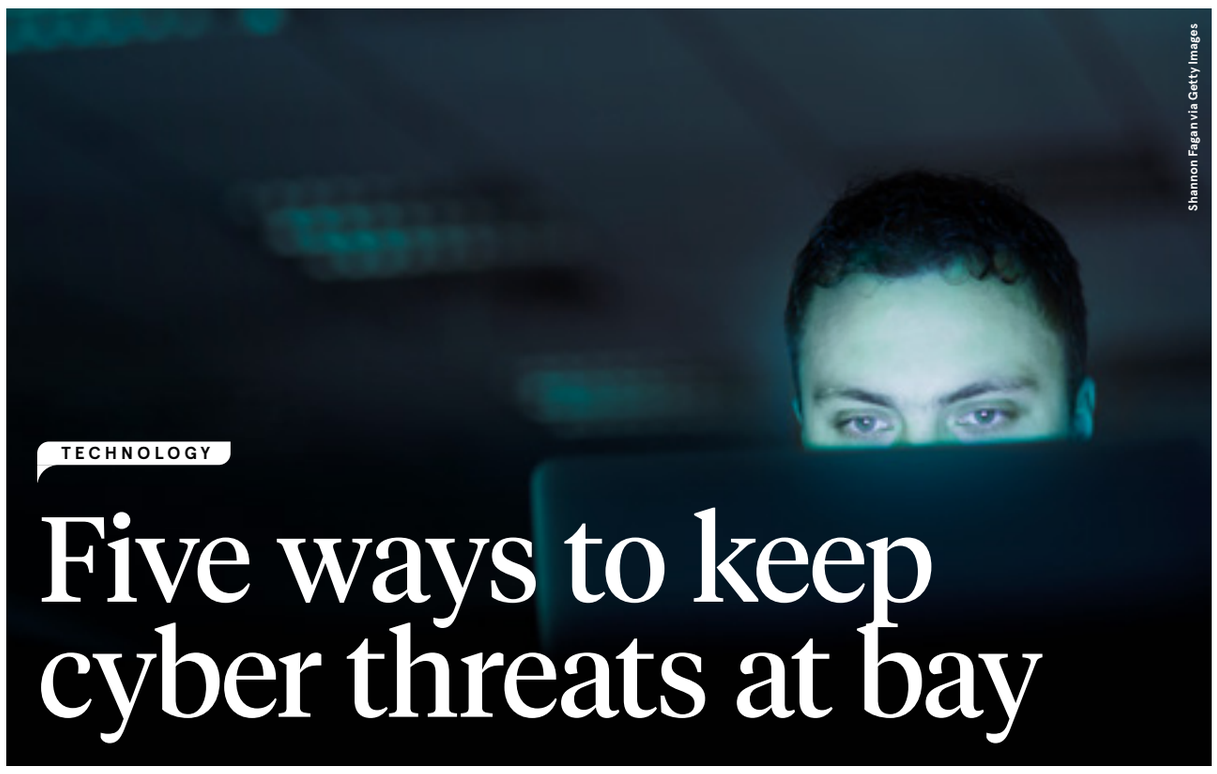
SMEs lacking in-house expertise can be just as digitally savvy and secure as big global corporations, thanks to cloud providers experienced in managing critical infrastructure. "It's important to choose a provider that fits your needs," says Haller. "The typical user journey starts just with email or a domain, but you might also require e-shops, online marketing tools or even full-fledged servers at a later growth stage. IONOS covers this entire journey, from professional back-up solutions up to our high-end cloud infrastructure platform."

A strong cloud hosting provider can offer more security than any individual company can on its own, as well as taking on critical security tasks such as patching and software updates. Small companies need to focus on their core business objectives, which makes outsourcing day-to-day maintenance of their cloud services an attractive option. IONOS provides a vetted pool of qualified experts through its partner network.

"There will always be criminals. Security and privacy will continue to merge, not in terms of compliance but the technical, organisational part. As cybercriminals become even more sophisticated, we on the defence side also have to continuously improve and adopt the best technologies. Greater complexities within systems mean humans can no longer do it alone. Automation will be key, supported by skilled people who can think about how to design this automation and to continuously maintain and improve it."

For more information, visit IONOS.co.uk

IONOS



Shannon Fagan via Getty Images

TECHNOLOGY

Five ways to keep cyber threats at bay

The widespread move to cloud-based hybrid working is putting CISOs under greater pressure than ever to protect their distributed organisations. Here are some of the safeguards they've been adopting

Alison Coleman

1 Never trusting, always verifying

As their hybrid working arrangements mature, firms are working hard to safeguard data security and ensure regulatory compliance. And increasing numbers of organisations are choosing to implement zero-trust networks.

This is a defence measure that moves away from traditional network perimeter security. Instead, following the principles of network segmentation and least privilege, no user or device enjoys inherent trust. With the focus on data and identity, users are given no more access to the system than the minimum they need.

In theory, any enterprise could adopt this 'never trust, always verify' approach to improve its data security.

"The benefits of zero-trust architecture include a reduced threat landscape and an improvement in the visibility of all user activity," says Samantha Martin-Woodgate, compliance community lead at elearning firm Skillcast Group. "This adds real value to all organisations with a large proportion of people working away from the traditional office environment."

But, she notes, most remote workers will still need access to sensitive data to do their jobs. "One of the big challenges of zero trust is the way that it locks down access – and that could bring workflows to a halt, affecting productivity," she says.

2 Strengthening account security

Multifactor authentication (MFA) can greatly improve account security – and consequently is a feature on many websites, applications and devices.

Jim Tiller, global CISO at Harvey Nash Group, says: "Although the concept isn't new, advances such as face and voice recognition systems, fingerprint readers and physical security keys have improved accessibility, effectiveness, privacy and optionality for MFA users."

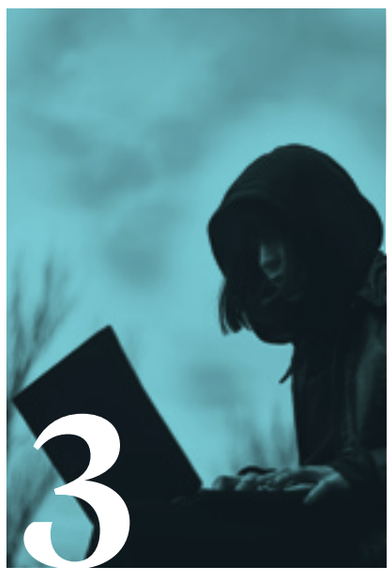
The benefits offered by such solutions are significant, as the technology reduces both parties' reliance on inherently insecure passwords while improving the user experience, privacy and interoperability.

"Every company can gain huge improvements in security by deploying MFA solutions that are either free or very inexpensive," Tiller says.

But he adds that "poor implementation has been a major downside. Examples of this include ineffective session management, the use of SMS text messaging [a relatively insecure authentication method] and a failure to deploy least-privilege or zero-trust methods. All these things will undermine the advantages."

The biggest problem has been the slow rate of MFA uptake so far. For instance, although Microsoft's cloud identity solution, Azure Active Directory, recorded more than 25 billion password hacking attempts in 2021, fewer than a quarter of its customers have adopted MFA to date.

3 Detecting suspicious behaviour by network users



Technology known as user behaviour analytics (UBA) provides an early-warning system that combines machine learning algorithms and statistical analysis to gather insights into regular user-generated network events – for instance, log-ins at certain times of the day. The data enables the UBA system to detect and analyse any deviation from recognised patterns, such as an access request from an unknown location in the middle of the night.

The system has the power to determine whether such an abnormality could represent a significant risk, says Haroon Malik, director of security consulting at cybersecurity consultancy NTT Data UK. It could indicate the presence of "an external threat actor pretending to be an employee or an actual employee who may be introducing an element of risk, say. A risk rating is applied to the suspicious activity and, if this is high enough, the system will alert the senior management team or the IT department."

UBA is used mainly by entities that hold large amounts of sensitive personal data, such as financial institutions and government agencies. It has the potential to detect threats before they can cause serious damage, but it's not yet within the reach of every organisation.

"UBA is an emerging technology that requires a lot of staff training and a period of refinement and calibration before an organisation can use it," Malik says. "This process can be costly, lengthy and labour-intensive."

4 Keeping watch across the gamut of system components

Extended detection and response (XDR) technology is a breach-detection system that works to secure the extensions of an organisation's IT capabilities. This, then, represents a proactive approach to threat detection and response by correlating data flows across servers, networks and cloud workloads.

"This technology applies analytics as well as automation," Malik says. "While XDR has been implemented in some way by businesses over the past couple of years, it's only now we're realising its full capability."

Like UBA, it's a pricey technology that's more suited to larger organisations that have the resources required to calibrate the solution. The biggest benefit is that it closes gaps in visibility while reducing detection and response times, which in turn enhances the productivity of staff in the security operations centre.

"XDR can be expensive and requires fine-tuning to reap its full benefits," Malik says. "The technology is costly for any deploying business in the short term – and it will continue to take up lots of resources in the future."

5 Bolstering ID management and data security

Organisations don't always understand exactly where their most valuable data is or who has access to it. This state of affairs presents a serious security risk.

Many IT and data security organisations use technology known as cloud infrastructure entitlement management (CIEM) as a gatekeeping tool. CIEM solutions apply the principle of least-privilege access to cloud infrastructure and services, helping users to defend against data breaches, malware attacks and other risks posed by excessive cloud permissions.

Joe Hubback, EMEA managing director at cyber consultancy Istari, says: "An identity and data security platform can help an organisation to locate its crown-jewel data and to assess who has access and what 'normal' access behaviour looks like, enabling it to enforce least-privilege access to ensure that it remains protected. For example, Sonrai Security's cloud security platform, Dig, graphically maps all of your identities and determines their effective permissions, allowing you to get least privilege across every cloud you use."

Remote working sparks cybersecurity review

In the era of remote working, cybersecurity is under threat as connections expand. A new technology, Secure Access Service Edge or SASE, promises to protect the distributed workforce

Hybrid working may be a blessing for those who crave a better work/life balance, but it can play havoc with cybersecurity. As employees enjoy the trend of working from a variety of remote locations and accessing apps in the cloud, the attack surface – the entry points for cyberattacks – is expanding rapidly. That's why the IT world is ablaze with talk of a new technology called secure access service edge (SASE) which provides cybersecurity protection for enterprises wherever their employees choose to work.

Today's decentralised workforce are logging onto their laptops from home, at the office, from a coffee shop or the local library. They'll use their smartphones to work on the move in taxis, trains, on street corners or at the airport. Homeworking became the norm during the pandemic and the trend to hybrid working from multiple locations is accelerating. According to Gartner, 75% of workers will continue to split time between home and traditional office locations – the hybrid work model – between now and 2026.

Meanwhile, the apps employees use for work are no longer sitting on the server at the office – they are being accessed in the cloud and can be hosted anywhere in the world. Keeping this growing web of connections secure is becoming a major challenge as organisations struggle against a cascade of cyberthreats and malicious attacks directed against their networks.

Before the spread of hybrid working, cybersecurity was far more centralised. Employees accessed work files and applications via their employer's data centre, the gateway for all the organisation's digital traffic. The data centre hosted cybersecurity controls and while this may have slowed down connections, it provided businesses with the certainty and power to secure data flowing in and out of the enterprise through a single point of access. But with the spread of remote working and the rise of apps hosted in the cloud, employees are no longer connecting to their work tools solely through the central data centre, but accessing apps, files and communications through the open internet and the cloud.

> **If staff are working from anywhere, how does the enterprise ensure that it protects itself?**

This transformation requires a security solution which can protect employee devices at the edge of the cloud, that can secure apps and key data and enforce cyber policies and rules across the vast range of connections employees make. That is why there is such a buzz around SASE, which brings together network connections and cybersecurity to offer a simpler and more effective way of keeping employees connected while protecting networks from cyberattacks.

As Kelly Ahuja, chief executive of SASE provider Versa Networks, says: "If staff are working from anywhere, how does the enterprise ensure that it protects itself? They need an effective, comprehensive security mechanism while being able to connect those users seamlessly and easily. SASE enables this while making sure the user, the data and the applications are protected. Security is multi-layered. When you protect your home, you don't just lock the front door, you secure the windows, switch on the alarm and secure the back door too. This is in effect what SASE allows enterprises to do with their networks."

Versa Networks is one of the leading independent providers of SASE systems, which have been a logical development of its offer of secure SD-WAN – a technology that enables enterprises to securely connect their sites, ensuring maximum application performance over internet, mobile and private networks. "We have been providing our market leading security and SD-WAN solutions for many years and overall as a company we have thousands of customers," says Ahuja. "SASE has come up in the last couple of years, but what we have been doing since the company was founded is preaching that networks and security have to come together and that there is no network worth having without security. That has been our mantra since day one," he says.

Initially incumbents offering network or security products argued against this.

"It turns out Versa was right. Security and networks are converging through SASE," says Ahuja.

Enterprises large and small are transitioning to the new all-purpose, fully integrated SASE networking and cybersecurity solution, simplifying their systems, protecting the business, and saving money along the way. This will allow today's generation of hybrid workers to adopt this flexible lifestyle while keeping the ubiquitous cyber marauders at bay.

For more information, visit versa-networks.com

VERSA NETWORKS

INSIGHT

'Cybersecurity professionals aren't born cybersecurity professionals'

A Q&A with **Eleanor Dallaway**, editorial director, *Infosecurity Magazine*, on gatekeeping practices and diversity in the cybersecurity industry

Q Why does a skills gap exist in the cyber industry?

A It's a multifaceted answer, but I believe the two most important components are industry gatekeeping and lack of diversity. A talent pipeline takes a very long time to build and nurture. Last year, the industry association (ISC)² estimated the cybersecurity skills gap to be 2.7 million people. While there are varying degrees of acceptance of this statistic, it is undeniable that the demand for infosec talent certainly exceeds the supply.

When analysing job advertisements and hiring practices in information security, it becomes quickly apparent that jobs are not being tagged as entry-level. Even junior positions require years of experience, formal education and even certification.

Although cybersecurity is an investment priority among IT departments, this does not mean that talent supply automatically exists to meet demand. Despite investment intentions, organisations sadly will not simultaneously be presented with a pool of trained and certified talent chomping at the bit to get their foot in the door.

Q Is the cyber industry losing out on opportunities because of restrictive hiring practices?

A Of course. There's certainly a skills gap, but I wonder whether we should consider it more as a demand gap given the gatekeeping taking place. Demand for entry-level people is so low that it's hard for people to break into the industry. There are unfulfilled jobs because hirers are demanding too much of the wrong things.

Some of the most inspiring people I've interviewed over the years have attributed their landing in the industry to serendipity, armed with no formal qualifications, but enormous passion and acumen. The onus should be on us, as an industry, to spot, welcome and nurture that raw talent. The cybersecurity industry needs to back itself as desirable, affluent and worthy, but it also needs to back entry-level talent as the next generation of infosec pros.

It is also important not to downplay or overlook the ethical impact of gatekeeping. Educational elitism is just one part of this, but diversity is another. The cybersecurity industry has a marketing issue on the diversity front. Industry rhetoric discourages diverse candidates from pursuing a career in the industry.

There's nothing wrong with the entry-level talent available. It is perfect the way it is. It is the hiring managers and the recruiters that need a dose of reality, a spoonful of ethics and a helping of fresh perspective.

Q What is the solution to the gatekeeping problem in cybersecurity?

A To address the gatekeeping problem, we need to change the perspective of the gatekeepers. We need to convince infosec leaders that it's not only important, but easy, to train the next generation of cybersecurity professionals.

It's important to recognise that technology will never solve the skills gap. AI will continue to forge ahead, giving a competitive advantage to defenders – but sadly, also to attackers. There is a huge amount to be said for automation, and I am certain that AI will have an increasingly meaningful impact on our industry. That said, the core of the cybersecurity industry will always be people.

Cybersecurity professionals aren't born cybersecurity professionals. Yes, there's a particularly desperate skills gap at mid-level and senior leadership levels, but that talent isn't ripe to be picked. We need to take the young and the hungry, those with curious minds and a passion for problem-solving and winning, and give them a chance. Cybersecurity, for all its complexities, isn't rocket science.

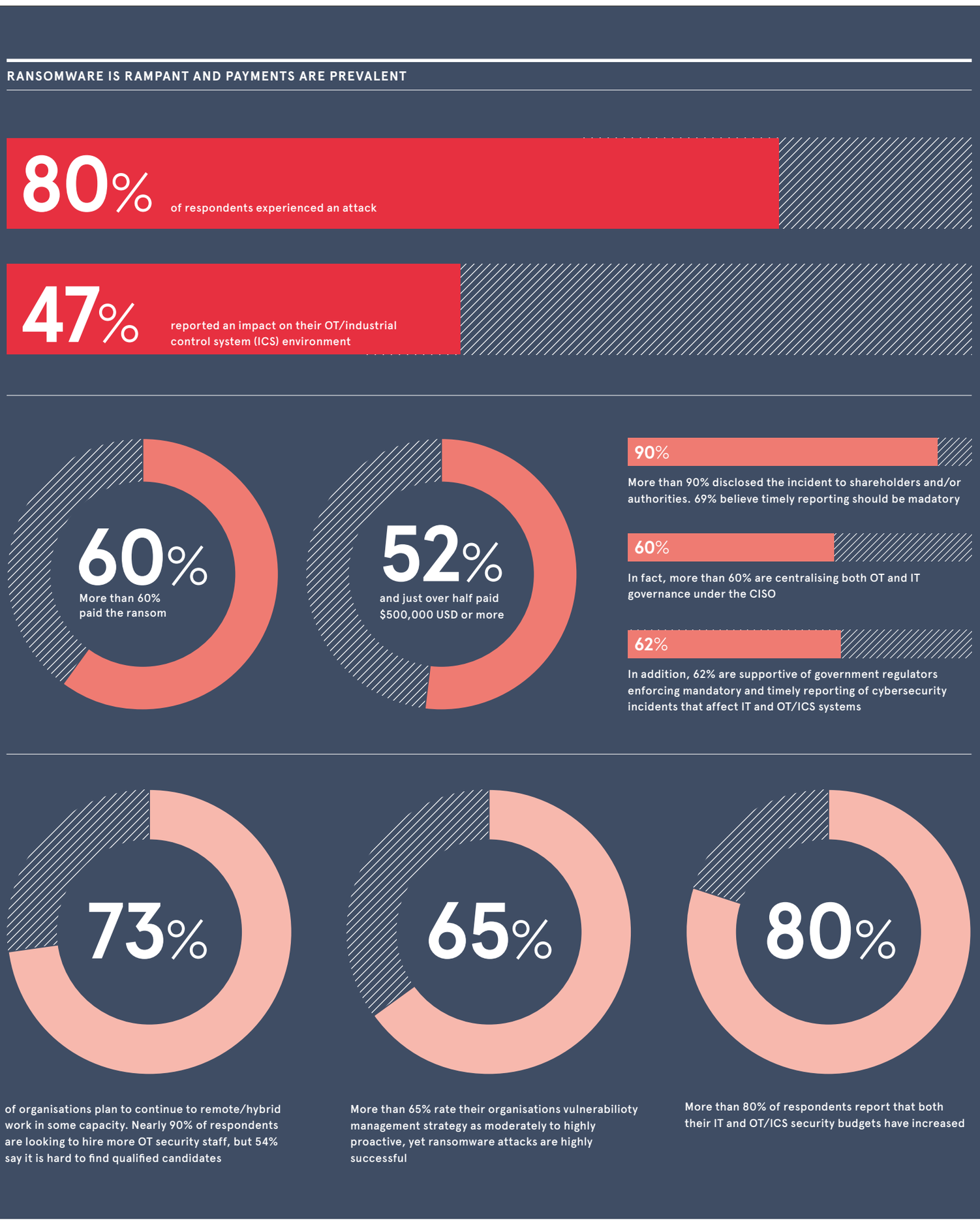
I refer to the saying, "Don't judge each day by the harvest you reap but by the seeds that you plant." Progress will take time, so we need now to plant the seeds. It's time to throw open the gates so fiercely guarded to date and search for talent, including diverse talent, without prejudice or preconceived ideas. ●

Eleanor Dallaway
editorial director,
Infosecurity Magazine
http://infosecurity-magazine.com

Commercial feature

Risks amplify in the connected world

Industry 4.0 has clashed with Covid-driven remote working to significantly expand the cyber attack surface, yet most organisations are unable to protect their cyber-physical systems



The cyber threat landscape has been largely shaped by two major events over the last couple of decades. In the wake of the 'fourth industrial revolution,' digital transformation pushed companies to automate and optimise their processes. More recently, the Covid pandemic not only accelerated digitisation but also forced businesses to embrace remote working. Staff and third-parties now access sites remotely. The result of both events is an enlarged attack surface which has given bad actors more entry points, increasing the frequency and impact of attacks.

Despite cybercriminals becoming more sophisticated in the technologies they use to attack companies, ransomware largely remains the weapon of choice. Some of the biggest critical infrastructure shutdowns last year, including the Colonial Pipeline, JBS Foods and Ireland's Health Service, were ransomware attacks, and a study by Claroty found that 80% of critical infrastructure organisations have experienced a ransomware attack in the last year.

Among those companies, 47% reported an impact to their industrial control system (ICS) environment and over 60% paid the ransom, more than half of which cost $500,000 or more. The majority of respondents estimated a loss in revenue per hour of downtime to their operations equal to or greater than the payout. And even among those who did pay the ransom, 28% still experienced substantial impact to operations for more than a week. It is perhaps unsurprising that manufacturing is the most targeted sector of all, with some 23% of ransomware attacks on manufacturing companies, according to IBM.

"Industry 4.0 is a major driver of this, and we've seen a rapid acceleration of the connected environment," says Simon Chassar, chief revenue officer at industrial cybersecurity firm Claroty. "Ten years ago, there were fewer than a billion devices connected. Today, there are almost 15 billion devices, and by 2025 we are talking more like 75 billion devices connected."

"Companies are trying to be more competitive, so they're adding more and more smart devices, which generate more data to fuel insights, automation and improve efficiency and productivity. The CEO of every company, particularly in manufacturing and healthcare, wants to push their top-line revenues and they know digital transformation, adding these connected assets, will help them to produce more and reduce costs. But this is also creating huge risks."

Cyber-physical systems are especially at risk – the connected devices that control the production process in manufacturing or that keep healthcare operations running efficiently. These systems are all interconnected, and if just one major supply goes down as a result of a cyberattack, there can be a vast impact on critical production lines – as well as, in some cases, the physical safety of production staff. The risk posed by these attack vectors means companies need to be selective on how to progress with digital transformation.

Analyst firm Gartner identified six steps in the maturity of the customer journey when looking at how to secure cyber-physical systems, starting with awareness. Organisations must understand the need to protect not just their IT, but also their cyber-physical systems in terms of their operational technology. According to Gartner, most organisations (60%) are in this awareness step and have secured a directive from the board to do something about it.

The second step is visibility, which presents the biggest challenge. Most companies have almost no visibility as to what assets are connected in the network, leaving them blind in understanding what they actually have to protect. The third step is assessment of the vulnerabilities and risks. A further 30% of organisations are between these two steps.

"That means 90% of businesses are caught between awareness, visibility and assessments. They basically haven't even started to protect their business," says Chassar. "They urgently need to be able to progress to the next steps.

Next is firefighting, prioritising the risks and starting to deploy solutions. The fifth step is the actual integration with the stock as well as the different tools in their security infrastructure. Then the final step is optimisation."

> **Ninety per cent of businesses basically haven't even started to protect their business**

Claroty empowers organisations to advance faster and more confidently through these steps. The company's unified platform, secures cyber-physical systems across industrial, healthcare and enterprise, integrating with organisations' existing infrastructure to provide a full range of controls for visibility, risk and vulnerability management, threat detection and secure remote access.

Through its research and engineering teams and thousands of sites deployed globally, as well as its partner ecosystem, which includes industrial giants such as Siemens, Schneider Electric and Rockwell, Claroty has the domain expertise to help organisations secure their cyber-physical systems. The company focuses on three major areas in protecting businesses. First, and perhaps most importantly, is understanding their risks, which means getting better visibility.

"That's number one, because most organisations don't understand the vulnerabilities and the risks associated with the assets they have," says Chassar. "Second is controlling the access. In our platform, we follow a holistic approach by acting like a one-stop-shop, and the control comes from secure remote access. When businesses changed their operations to remote access during the pandemic, it presented a lot of new risk, so this is an essential step.

"The third area is to detect and respond to threats. To do this, we have continuous threat detection in real time with alerts and reports, ensuring companies understand if something is going on that needs to be addressed and mitigated. The combination between our domain expertise and holistic approach is critical for organisations to be successful.

For more information, visit claroty.com

CLAROTY

Q&A

Securing the Extended Internet of Things

The extended internet of things (XIoT) is exposing businesses to new cyber threats. **Yaniv Vardi**, CEO at Claroty, discusses the key vulnerabilities and how CISOs can better prepare

Q What do you mean when you refer to the XIoT?

A Think about everything connected within the four walls of a manufacturing site. You've got operational technology (OT), which which consists of the actual assets that are part of the production line; the controllers and human machine interfaces (HMIs); the temperature sensors and other sensors that are part of the production process. Or in a healthcare setting, there are the medical devices, the clinical assets, the MRIs and imaging devices. But then also think about enterprise IoT, such as smart printers, building management systems and humidity sensors. All of it is now connected, and you cannot overlook any element from a security perspective.

Q To what extent is security designed into XIoT assets in the first place?

A Many if not most of the connected assets in the XIoT were not designed with security in mind. These are legacy assets. The controllers in production lines are a good example. They used to be completely isolated and air gapped, so there was little reason for the manufacturers producing them to think much about security. Those legacy assets still exist today. And even though newer assets in manufacturers' product portfolios have been designed with security in mind, they are continuously operational 24 hours a day, 365 days a year. That makes it really hard to patch or upgrade, which is what makes these assets so vulnerable to cyber threats.

Q What are the biggest challenges facing CISOs in the XIoT?

A The biggest challenge, if you speak to CISOs and CIOs, is they have no visibility of these assets in the XIoT. Their view of OT and IT environments is very much separated. They know everything that's going on in the IT side, but not the OT side. They've had decades of experience managing IT, but OT is really the dark side for them because assets were not previously connected but suddenly now they are – and how can you protect something you can't see? It's a big visibility gap, and these assets are typically on the same network as your critical infrastructure and assets. The consequences of an attack on these assets can be dire.

Q How alert are cybercriminals to these vulnerabilities?

A Attackers will always go for the easiest path to get in and they are very much going after the XIoT as we speak, which is why we are seeing such a huge increase in ransomware. Cyberattacks on the software supply chain, meanwhile, are changing the market. The SolarWinds attack at the end of 2020 rocked the business world and brought numerous challenges in 2021. The European Union Agency for Cybersecurity expected there to be four times more software supply chain attacks in 2021 than there were in 2020. However these types of attacks are nothing new. The attack on department store chain Target was nearly a decade ago now. The NotPetya ransomware attacks, which resulted in $10bn of damages, was back in 2017, though we are still seeing the impact today. And it's not just Russia attacking Ukraine – the impact spreads far beyond that. The software supply chain is really a very significant risk to businesses, as it spreads so quickly through the global markets.

Q What will separate the winners from the losers of business in the XIoT age?

A The winners in the years ahead will be those who go through the full journey to secure their cyber-physical systems. They will gain visibility, understand the network, control access to that network and monitor it for threats. If you haven't already, you need to start that journey today. The winners will be those that connect security with the business to create real business continuity, deploying solutions with domain expertise. The more critical and complex the environment is, the more specialised the security tools need to be. You cannot just have a generic tool to do that. It's like getting new doors and windows, smart cameras and alarm systems, but then leaving your window open. That's exactly what you do when you protect IT but not OT assets. If you have hundreds of proprietary protocols, you cannot simply think that because you already have a security solution for enterprise IoT, firewalls and the like, that it will protect the industrial networks in manufacturing and healthcare settings. It won't. Attacks will happen, no doubt, and there is an enormous impact on a business when they do. You have to do it right.

> **The winners in the years ahead will be those who go through the full journey to secure their cyber-physical systems**

For more information, visit claroty.com

CLAROTY