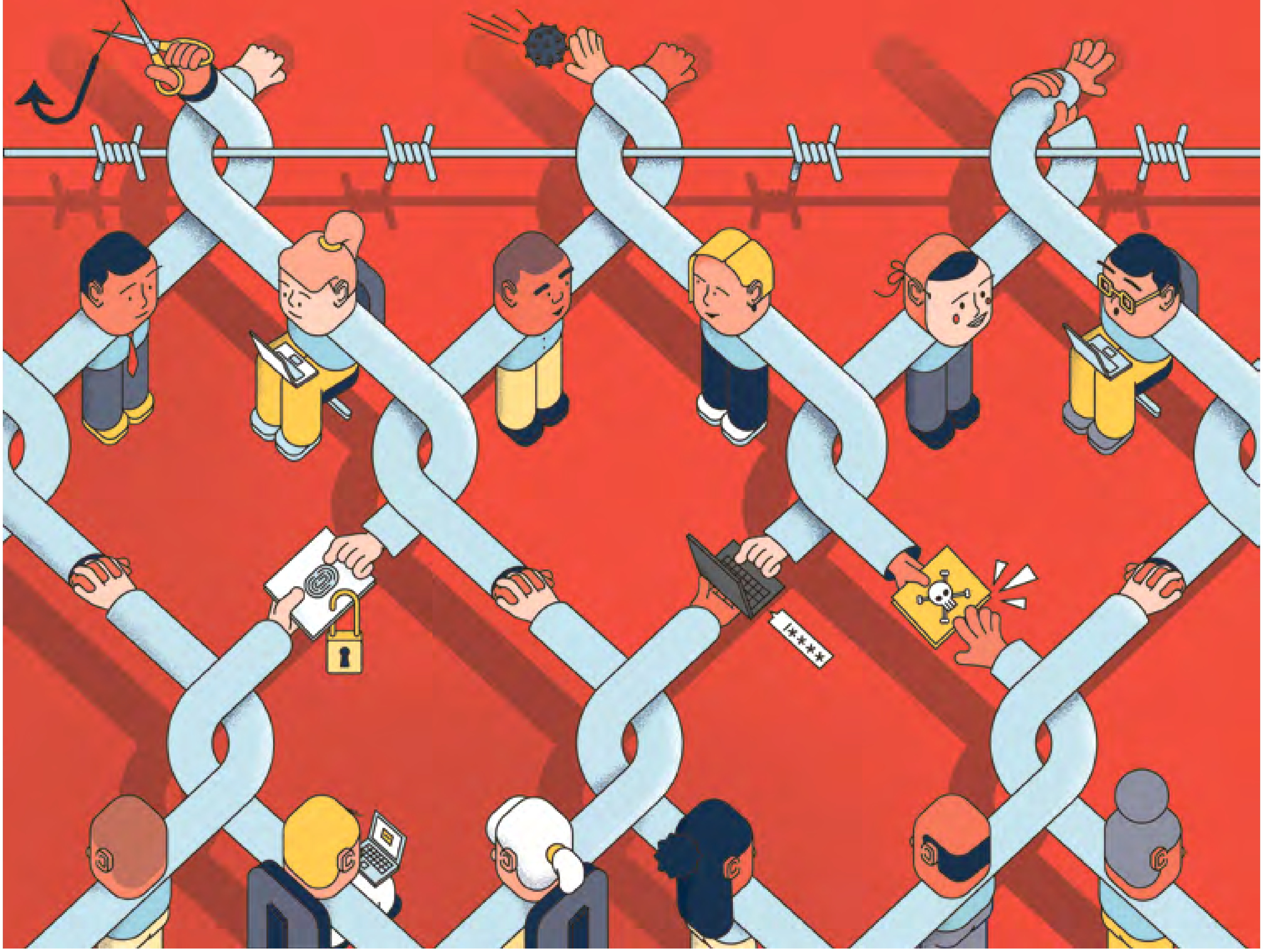
INDEPENDENT PUBLICATION BY Raconteur RACONTEUR.NET #0885 21/09/2023

CYBERSECURITY & THE CTO



CYBERSECURITY & THE CTO

Distributed in
THE TIMES

In association with
DIGITAL LEADERS

Contributors

Christine Horton
A long-term contributor to specialist IT titles, writing about technology's impact on business.

Andy Jones
An experienced journalist and broadcaster who has written for a range of national newspapers and magazines.

Rich McEachran
A journalist covering business, technology and sustainability for publications including *The Guardian* and *Wired*.

Josh Sims
A freelance journalist, author and editor who contributes to titles in several countries.

Seven Standen
A freelance writer covering a wide range of business issues, including disability in the workplace.

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

Raconteur

Reports editor
Ian Deering

Deputy reports editor
James Sutton

Editor
Sarah Vizard

Chief sub-editor
Neil Cole

Sub-editor
Christina Ryder

Commercial content editors
Laura Bithell
Joy Persaud

Associate commercial editor
Phoebe Borwell

Head of production
Justyna O'Connell

Production executive
Sabrina Severino

Design
Harry Lewis-Irlam
Colm McDermott
Samuele Motta
Sean Wyatt-Livesley

Illustration
Sara Gelfgren
Kellie Jerrard
Celina Lucey

Design director
Tim Whitlock

Although this publication is funded through advertising and sponsorship, all editorial is without bias and sponsored features are clearly labelled. For an upcoming schedule, partnership inquiries or feedback, please call +44 (0)20 3877 3800 or email info@raconteur.net
Raconteur is a leading business media organisation and the 2022 PPA Business Media Brand of the Year. Our articles cover a wide range of topics, including technology, leadership, sustainability, workplace, marketing, supply chain and finance. Raconteur special reports are published exclusively in *The Times* and *The Sunday Times,* as well as online at raconteur.net, where you can also find our wider journalism and sign up for our newsletters.
The information contained in this publication has been obtained from sources the Proprietors believe to be correct. However, no legal liability can be accepted for any errors. No part of this publication may be reproduced without the prior consent of the Publisher.

@raconteur raconteur-media @raconteur.stories

raconteur.net /cybersecurity-sep-2023

TEAM STRUCTURES

The case for merging the fraud and cyber silos

The rise in highly skilled criminal gangs is a strong argument for cybersecurity and anti-fraud professionals to join forces

Andy Jones

During the Covid-19 pandemic, 3.2 million UK households bought a pet to stave off lockdown loneliness. Unfortunately, where that kind of cash goes, criminals usually follow.

Pets4Homes, the most popular pet-classifieds platform in the UK, was soon besieged by fraudsters and cybercriminals keen to dupe would-be pet-owners. Axel Lagercrantz, its CEO, soon realised that the unprecedented consumer demand led to a spike in activity from sophisticated and multi-disciplined criminal gangs.

This ranged from puppy smugglers and fraudsters marketing puppies that didn't exist, to cybercriminals attempting to steal data. Despite the company's interventions, the fraudsters would reappear on the site using different names and contact details.

Lagercrantz decided to set up a 24/7 reactive team. Its brief was simple: to identify fraud and cybersecurity threats and, crucially, share that information around the business, with a focus on seamless, silo-free communication between the company's risk-detection points.

This team cross-checked IP addresses to confirm the vendors behind each advert did live at the address listed on their account. They then applied the banking industry's Know Your Customer identity checks on pet vendors, with breeders required to provide a photo of themselves alongside a picture of their ID. Any new photo of a puppy was also checked to make sure the image hadn't simply been stolen from elsewhere on the internet.

Pets4Homes soon found it was consequently blocking more than 40% of all adverts, as attempts to place fake or misleading adverts increased by more than 300% compared with 2019.

Today, less than 0.1% of advertisers with Pets4Homes are flagged as problematic in any way, observes Lagercrantz. "And with every added layer of verification and security, we have seen a constant drop, not only in confirmed cases but as well in attempts."

This principle – that fraud and cybersecurity teams have been kept apart for too long – is one that other parts of UK plc would do well to discover for themselves.

For instance, the financial services sector spends £22,000 every hour fighting fraud and financial crime.

Klaus Vedfelt via Getty Images

But with cyber crime and fraud moving in closer circles because of the rise of highly skilled crime gangs, this investment may be going to waste unless all the information about digital threats is shared effectively.

Anti-fraud and cybersecurity teams should therefore have transparent lines of communication, sharing their findings, workflows and resources. This should be the case across the three core threat functions of identification, monitoring and response. So says Marit Rodevand, co-founder and CEO of Strise, an anti-money-laundering software which is widely used by banks across Europe.

Rodevand goes on to explain that while the sensible application of AI can help to overcome any gaps in legacy technology, businesses should also constantly examine how and where risk information is shared among their teams. When a high-risk customer has been denied certain services by one department, it should be impossible for them to become a customer in another.

"In larger organisations, a chief risk officer oversees these combined efforts and implements greater internal collaboration," Rodevand continues. "Especially when a transition from siloed legacy systems is required, as this is often a complex barrier to integrating fraud and cyber departments."

Effective protection isn't about blindly merging cyber and anti-fraud teams, though. Instead, teams should be encouraged to share information about threats by establishing a 'cyber-fraud' function, such as a regular meeting among key team members. That's according to Eliza-May Austin, co-founder and CEO of cybersecurity consultancy th4ts3cur1ty.company.

"Equip them with a whiteboard and allocate 2 hours to see what unfolds," she suggests. "Observe how these sessions benefit your business and how the people involved in them perceive the potential synergies. If this approach proves effective, consider making it a regular practice or explore the idea of a broader restructuring."

Quick wins, like applying shared terminology across teams, can ensure jargon does not get in the way of closer collaboration. "You'd be surprised how effective a shared vocabulary can be in achieving a common end goal," says Rodevand.

Businesses can unite fraud and cyber operations further by standardising risk-scoring across teams, says Rodevand. "This avoids duplication of risks. It's easily achieved by assigning people with responsibility for overseeing these efforts."

While not every potential fraudulent email has to be reviewed by a cybersecurity expert, fraud specialists must share insights into emerging trends and scams with their cyber counterparts, says Austin.

Removing some of the barriers between fraud detection and cybersecurity isn't about forcing talented people to job-share or cover two functions at once, adds Austin. "Fraud analysis is an individualised process. It demands a dedicated and competent team capable of responding to anomalies in say, card usage, or detecting attempts by individuals to impersonate vulnerable relatives over the phone. Fraud focus remains on individual cases.

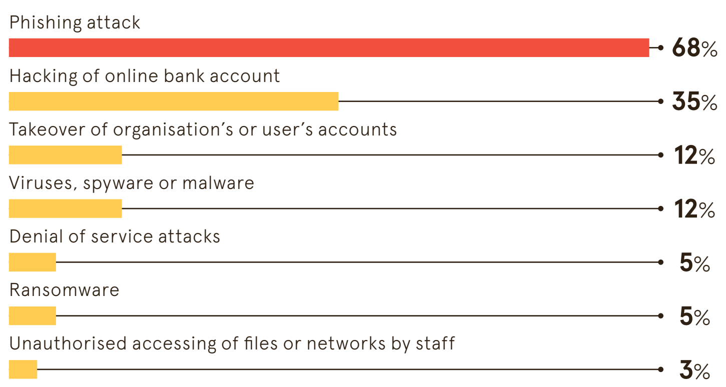
"On the other hand, cybersecurity is a broad domain encompassing network security, endpoint security, infrastructure as code-based forensics, incident response, testing, detection and response, and engineering, among other aspects. Each of those requires a distinct skill set."

Separation is also an important part of compliance checklists, which will likely vary across cybercrime and fraud departments. After all, a Know Your Business (KYB) checklist is different from a cybersecurity checklist, says Rodevand. "Implementing a centralised checklist would require employees to undertake checks that may not always be necessary, draining time, money and resources."

While treating cybercrime and fraud as a shared problem encourages teams to share operational expertise and have the same goals in mind, it's worth applying skilled professionals wisely, says Austin. "There's little value in deploying highly skilled cybersecurity analysts to investigate whether someone on a call was impersonating a relative to secure a loan. To the untrained ear, anti-fraud and cyber detection may seem similar, but they are fundamentally different in terms of their focus and required skill sets." ●

CYBER-FACILITATED FRAUD MOSTLY COMES VIA PHISHING

Prevalence of attack vectors among UK businesses that suffered cyber-facilitated fraud in 2022



Department for Digital, Culture, Media & Sport, 2023

EDITOR'S NOTE

'The cyber experts need to get their house in order'

In a vicious threat landscape where cyber criminals are increasingly going after managed service providers themselves, the good guys will need to up their game

Ten years ago, back when the West was first waking up to the rising threat of Chinese state-sponsored cyber attacks, American legal scholar and political commentator Noah Feldman had this to say: "As a strategic matter, [these attacks] do not differ fundamentally from older tools of espionage and sabotage."

At the risk of going all 007 here, the comparison remains an apt one today, whether we're talking about attacks at the level of nation states, or among businesses and individuals. After all, the vast majority of cyber attacks don't come direct from governments or the military; they generally involve a certain amount of deniability, given the various steps that can be taken to obscure an attack's origin; and there are some significant prizes up for grabs, especially if the attack results in financial losses or major data breaches.

Crucially, though, anything goes. "Cyber war takes place largely in secret, unknown to the general public on both sides," Feldman wrote. (The latter point there has aged a little, but we'll forgive that.) "And best of all for China, the rules for cyber war are still very much in flux."

Even a decade on, that state of flux is still a defining feature of modern cyber espionage. And the latest twist is that corporate cybersecurity providers around the world are increasingly finding themselves in the firing line. Were this a Bond movie, this would be the point at which the villain becomes obsessed with destroying our hero, usually to the detriment of their own dastardly plans.

And things really are getting personal out there. For instance, as the *Financial Times* reported last month, the CEO of one US-based cybersecurity company received a message earlier this year in which a hacking group declared that it had accessed his firm's email server and threatened to publish sensitive data unless a ransom was paid. When the CEO refused to play ball, the hackers found his son's passport details, school and telephone number online.

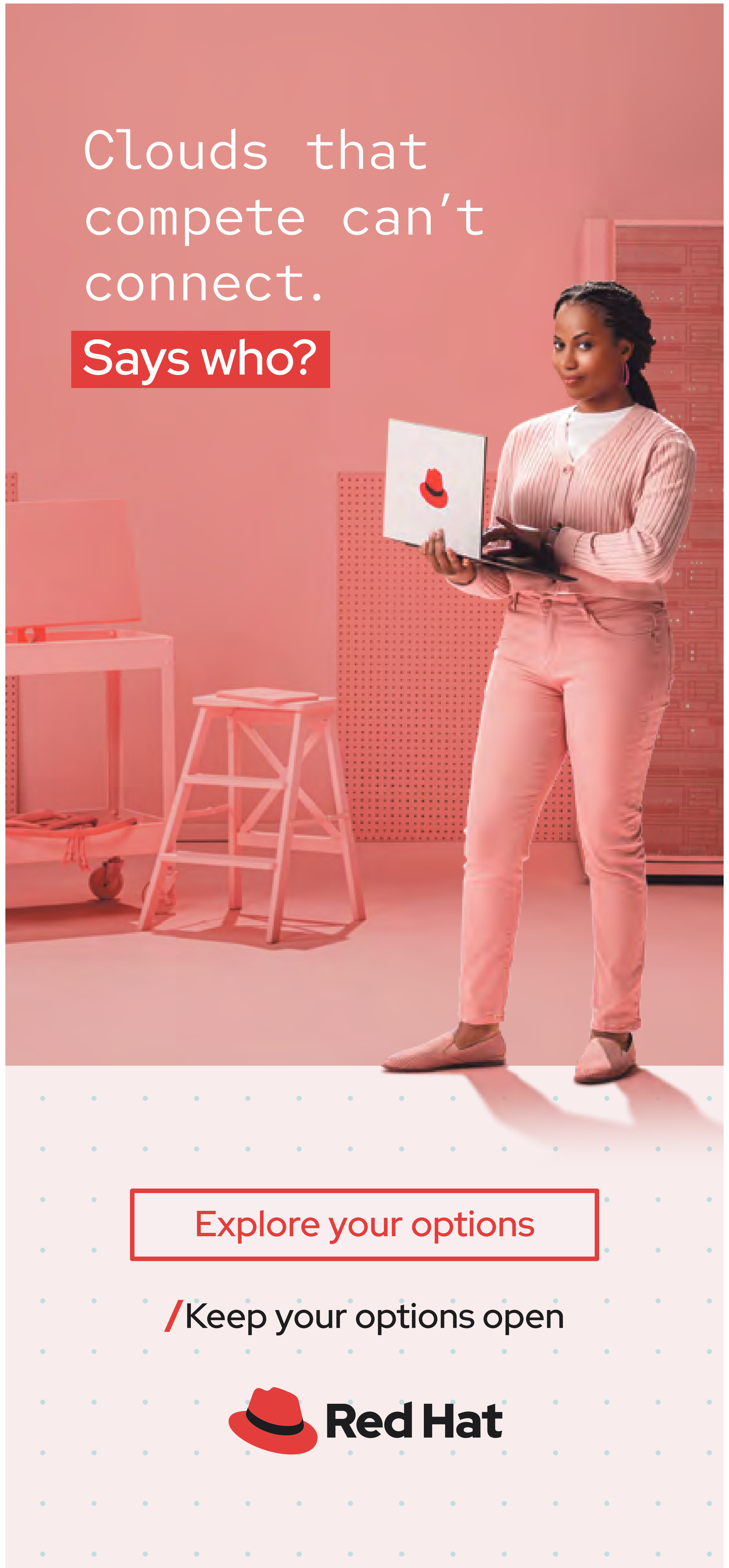
That experience is far from unique. Beyond conventional forms of attack, techniques such as 'doxxing' and 'swatting' – publishing someone's personal details online, and calling in a police Swat team to someone's address – are increasingly being turned against the good guys, as opposed to simply being used against familiar targets in the public and private sectors. The scale of the problem is such that the leaders of the US, UK, Australian, Canadian and New Zealand cybersecurity agencies issued a joint warning about the threat to managed service providers at last year's CyberUK conference.

In short, then, we're witnessing a campaign of aggression and intimidation which owes little to the era of the gentleman spy. In fact, this is where the Bond analogy is apt to break down entirely. The modern cybervillains aren't doing this because of some particular animus they bear towards cybersecurity providers. Rather, going after those firms protecting their real targets – in this case, businesses – is a shrewd and calculated strategy.

Fundamentally, it's a strategy that both cybersecurity providers and their clients will need to adapt to – and fast. To begin with, the cyber experts will need to get their house in order, or else they risk adding embarrassment to their more tangible losses when they themselves fall victim to an attack. In the short to medium term, that will mean investing in both technical upgrades and a thorough audit of existing processes and in-house skills, to ensure that all bases have been covered and gaps plugged.

And on the client side, most businesses would be well advised to pay far closer attention to their vetting process when selecting a cybersecurity provider. Hiring the flashiest firm that comes along and hoping for the best will no longer cut it. Instead, the C-suite needs to up its understanding of cybersecurity and start asking the right questions of their providers. After all, in an ever-evolving threat landscape, that may be the only quantum of solace up for grabs. ●

James Sutton
Deputy reports editor, Raconteur



Solving today's biggest IT challenges

From operational resilience and talent shortages to AI and sustainability, adopting an open source approach can help CTOs better address their most pressing IT issues. Red Hat EMEA chief technology officer **Julio Guijarro** discusses why an open source approach can help solve those challenges

As talent shortages and growing cybersecurity risks pile pressure on IT teams, innovative solutions that improve resilience and make businesses more sustainable are making a significant impact, transforming the way pain points are addressed.

Q What are the top IT concerns you're hearing in your conversations with CTOs?

A The first one is talent and getting access to the right people who have the right skills to understand current technology, but also how fast the technology is evolving. The second one that is on everybody's mind right now is artificial intelligence and machine learning and what impact it is going to have on their business and their workforce, as well as how to use AI as a competitive advantage. The third key issue is cybersecurity and security compliance, especially in Europe and the UK with the increased regulatory focus around operational resilience. And another topic that frequently comes up at the moment in conversations with CTOs is sustainability, but for different reasons. For some people, sustainability is about cost and trying to reduce energy consumption because of higher energy prices. For others, it is about reputation—customers increasingly expect companies to be more sustainable. And lastly, it is also about regulation and the need to meet CO2 emissions reduction targets.

> Until now, security has been an afterthought, but it's becoming more and more prominent

Q What are the biggest skills gaps that businesses face?

A Everybody's transitioning to a more digital world and so there is an explosion in the need for people with specific skills. Take cybersecurity – until now, security has been an afterthought, but it's becoming more and more prominent. We have seen hackers modifying open source packages like the Log4j hack, which became a vulnerability across the entire industry. We are also seeing problems at the hardware level. All of those require specific skills around security. And AI is exactly the same. The skills you need are not something traditional computer science graduates would have, a lot of it relates more to mathematics.

Q What can companies do to improve operational resilience?

A The way we see operational resilience is that there are five foundations. The first is defining infrastructure as code and automating everything. The second is understanding your software supply chain. Third is making sure that security and compliance are built into your development processes. Fourth is evolving your working practices so they are always fit for purpose. And fifth is having a culture of collaboration and openness. One way we are supporting the industry on operational resilience is through the Linux Foundation's FINOS (Foundation of Open Innovation in Financial Services) organisation. FINOS has just started a new group around operational resilience called the Common Cloud Controls project, which is aimed at driving security standards and governance for public cloud deployments in the financial services sector.

Q What can businesses do to succeed in areas such as the Internet of Things (IoT) and AI?

A A lot of the de-facto standards in IoT architecture have been driven by innovations and projects that were incubated inside the open source community. So again, it's about tapping into this innovation globally. When I talk to a lot of CTOs or executives, sometimes they have teams trying to replicate products that are already available in open source. So, do you really want to apply your best talent to solve things that have already been solved? Companies should be focusing on their core competency and what gives them a competitive advantage. If you think about AI – a few years ago, if you wanted to do AI, it was limited to big departments of universities and research labs. But today, thanks to open source, it is accessible to anyone. When ChatGPT 4 was launched, three or four weeks later there were about 20 or so large language models in open source that allowed anybody to start experimenting and using it commercially – not at the scale of ChatGPT 4, but good enough for the needs of many companies.

Q What is Red Hat doing to help businesses become more sustainable?

A We recently released a piece of open source software called Kepler that allows companies to measure the electricity consumption of each application they are using in their IT environment. Previously, you could understand the energy consumption of your data centre or rack or machine, but you didn't have the level of granularity to be able to understand the implication of individual applications. Kepler gives our customers the ability to measure something that they couldn't until now. Many were doing it before by way of approximation, and many are finding that what they thought was accurate is not. This enables companies to optimise their energy consumption, for instance only running a particular application at a certain time of day when green energy is available or understanding how making changes to applications would impact energy consumption. With new regulation for carbon emissions coming, this is something that is critical.

> Open source enables you to tap into the diverse and collective talent worldwide

Q Why is Red Hat focused on open source software?

A Open source is core to Red Hat – it is our core belief and mission. All of our employees believe in open source as a way of driving innovation, as a way of driving collaboration, and as a way of creating software. What we do is try to bring simplicity and stability to open source for our customers because open source evolves and changes so quickly. We take open source and make it enterprise-ready so that our customers don't have to deal with that fast speed change themselves. And then we reinvest and contribute back into the open source community and help other people innovate as well.

Q How does open source help drive innovation?

A Open source enables you to tap into the diverse and collective talent worldwide. For me, diversity is critical – everything from gender diversity to where people are from – and open source lowers the entry point for people to innovate. Talent is not exclusive to a number of computer scientists that had the luxury of going to university and getting a PhD. Today, there is so much talent out there, and open source allows you to access that. Those communities are driving innovation and breaking frontiers at a much faster pace than you could in a normal company or a small lab. So that's how open source can help drive innovation – we can tap into the talent in diverse global communities to create better software.

To find out more about how your organisation can use technology to accelerate its innovation and digital transformation journey, visit RedHat.com

Red Hat

How Red Hat's Kepler project is working to advance environmental efforts in IT

For many, the word sustainability evokes images of reusable water bottles, paper straws and household compost bins. For others, it conjures up images of 'reduce, reuse, recycle' posters and canvas tote bags at a local farmers' market.

What won't immediately spring to mind for the majority is data centres. But as sustainability becomes a cornerstone of government policies, enterprise initiatives and consumer trends, tech leaders have been hard at work building technologies dedicated to helping users monitor how their software usage might drive energy consumption.

In recent years, the rapid growth in workloads handled by data centres has resulted in greater energy usage. This has increased by between 10% and 30% per year and accounts for between 1% and 1.5% of global energy consumption, according to figures from the International Energy Agency.

That means that in order for businesses to meaningfully reduce their environmental impact, IT leaders take this into account. And they undertake deeper analysis of the efficiency of their equipment and the tools they use to evaluate the sustainability of their data centres.

Enter Kepler.

> In recent years, the rapid growth in workloads handled by data centres has resulted in greater energy usage

Better understanding IT energy consumption

Kepler, or Kubernetes-based Efficient Power Level Exporter, is a project founded by Red Hat's emerging technologies group, with early contributions from IBM Research and Intel. It is a community-driven, open-source project that captures power-use metrics across a wide range of platforms, focusing on reporting, reduction and regression so enterprises can better understand energy consumption.

Kepler uses proven cloud-native methodologies and technologies – such as extended Berkeley Packet Filter (eBPF), CPU performance counters and machine-learning models – to estimate power consumption by workloads and export them as metrics. These metrics are then used for scheduling, scaling, reporting and visualisation. This arms system administrators with information on the carbon footprint of their cloud-native workload.

The Kepler Model Server continually adjusts and fine tunes its pre-trained models using node data from Kepler's power-estimating agents. This is how Kepler adapts its calculations to best serve the user's unique systems and needs. With the knowledge gained from Kepler, enterprise decision-makers can better assess how to optimise energy consumption, address evolving sustainability needs and reach their organisation's goals.

The future with Kepler

Future innovations in sustainability develop faster with open source community collaboration and an upstream-first mindset. With this in mind, Red Hat is in the process of contributing Kepler to the Cloud Native Computing Foundation sandbox, where contributors explore how to integrate Kepler into their own use cases.

Kepler can enable a host of new innovations in the open-source community that allow service providers to better observe, analyse, optimise and document power consumption of cloud native applications, including:

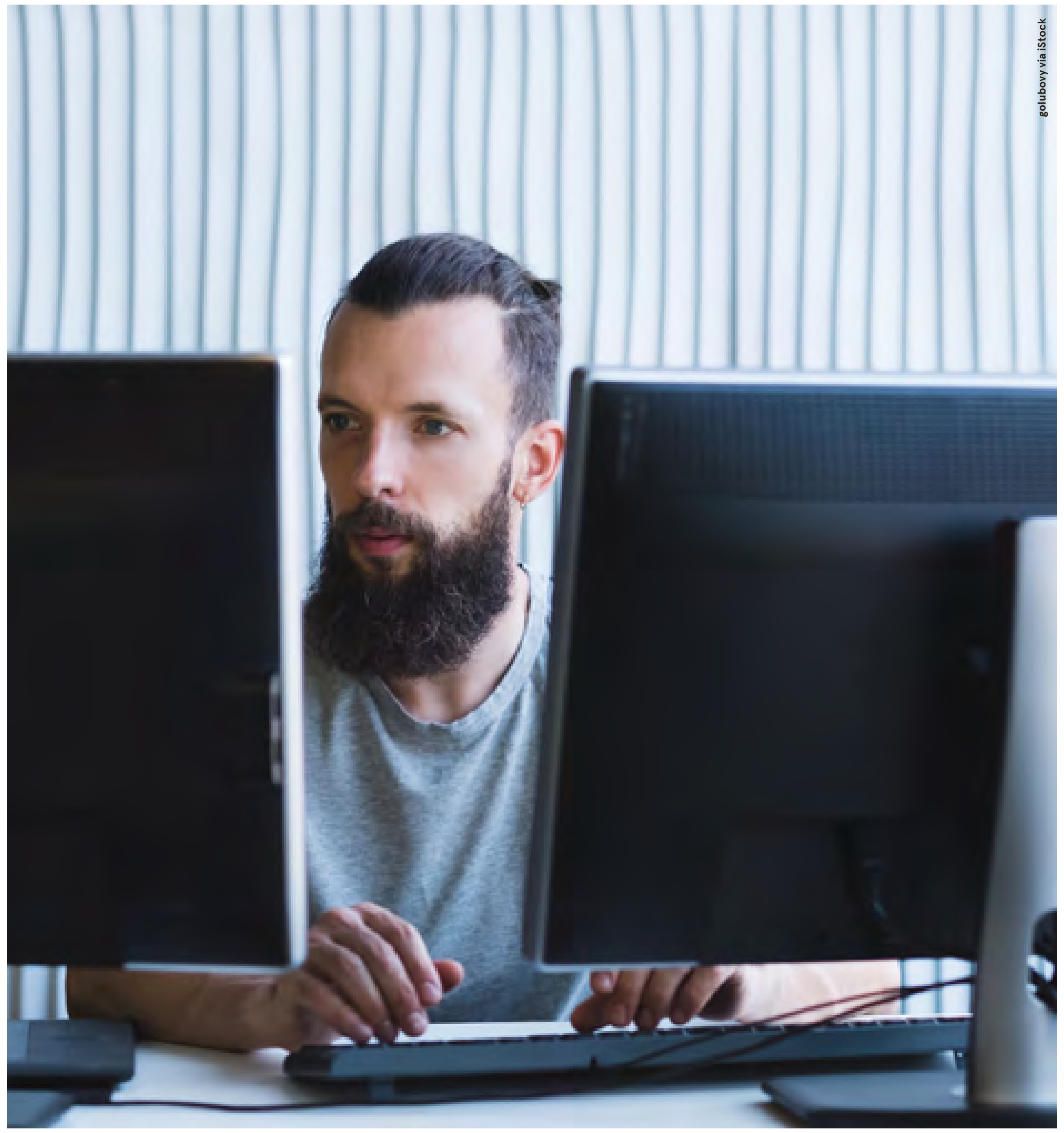
▶ **Power consumption reporting**
Kepler metrics are a time series. This means they can be used to build dashboards that present power consumption at a variety of levels, including containers, pods, namespaces or different compute nodes in the cluster.

▶ **Carbon footprint**
Kepler's energy consumption metrics can be coupled by the user with its data centre's power usage effectiveness (PUE) and electricity carbon intensity to calculate the estimated carbon footprint of the workload.

▶ **Power-aware workload scheduler and auto-scaling**
Kepler metrics can be used by a Kubernetes scheduler to place the upcoming workload on the compute node that is projected to improve performance per watts, ultimately reducing the cluster-level power consumption. Similarly, Kubernetes auto-scalers can use Kepler's power consumption metrics in auto-scaling algorithms to determine the resources needed to achieve better energy efficiency.

▶ **CI and CD pipelines**
Kepler can also be used in the software development lifecycle to help produce more sustainable software products. For example, Kepler can be deployed in continuous integration and continuous development (CI/CD) pipelines for software testing and release. Kepler's power consumption metrics can help developers measure, analyse and optimise software stacks.

Get involved with the Kepler project via GitHub and learn more on Red Hat's Emerging Technologies blog.



golubovy via iStock

STRATEGY

Double the fun

Some firms have decided to merge the chief product and chief technology officers. While the combined role could lead to greater efficiency, CPTOs will likely face a difficult balancing act

Chris Stokel-Walker

Simone Basso first came across the role of chief product and technical officer (CPTO) at his previous employer, Just Eat, six or seven years ago. One chief officer left the company, another semi-retired and the company subsequently decided to replace them with one person to do both jobs.

Basso thought the decision was inspired, particularly as tech companies began offering tech as the product in the first place. It sparked an interest in combining product and technical roles that Basso continues today as CPTO of Italian tech company WeRoad.

WeRoad is far from the only company to take the leap in combining two roles that once required different skills. Epicor recently said it is combining the posts of chief product officer and chief technology officer, joining a long list of companies that are at least having the conversation about merging the jobs – if not outright adopting it. Many are in the fast-moving startup sector, but increasing numbers are from long-established businesses looking for efficiencies in their operations.

The reasons for adopting a CPTO model are multifarious. Tech now underlies whole business strategies, so it makes sense to squarely align products and services with the technology that drives the wider business goals. Combining the roles also facilitates faster decision-making concerning product development and deployment.

Sarat Pediredla is CEO of global tech consultancy Hedgehog Lab, one of many companies to combine tech and product roles into one CPTO. According to him, unifying these roles can streamline decision-making, simplify communication and foster an integrated approach to tech and product strategy. "It eliminates the 'middleman', which enables faster decisions to be made and it leads to more efficient outcomes," he says. But the change has, he admits, caused some issues. "It presents challenges such as potential conflicts of interest and the risk of diluting focus," he says. CPOs are usually seeking to meet market demands, rapidly innovating and occasionally cutting technical corners to get a product out to market. CTOs, on the other hand, are more often focused on maintaining the long-term tech stack within a company, and so will frequently advocate to go slower. "Combining these roles may lead to neither technically sound nor product-optimised compromises," he warns.

Despite those potential pitfalls, Hedgehog Lab decided to go ahead with combining the roles – to good success. "Is it sensible? It likely depends on the specific context of the company. It might make sense for startups or smaller businesses, where agility and fast decision-making are essential. It certainly works for us," says Pediredla. But he observes that others may decide differently: "Keeping the roles separate in larger, more complex organisations could allow for the necessary checks and balances."

Basso believes that combining the roles is a net positive, where it's possible. Having one person overseeing both aspects of a business frees up the CEO because they are no longer required to be the arbiter between competing interests and competing teams. "It makes decision-making much faster because there are fewer points of debate and conflict," he says. "You just want to have one voice at the executive table."

> Unifying these roles can streamline decision-making, simplify communication and foster a more integrated approach to tech and product strategy

But it isn't all plain sailing. A CPTO needs skills that will benefit both teams. He finds that many CPTOs are firmly from one background or the other and biased towards one team. That can present difficulties when combined with the personal people-management skills that are required at an executive level. "It's easier to go from an engineering background to become CPTO," he says. "You can learn the products if you have a bit of business sense."

It's not just the company and how it works that must be carefully weighed up before deciding whether to combine these roles. Deciding who will fill the shoes of the combined CPTO position is also important. The demands on an individual in the CPO and CTO roles are different and being able to thread the needle between them is vital.

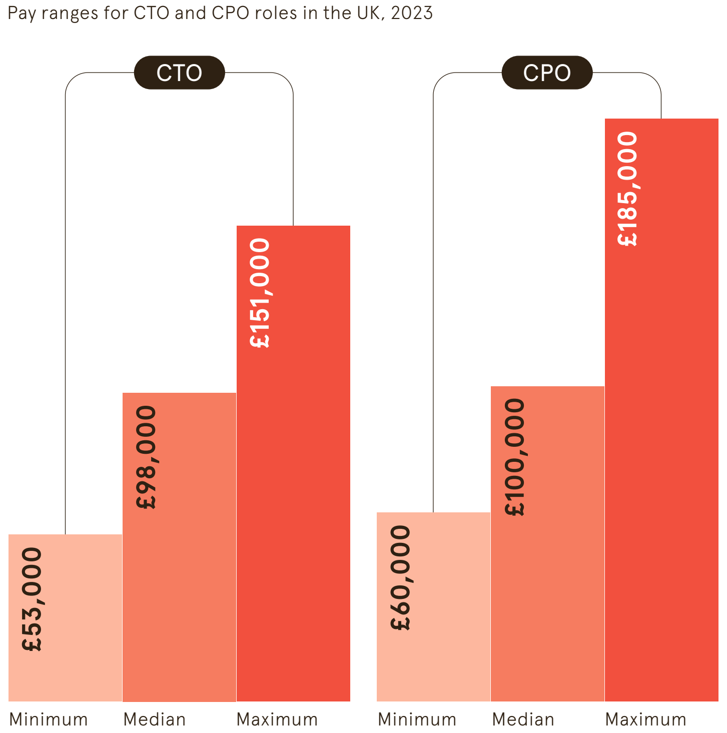
"A lot boils down to being able to balance these divergent interests," says Pediredla. "Either way, the model must be carefully considered and tailored to the company's existing and future needs and challenges." There's an element of the CTO speaking truth to the CPO's power, says Ratcliffe, which can be difficult if it's just one person. "You have a tension between the technology and what's working for the product," he adds.

Picking candidates is also less preferable than the right person for the job making themselves known naturally through the course of doing business. Steven Ratcliffe's journey to becoming CPTO at tech company Eque2 began in the pub over Friday night drinks. There, his company's technical team and product teams would often disappear into their own corners of the tavern to drink with their respective teams – and would barely intermingle. "I was one of the few people who enjoyed both sides of that conversation," he says. That helped him to be accepted as a neutral arbiter over both teams when he migrated into the CPTO role.

Managing people can be problematic for new CPTOs. "You need to be able to read a much wider spectrum of people and ideas," says Basso. For Ratcliffe, avoiding favouritism is vital to his ongoing success. Keeping tension and healthy competition between teams can drive the businesses but, he says, being a CPTO is a lot like being a parent: "You don't favour one over the other." ●

COMBINING CTO AND CPO ROLES MAY MAKE GOOD FINANCIAL SENSE FOR CASH-STRAPPED BUSINESSES

Pay ranges for CTO and CPO roles in the UK, 2023



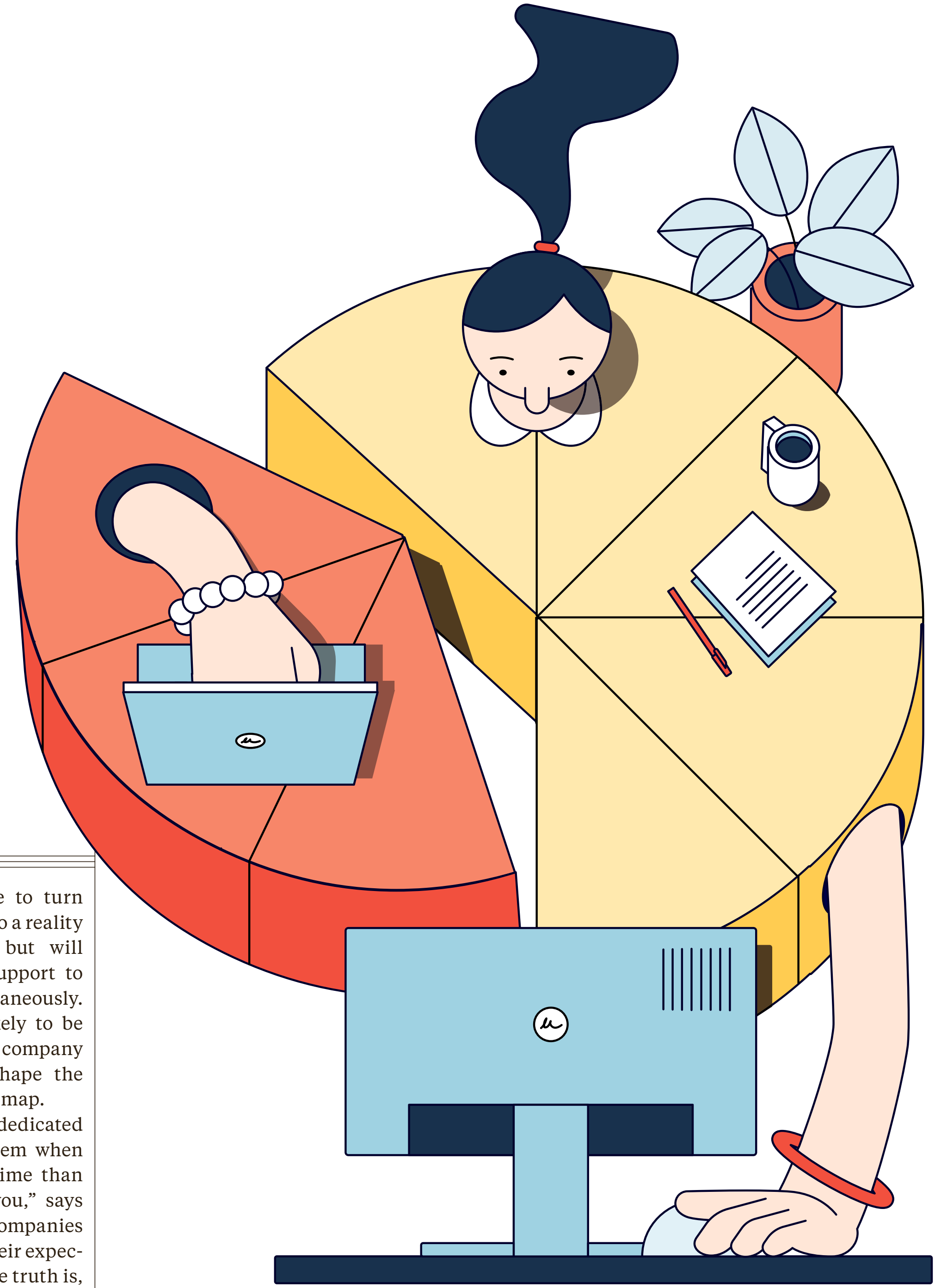
Payscale, 2023

LEADERSHIP

Should you hire a fractional CTO?

A chief technology officer who works a fraction of the time for a fraction of the cost can be impactful. But there are things to consider

Rich McEachran



Hiring a full-time CTO in the early stages of an organisation's growth can be an expensive overhead. But businesses still need a guiding hand to build the right technology at the right time and in the right way to ensure that their company can meet future growth objectives. This is where a fractional chief technology officer (CTO) can come in.

A fractional CTO is a technology chief who works a fraction of the time, often on a fraction of the organisation's projects as opposed to across a whole business, and for a fraction of the cost.

The role is perfect for startups and growth companies that want to focus their capital on scaling the business. But it could also be attractive for companies that don't need full-time technical support but do need help creating technical solutions, such as companies that are planning a digital transformation of legacy systems and need an external voice to guide their strategy.

But while hiring a fractional CTO can help to minimise risk and reduce technical debt, it won't automatically be the right strategic move for every company.

Generally when companies recruit for the CTO position, they're looking for a candidate who can jump right in and won't need a lot of time to get up to speed. A fractional CTO typically has a wealth of experience supporting companies in different industries and at various stages of their growth journey. In effect, they specialise in getting straight down to business, which is perfect for companies needing project-based support, or guidance in developing or implementing a digital strategy.

"These experienced fractional CTOs are effectively consultants. They're quick to onboard and can start to add value quickly," says Jeff Watkins, chief product and technology officer at mobile and app development firm xDesign.

Robin Beattie, managing director at Spinks, the startup and scale-up recruiting arm of digital services consultancy Nash Squared, adds: "Fractional CTOs themselves love it because they get variety and exposure to lots of different technology and projects."

The downside, though, is that companies won't be getting someone who can stick around. A fractional CTO can come in and use their practical knowledge to turn the vision for a product into a reality within several months, but will often provide strategic support to several companies simultaneously. This means they're unlikely to be able to devote to any one company the time necessary to shape the long-term technology roadmap.

"You're not getting a dedicated CTO. This can be a problem when you need more of their time than they can afford to give you," says Watkins, adding that companies need to be realistic with their expectations. He continues: "The truth is, their attention is always going to be split between their engagements. That means they'll probably be less invested and culturally integrated into your business."

Nevertheless, a key advantage of a highly experienced fractional CTO is that, more often than not, they will have a strong network that they can rely on for support and expertise. This can be particularly advantageous if a company needs to access certain resources and connect with potential partners and vendors further down the line.

> Fractional CTOs are effectively consultants, meaning they're quick to onboard and get up to speed

While strong communication and people skills are essential qualities for any business leader, they are especially important for a fractional leader, who will need to join a company and inspire teams from the outset to achieve what they've been brought in to do in the short amount of time they have.

"A fractional CTO role isn't about subject-matter expertise; it's about digital-business leadership," says Jaco Vermeulen, CTO of BML Digital, who has held portfolio roles at Boots, Park Holidays and the Post Office. "They need to be able to demystify technology for the company. That means no tech speak, buzzwords or IT acronyms."

Yet, while a fractional CTO may be able to use their soft skills to ensure everyone is aligned with the company's vision and that goals are being met – while also addressing any teething issues with new technology teams – the nature of a fractional role could leave them feeling like a lone wolf. Employers would be wise to avoid letting that happen.

"There needs to be some intrinsic motivation for a fractional CTO to act in the same manner as a full-time equivalent," says Evgeny Smirnov, co-founder and CEO of Denovo, a consultancy that, among other things, runs a fractional CTO matchmaking service for startups.

The incentives don't need to be the same as those offered to full-time hires, such as equity or stock options. But something as simple as the CEO granting the fractional CTO a comparable level of autonomy and acknowledging the work they're putting in can do the trick.

As motivated as a fractional CTO might be, a company will need to take the plunge and hire a full-time CTO. There's no right or wrong moment to do this and it will be different for every business and depend on the level of involvement required, says Watkins. Growing engineering teams, for instance, may need a more hands-on management style that a fractional CTO can't provide.

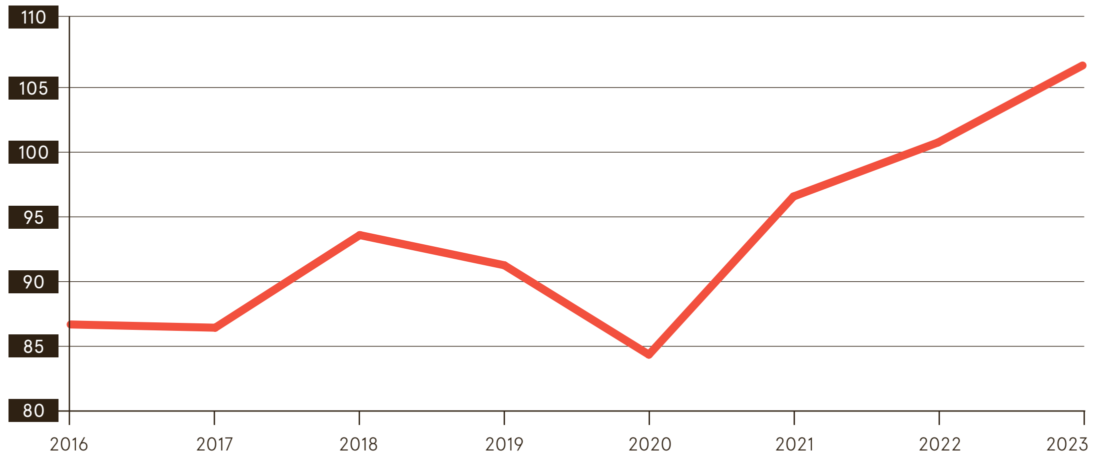
"As a rule, it's when the business starts to scale and the founder can't manage it alone," says Beattie.

On whether and when to seek a full-time tech chief, Watkins concludes: "It's about your size, your tech complexity, what level of commitment and presence you expect – and for how long." ●

BRITISH FIRMS ALREADY SPEND A LOT ON TECHNOLOGY CONSULTANTS' SERVICES

Statista, 2023

UK businesses' average annual spend on technology consultants per employee, £

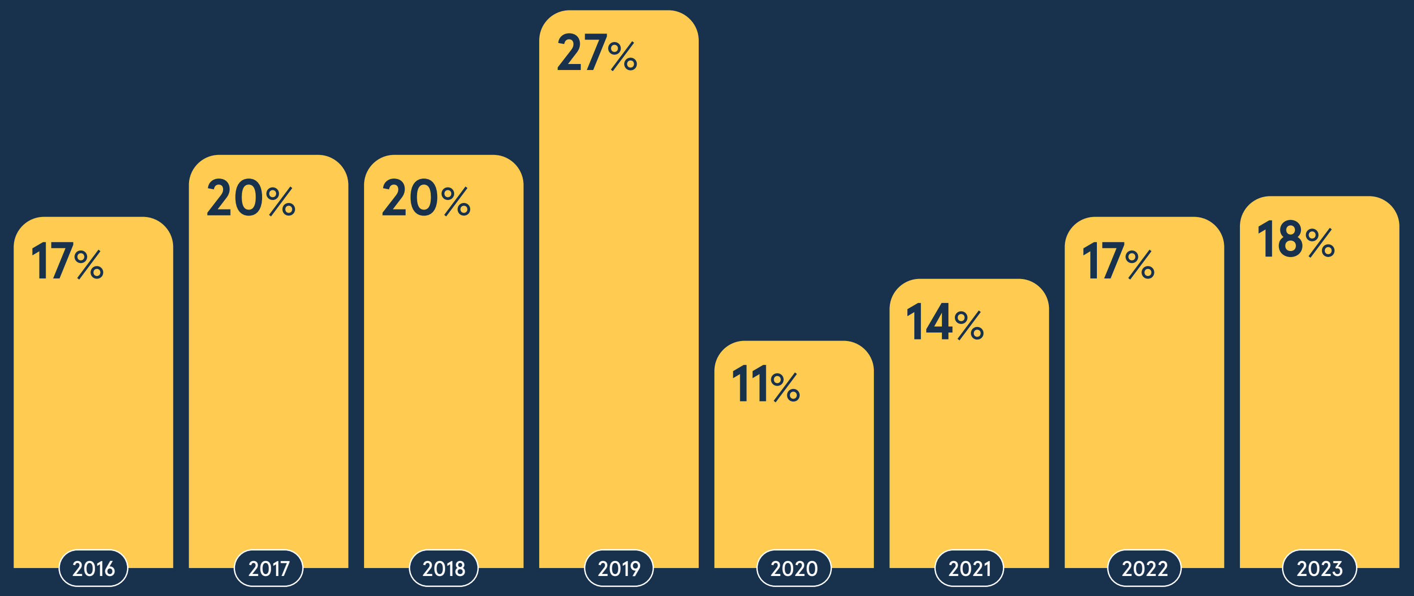


UK PLC'S CYBER WEAKNESSES

By definition, the fundamentals are important in cybersecurity, and they make an outsized difference to both an organisation's odds of suffering a cyber breach and also how well that organisation will be able to respond. But according to a survey by the Department for Science, Innovation and Technology, UK businesses are still falling short when it comes to defending themselves. So, where should they be upping their game?

COMMITMENT TO STAFF CYBERSECURITY TRAINING COMES AND GOES

Share of UK businesses which have held training sessions on cybersecurity in the past 12 months



3 in 10 ●●●○○○○○○○

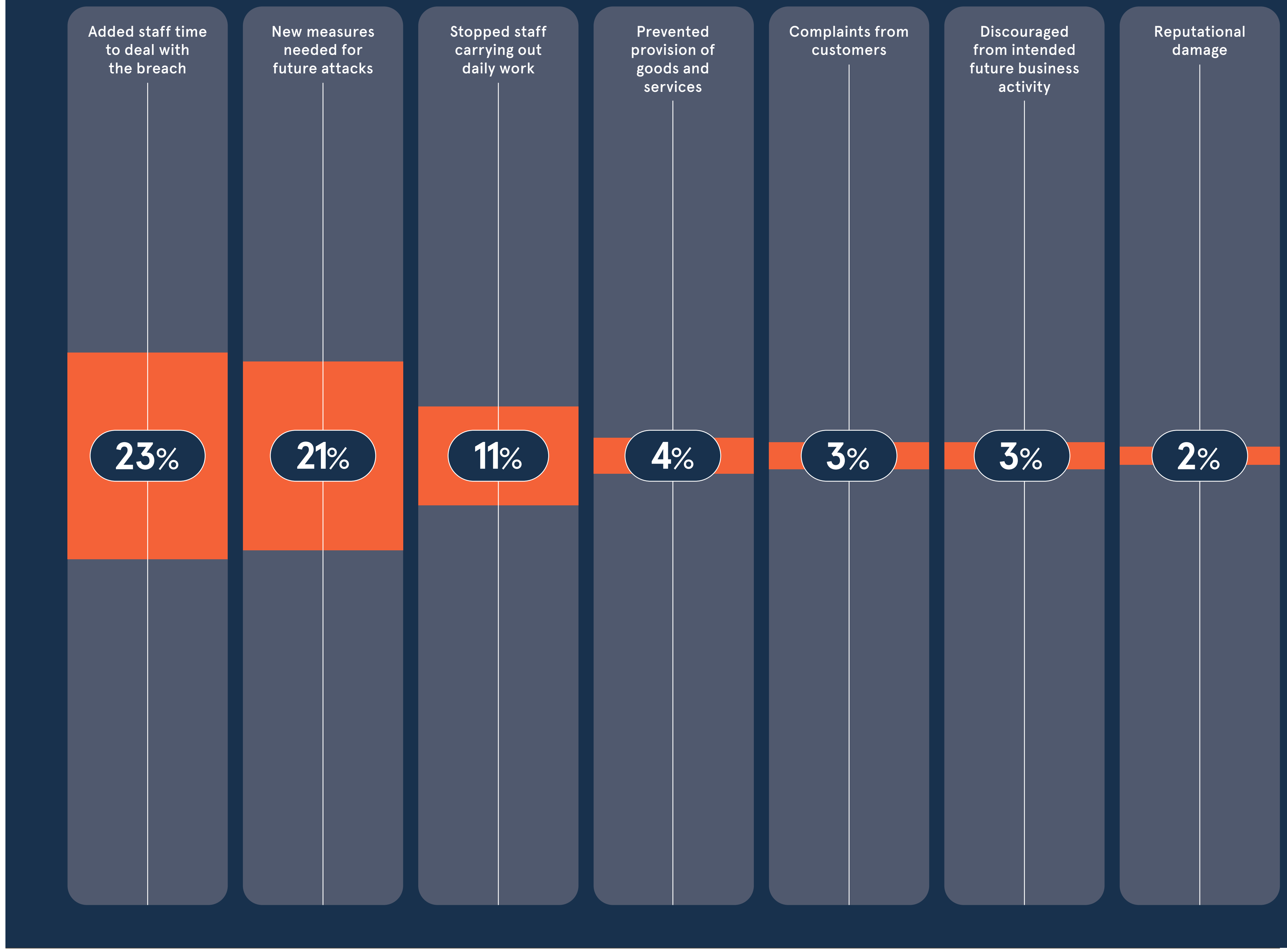
firms have a board member with explicit responsibility for cybersecurity

2.39million instances of cyber crime affected UK businesses over the past 12 months

49% of UK businesses actively sought external information or guidance on cybersecurity in the past year

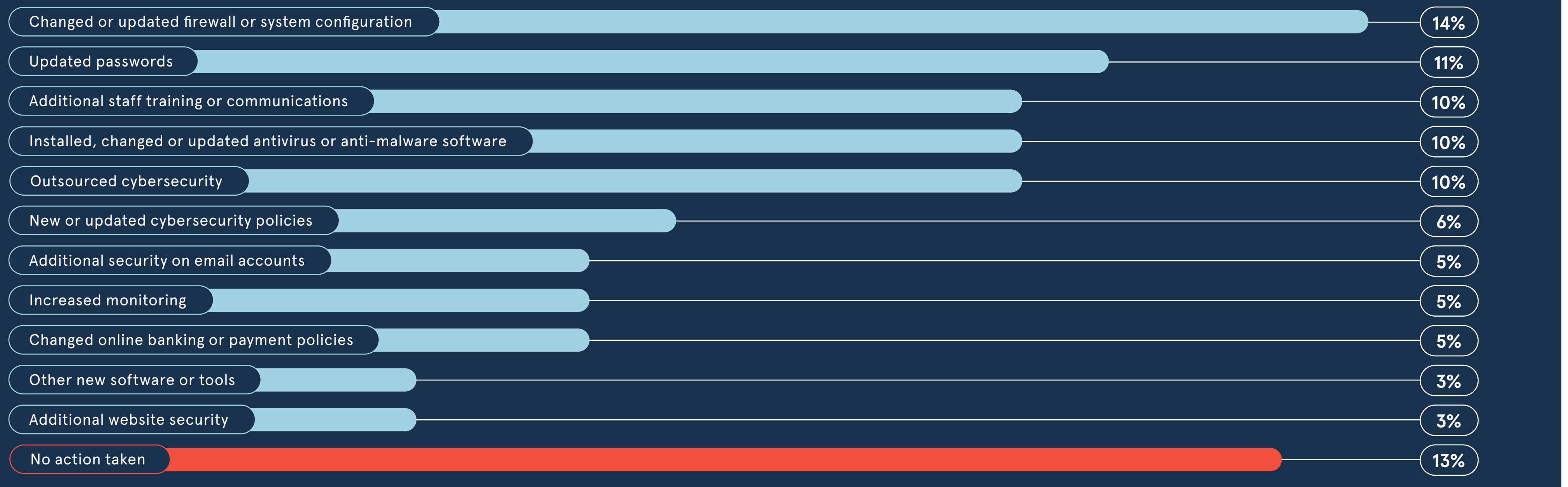
WEAK CYBER DEFENCES ARE HURTING UK FIRMS IN MANY DIFFERENT WAYS

Share of UK businesses reporting the following non-material impacts from a cyber incident in the past 12 months



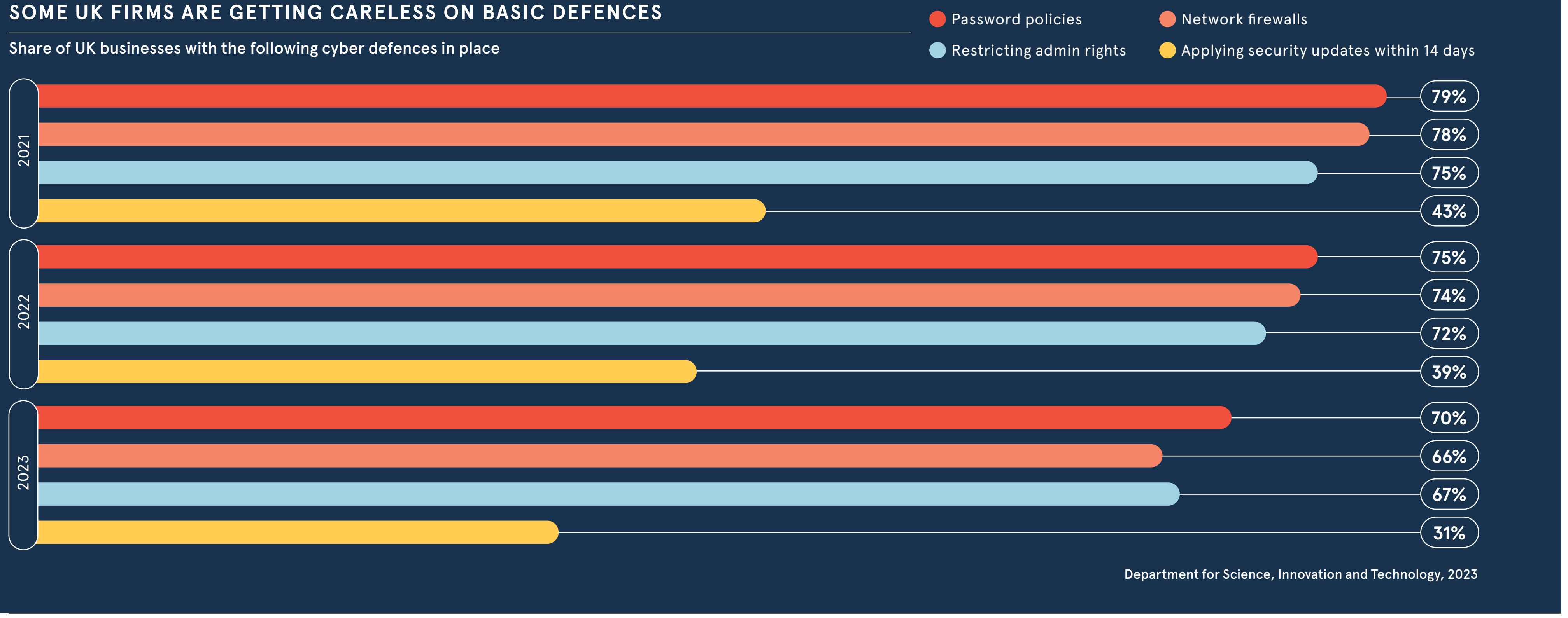
TAKING NO ACTION IN THE EVENT OF A CYBER INCIDENT IS STILL A COMMON RESPONSE

Share of UK businesses that have done any of the following since their most disruptive breach of the past 12 months



SOME UK FIRMS ARE GETTING CARELESS ON BASIC DEFENCES

Share of UK businesses with the following cyber defences in place



Department for Science, Innovation and Technology, 2023

TALENT

5 interview questions to ask cybersecurity talent

It's difficult to find the right candidates for cybersecurity roles at the moment. So, what kinds of questions should you be asking to make sure someone's up to the job?

Christine Horton

Organisations are constantly searching for new ways to recruit and retain talent. But business leaders hiring for cybersecurity roles face a particularly difficult balancing act.

For instance, not only must they ensure their interviews are rigorous enough – candidates need to know their stuff and be able to act fast, think critically and handle the many pressures of the job – but they must simultaneously make sure they're not discouraging potential candidates who perhaps have no direct experience in cybersecurity.

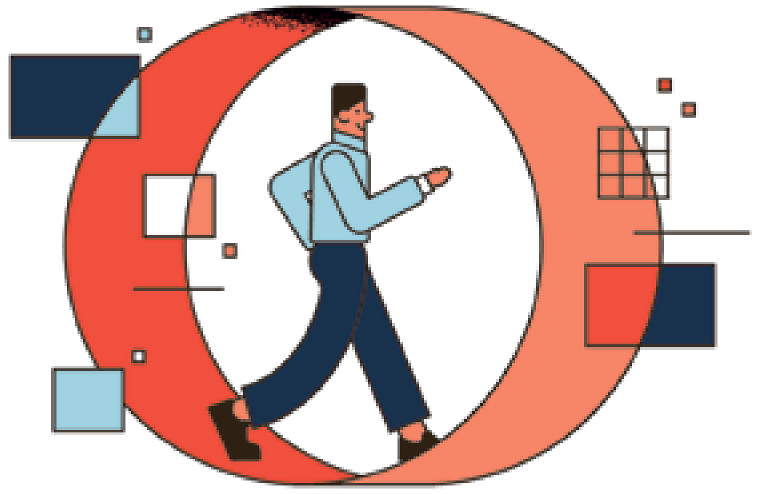
So, what sort of questions should they be asking to strike the right balance? Here are five 'go-to' approaches suggested by senior business leaders with experience of hiring for cybersecurity roles.

Explain something security-related – and why it's important – to a layman

In an average business, less than 1% of employees are focused on cybersecurity. That means it's important that the language which security teams use is easily understood by the majority of colleagues.

Nicholls suggests asking a candidate to explain something security-related, such as secure email, to a non-technical person, as it's a great way to see how they communicate.

"My answer would be that non-secure email is like sending a postcard – everyone can read what's on the postcard on its journey to the recipient. Secure email is like putting that postcard in an envelope to protect the message while it's en route to the recipient."



How would you keep the business running while dealing with a problem?

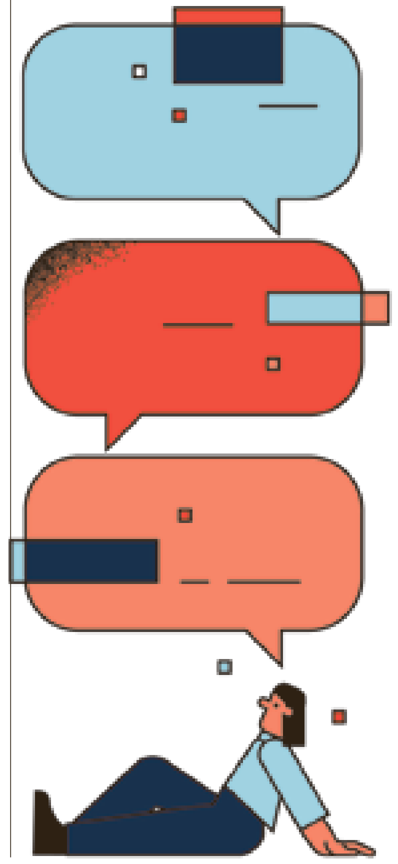
Mark Nicholls is head of information security, risk and compliance at Ramsay Health Care. His interview questions are based on how the candidate approaches problems in an environment where security is not the main focus of the business.

"For example, my organisation is an operator of private hospitals," he says. "So everything I do relates back to providing that service. I can't just turn off a heart monitor because it could be vulnerable to a cyber attack; the patient always has to come first."

As such, he wants to distinguish candidates who only know the cyber theory from those with real-world experience of protecting a business. For example, he may ask: "The main internal customer database is on the public-facing network and has a critical vulnerability that needs immediate patching. To patch this server requires 2 hours of downtime, but the business can only give you 30 minutes. What do you do?"

"Cyber professionals who haven't worked in a real business just apply cyber theory: take the server down till the vulnerabilities are fixed. But that approach would not, of course, be good for either the business or the security team.

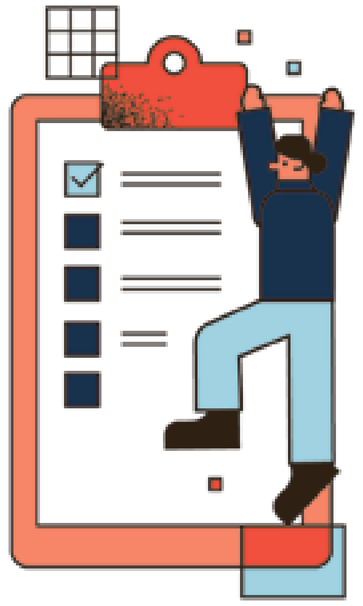
"I'm looking for those who seek out ways to keep the business running while mitigating risk. Take the question apart: it's an internal database, so why is it on the public network? In 30 minutes, we can reconfigure the network adapter, so the server is internal only. The vulnerability might only be exploitable if the server is accessible externally, so by moving it internally we can reduce the risk."



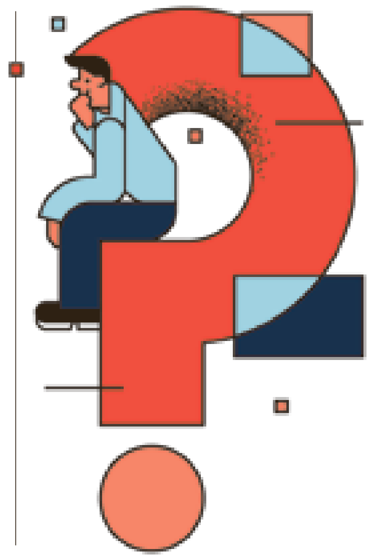
What non-technical skills do you bring to the table?

As head of SecOps on a huge greenfield technology project for a major UK retailer, Lianne Potter has plenty of experience in building a security team from scratch. Her emphasis isn't so much on candidates demonstrating their cybersecurity knowledge. Instead, she prefers to look for their potential as a team member.

"When I ask particularly technical questions, I emphasise to the candidate, 'These are not to catch you out.' It's for me to understand them, because technical skills are not the be-all and end-all. Even with technical roles, it's about 'What other things can you bring to the table?' It's just so I know what level you're at so I can give you the opportunities to develop in those areas."



Potter says this goes a long way to ease the conversation. "Speaking from my own experience, you always aim for perfection when you're doing interviews. And that's just not possible. I'm not looking for perfection; I'm just looking for creativity in your answers. And, actually, the ability to be humbled by what you don't know, because I think that's such a valuable skill."



What would you do if you don't know a solution?

Potter says she always includes a technical question that has a vague or ambiguous answer.

"The answer I'm looking for is: 'I would Google it.' I need to know that people won't just sit there panicking and not ask for help or do some research. You'd be surprised how many people come through this industry who don't think that Googling is an option. Instead, they just sit and stew on that problem.

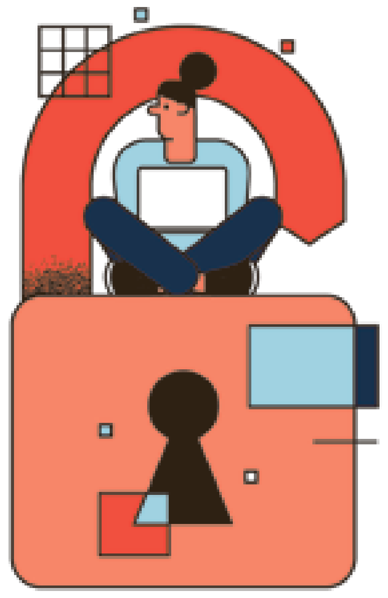
"But the answer should be: 'I would ask for help.' And that's what I want to see demonstrated in the answer to that question."

How would you define our security perimeter?

There is, of course, still a need to ask questions that probe the candidate's knowledge – not just of the specific technology in question, but of the wider cybersecurity landscape.

Aurelia von Pentz is principal engineer and head of advanced projects at HSBC. She explains that she asks candidates what they would define as their security perimeter, and then how they would go about protecting it.

"This is a more open question provoking a discussion, and mainly aims to see if the candidate understands that in a distributed world with more and more software-as-a-service, cloud infrastructure and third-party suppliers, your perimeter doesn't end at your local network border anymore," she says.



"Monitor global security bulletins; have effective third-party risk assessments; and have the ability to act swiftly if a supplier is compromised are all vital. At the same time, these connections don't allow you to draw a clear border anymore, even within your network, and will force you to adopt increasingly defensive depth and zero-trust strategies for effective protection." ●

Commercial feature

Net gains: why cybersecurity is a team sport

The cost of getting things wrong has never been higher – meaning consolidation and reassurance across an entire company is vital

Cybersecurity has long been a matter of high importance for organisations. But a perfect storm of events has pushed the fear of falling foul of a cyber attack higher up the risk register.

Coupled with an overall rise in cybercrime, changes to the way people work mean the risk of becoming a victim is at an all-time high – and with it, the expense when something goes wrong. Research from IBM puts the global average cost of a data breach in 2023 at $4.45m (£3.57m), a 15% rise over the past three years. The ramifications are immense when hackers get past an organisation's line of defence.

And increasingly, they can. "Hybrid work has changed everything, from the way employees communicate to the infrastructure needed to maintain organisational efficiency," says Andre Schindler, general manager of EMEA and vice-president of strategic partnerships at NinjaOne. He points to a common problem among cybersecurity teams. "Employees now access company data from different devices and locations. That makes it more challenging to secure sensitive information," he notes.

It's not a case of protecting pre-checked and company-issued devices and their access to proprietary information. "It's personal laptops and personal mobile devices as well," says Schindler. "These devices aren't protected by a company network perimeter, which makes endpoints more vulnerable and requires them to be more secure or pose a risk to company data," he says.

In a hostile environment where attackers are constantly closing in on organisations' IT systems, securing every touchpoint can be a tricky task to tackle. The tried-and-tested method of throwing up a perimeter around on-premises infrastructure and networks no longer cuts it. "With the shift to remote work and cloud-based services, that traditional security perimeter has dissolved," says Schindler. "In many cases, it's up to IT teams to solve these new problems."

As the head of IT teams, chief information security officers (CISOs) have eyes on them from every corner of the boardroom. According to Deloitte, 70% of C-level executives say cyber is now regularly on their board's agenda, either monthly or quarterly. There has been a significant emphasis put on warding off such attacks, with device security rapidly becoming a strategic imperative for companies.

> “ Hybrid work has changed everything, from the way employees communicate to the infrastructure needed to maintain organisational efficiency

For good reason: ransomware attacks grew by 41% in 2022, according to Schindler, and identification and remediation for ransomware breaches took 49 days longer than the average cybersecurity breach. And with 2,200 incidents happening on an average day to businesses around the world, businesses need to tackle the issue.

"Executives and boards of directors now recognise that cyber threats are a significant business risk," says Schindler. "This has led to increased investments in cybersecurity." Remediating risk is a multi-part problem, he points out. One part is improving awareness among staff, with training, phishing tests and other tests for employees to inform them how attacks happen. That results in shared responsibility, reframing security as a core business value. "It's no longer the cybersecurity team's job to secure critical business data; it's everyone's," says Schindler.

But it's not just about informing staff of the risks involved and ensuring they have the tools to avoid issues – and tackle them if and when they crop up. Organisations need to refigure their endpoint security to accommodate the changed way of working – broadening out the perimeter that once ended at office walls to the work-from-home setups that are normal today. "Ensuring deep visibility into all endpoints within the network allows businesses to promptly detect and respond to potential threats," says Schindler.

Better visibility can highlight potential problems before they become problems, such as a lack of patching software vulnerabilities. Patching – applying updates that address security vulnerabilities within a program or product – is one of the most critical security tasks IT teams perform. It is also time-consuming, taking an average of 5.1 hours per endpoint per month to keep devices secure, according to NinjaOne's recent findings. "I'd say more than half of all ransomware breaches can be mitigated through fast and effective patching," says Schindler.

He also recommends stripping back unnecessary services from endpoints and implementing stronger controls on the devices that have access to them, so that if the worst were to happen to a home worker and hackers accessed their device, the issue can be isolated there and not spread.

Rigorous and regular backups are also vital so that data can quickly be restored in the event of a breach. "These measures collectively strengthen an organisation's cybersecurity defences and reduce vulnerabilities in an ever-evolving threat landscape," says Schindler.

Taken collectively, that may seem a significant ask when budgets, time and staffing are all constrained. But there are ways to ensure the business's IT remains secure and manageable. "IT teams can leverage automation as a powerful system to mitigate vulnerabilities and enhance cybersecurity," says Schindler. "Automating patch-scanning, approval and reporting can yield substantial benefits while allowing IT teams to focus on strategic initiatives that drive value for the business."

It's also important that organisations consolidate their IT management workflows to turn this from a theoretical benefit into a realised one. "By streamlining IT management, organisations can implement consistent and robust security measures across their entire IT infrastructure, again reducing vulnerabilities and enhancing our overall cybersecurity posture," says Schindler. It also allows companies to do more with their existing IT resources, making their business more effective – and more efficient.

Automation is something that NinjaOne has plenty of expertise in. The company oversees the IT security of some of the world's largest companies, from Nvidia to Nissan and Hello Fresh to Konica Minolta. Its tools analyse more than 5 million endpoints across 83 countries. "Solutions like NinjaOne offer user-friendly tools and powerful cross-platform automation that significantly minimise administrative burden," says Schindler. "This means that IT teams become more efficient and effective, freeing up valuable time and resources that can be redirected toward strategic initiatives that drive innovation and business."

Between CISOs adopting a more strategic stance, IT staff keeping endpoints secure, and employees across the wider business taking on greater responsibility, it seems collaboration is the name of the game.

GLOBAL THREATS

Why Taiwan is on the front line in the cyber wars

State-sponsored cyber attacks from China have become far more common in recent years, but it's not just Taiwan in the firing line. The implications for global semiconductor supplies could be critical

Seven Standen

An island population cut off from the world when its communication lines are suddenly severed sounds like the plot of a dystopian thriller. But that was the reality for 14,000 people in the East China Sea this February.

The Matsu islands are part of Taiwan, but when their internet access suddenly disappeared earlier this year, Taipei's backup system could only restore 5% of the bandwidth the cables had provided.

Amid rising tensions with China, this may well be a sign of things to come. Concerns have also been raised about what might happen if Taiwan's 14 remaining international sea cables were unexpectedly put out of action.

And that's not the only threat. Interrupted access to the internet is bad enough, of course, but cyber attacks can bring far greater disruption. A recent Fortinet study reports that Taiwan is the target of 15,000 cyber attacks every second, with manufacturing, IT and logistics among the most heavily affected industries. Given that 90% of the world's advanced microchips, as used in smartphones and data centres, are made in Taiwan, successful cyber attacks could result in large-scale, global shortages. That could leave businesses worldwide facing the same kind of reality as the people of Matsu did; missing vital communication links.

The situation is rapidly worsening too. In the first half of this year, the number of daily cyber attacks on Taiwan was up 80% on the same period in 2022. Its big industrial players are routinely targeted with malware that includes malicious phishing campaigns and harmful URLs. These methods can result in a company's data being taken and held for ransom.

Paul Bantick is global head of cyber risks at FTSE 100 insurer Beazley. He comments that the attacks are escalating not just because of Chinese hostility but also because of broader trends: "Cybercrime, particularly ransomware, is a high-growth industry and a lucrative business, and the barriers to entry are getting lower."

This has concerning implications for businesses worldwide.

Richard Meeus, EMEA director of security technology and strategy at Akamai, explains that these attacks on Taiwan's manufacturers are "intended to disrupt supply chains", which is used as leverage by hackers. "Attacks can disrupt production processes, leading to costly downtime and delays, resulting in significant financial losses for organisations," he says.

The disruption of semiconductor supply chains is by far the most serious global threat stemming from Taiwan's predicament, given that the chips are used in such a wide variety of consumer, commercial and healthcare products.

Bindiya Vakil is CEO of supply chain risk management specialist Resilinc. She predicts that the cyber attacks on Taiwan could result in "shortages [that] disrupt the supply of virtually everything we use daily".

The timing couldn't be worse, either. Many businesses are still recovering from the global chip shortage of 2020, created by disrupted supply chains and the increased demand for technology during the Covid-19 pandemic.

James Williams, head of TMT & Legal at IT security provider NCC Group, says that the pandemic highlighted the far-reaching consequences of supply chain disturbances. Manufacturers were forced to temporarily halt or permanently shut down production. As a result, car makers alone lost out on $61bn (£48bn) of sales in 2021.

Multiple industries, including makers of vehicles and consumer electronics, continue to face challenges from that previous shortage of semiconductors.

Further delays and slowdowns could result in the collapse of struggling companies. Although semiconductor supply chains appear to be stabilising, Vakil expects shortages to continue into 2024, so businesses should plan for delays.

As a result, Vakil advises businesses to insulate themselves from the cyber attacks on Taiwan by "taking appropriate steps to mitigate potential risks". That might mean "diversifying their suppliers, investing in AI-driven solutions, or implementing planning techniques". She also highlights the importance of using advanced monitoring techniques to create greater cyber resilience in the supply chain.

Diversifying supply chains might be more complicated, but it will help to build resilience. For instance, Nvidia, the world's largest semiconductor company, was targeted by ransomware in 2022, resulting in the theft of sensitive hardware and software data. Businesses that are reliant on Nvidia would have faced greater disruption than those with diversified supply chains.

Bantick points out that companies with links to Taiwan need to install security patches quickly, limit users' permissions, have secure backups and, crucially, make sure that they have well-planned disaster recovery plans in place. After all, he points out, it's important to implement cybersecurity at all business levels, as it's usually the weakest link that is targeted; often manufacturers, like those in Taiwan.

Of course, Taiwan has been working extremely hard to improve its cybersecurity at a national level, with President Tsai Ing-wen even setting up a cybersecurity research institute. The risk of cyber attacks, however, has prompted some leading technology firms to relocate their manufacturing operations.

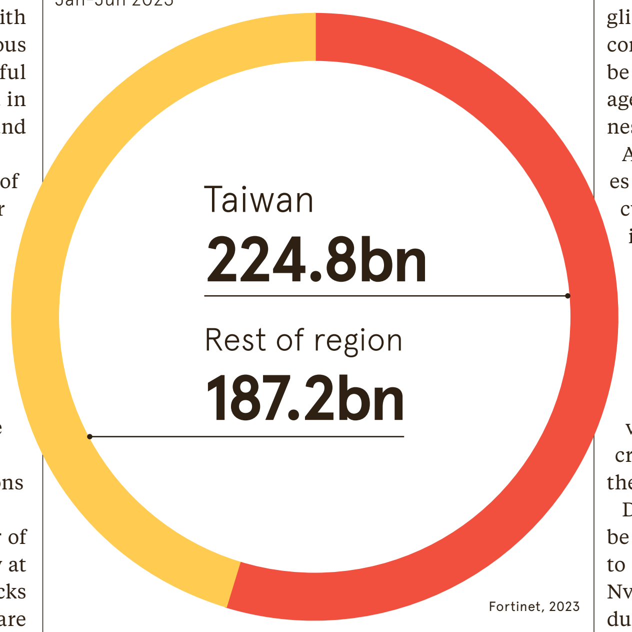
Shien-quey Kao, Taiwan's deputy minister for national development, admits that big businesses are increasingly looking to other locations in order to protect their operations. Taiwanese Semiconductor Manufacturing Company, which provides chips for Apple, is already building a factory in the US, which is expected to be operational in 2024.

The better prepared the business, the better it will be able to weather cyber attacks and any resultant breakdowns in the global supply chain. Otherwise, much like the people of Matsu, thousands of employees could end up being disconnected from the outside world, unable to work, and without the technology needed to do their jobs. That really would be a dystopian reality in the making. ●

> Attacks against Taiwan could disrupt the supply of virtually everything we use daily

TAIWAN EXPERIENCES MORE THAN HALF OF ALL CYBER ATTACKS IN THE ASIA-PACIFIC REGION

Malicious cyber attacks in the Asia-Pacific region by target, Jan-Jun 2023



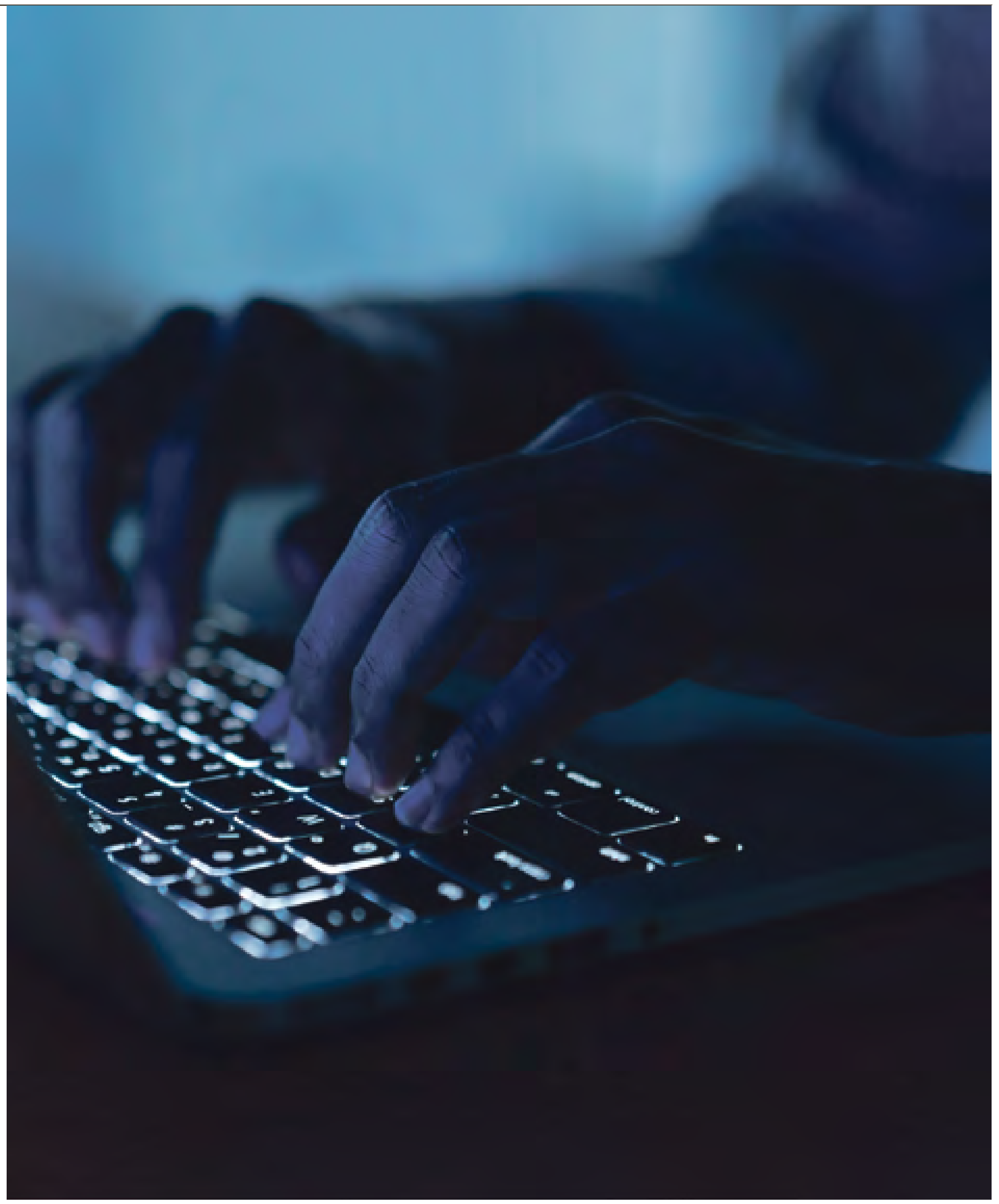
Fortinet, 2023

The Matsu islands are an established flashpoint in Taiwan's decades-long stand-off with China

Commercial feature

Generative AI ups the ante for cyber criminals

Global consumers aren't the only ones using generative AI – cyber criminals are adopting it too. This has huge implications for global cybersecurity



ChatGPT and other generative AI systems have taken the world by storm. The global populace has found their human-like and intelligent interactions extremely valuable over the past year – and so have criminals. Generative AI may be one of our greatest technological opportunities to date, but it is also one of our greatest threats, making enterprises a lot more vulnerable to attack.

Take phishing emails: these were one of the first attack methods to be optimised using generative AI. Now more realistic and highly personalised messages pop up in peoples' inboxes, cleverly disguised as a bank security check or a failed package delivery note, fine-tuned using AI. With a few keywords and the right query, a large language model such as Bard or ChatGPT can generate increasingly realistic phishing emails.

The number of email-based attacks in the first six months of this year has experienced a staggering 464% surge versus the same period in 2022, with phishing making up nearly three quarters of these attacks, according to Acronis' mid-year cyber threats report. It is likely that the rise of this cyber threat over the past 12 months can be partly attributed to bad actors utilising generative AI.

"Generative AI is the latest tool, and like any tool, you can use it for good or bad. The better you know how to wield the tool, the more damage you can create. History has shown that bad actors are quick adopters of such things. It doesn't help that generative AI is very easy to use. When it comes to cybersecurity, the regular rules don't apply anymore," explains Candid Wuest, vice-president of research at Acronis, a global cyber protection company, which works with more than 500,000 businesses globally.

"These are early days, but it could turn into a tsunami of cyber crime. Enterprises must act now in order to combat this new threat. Generative AI is also evolving and learning fast. Expect more frequent, more sophisticated attacks and the further automation of cyber attacks in the future. This is an asynchronous battle."

A growing threat

Even though developers of generative AI have introduced filters making it difficult to obtain certain content, these can be bypassed, depending on the query entered into the chatbot. The dark web also has its own generative AI tool, WormGPT. It has become the cornerstone of cyber criminals' arsenals. Now bad actors can create phishing emails in a myriad of languages and produce hundreds of slightly different email texts to make classic static detection difficult.

"Generative AI-driven cyber attacks are the fastest growing threat we see today. It's also luring more people into cyber crime. That's because the barrier is being lowered. It's just like asking Google. Chat type queries and responses can easily generate sophisticated and potent cyber attacks through this form of artificial intelligence," details Wuest.

The threat applies to both consumers and enterprises, with generative AI enabling a step change in capability for the cyber criminals. Feedback loops are ensuring exponential change, as more data is fed into generative AI tools. Through reinforced learning, this form of AI is now empowering new forms of cyber attack. For instance, it is learning which topics work well, improving the authenticity and trustworthiness of phishing emails.

"Because it is evolving so fast, many organisations are not aware of how big an issue this is going to become. A wait and see approach could be fatal. Raising the cybersecurity budget a bit for 2024 isn't going to cut it either. If enterprises have put in a budget for tackling generative AI-driven threats for next year, they should think about doubling it. That's how big this issue is going to be," points out Acronis' Wuest.

Time to fight back

Generative AI models are also good at understanding programme code. Cyber criminals can therefore paste source code into it and ask about potential weaknesses, thereby producing improved malware and ransomware.

The use of this form of AI by enterprises is also a risk in itself. If internal data is being used to fine-tune AI models, this could be leaked by hackers. Enterprise generative AI tools can also be corrupted by bad actors such that they either cause reputational damage or incur costs to an organisation.

"Going forward, we expect to see more attacks against the AI itself. Generative AI chatbots could even be corrupted to give wrong answers so that it promotes the competition. Or a piece of malware could use up your AI budget by making thousands of fake queries. We've seen something similar in the past with Google AdWords. Data breaches falling foul of GDPR legislation with big fines are also possible. AI-on-AI wars could become a reality," warns Wuest.

"It helps that we've been using artificial intelligence for a decade to defend against increasingly sophisticated attacks. Knowing the technology landscape for this threat is crucial. The security community is now actively working on developing countermeasures to generative AI threats. But organisations need to be aware of where exactly they are vulnerable."

Visibility is important in this regard. Businesses need observability across their entire IT estate, whether that's laptops used by employees at home, servers in the cloud or on-premises infrastructure. Then there are supply chain partners who could be a threat. Data sharing will be a crucial part of finding these vulnerabilities.

Simplification is also vital. Consolidating IT infrastructure and service providers can help in this process. After all, infinitely complex systems are inherently difficult to control when it comes to automating tasks, security checks, firefighting and reducing human error. For instance, 22% of global companies use more than 10 security solutions in parallel, according to research by Acronis.

"The more solutions you have, the more opportunities there are for things to go wrong. Reducing the number of vendors is crucial. That way you have less training, fewer interactions and fewer licences, so it can also be cheaper. The focus should be on building a resilient organisation," says Wuest.

"Also, working with cybersecurity partners that are constantly updating their systems to deal with the next generation of threats is really important. This is a crucial point in time. Privacy laws are getting stricter, with higher fines. Attacks are becoming more sophisticated and profitable. It's a tsunami coming your way."

> Chat type queries and responses can easily generate sophisticated and potent cyber attacks

To learn more, go to www.acronis.com

Acronis #CyberFit

shih-wei via Getty Images

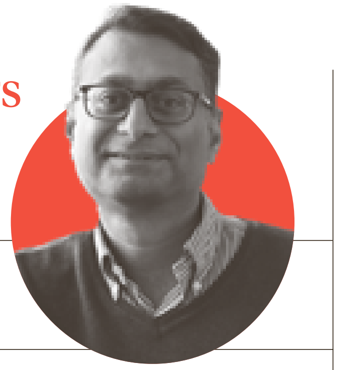
DEBATE

AI in cybersecurity: blessing or curse?

The rise of artificial intelligence is the latest escalation in the cyber war, enabling both more threats to be generated at speed and more effective real-time defences to be rolled out. So, who benefits most: the good guys or the bad guys? Two cybersecurity experts have their say

As told to Josh Sims

> “As far as bad actors are concerned, it’s a win-win”



Professor Muttukrishnan Rajarajan, Director of the Institute for Cyber Security at City, University of London

We’re in the early stages of assessing the impact of AI on cybersecurity, as we are in assessing its impact on so many other aspects of life.

But one thing is clear. The overall problem for security is going to be one of speed, veracity and automation, because AI is allowing attacks on systems in real time and, once set in motion, continuously and with minimum effort. Responding to that is something I worry that the good guys haven’t grasped yet. That fact is that whatever line of defence might be put in place, AI malware is finding a way around it.

Cracking good passwords, for example, is not necessarily a new feasibility; it’s just that what might have taken months or years before may now take days or even minutes. AI phishing attacks will reach a new level of sophistication, not least because AI can create customised phishing emails that will be hard for people to differentiate.

It’s often suggested that false positives are going to be one of the bigger headaches for cybersecurity in future. On the one hand, AI will undoubtedly boost threat reporting, helping companies to safeguard systems when they encounter new, unknown threats that don’t fit into existing patterns. Unfortunately, AI-powered attackers will also be able to generate malicious false positives, to encourage unnecessary shutdowns. As far as bad actors are concerned – or at least those who just want to disrupt for ransom, perhaps – it’s a win-win.

Part of the bigger problem is that there are going to be more and more means by which AI malware can find an entry point. As a result of the Internet of Things, for instance, we have ever more smart devices that are connected intuitively. They talk to each other without much input from us. That brings conveniences, but such connectivity also opens up huge vulnerabilities.

AI also means that resources will be a massively important issue. AI is not cheap, so to employ it in defending against a cyber attack will prove costly. Big business may be able to cover that, but it likely leaves micro-businesses, of between zero and nine employees, open to attack. That’s a problem because, in dealing with those smaller businesses – through banking, for example – that still leaves bigger businesses exposed by the back door, throughout the supply chain.

It isn’t only monetary resources that will be a factor. It’s human resources, too. There’s a huge skills gap when it comes to people who understand the implications for AI in the cybersecurity space. Even large companies can’t find the expertise. It’s also why I think the use of AI to break security systems is, initially at least, going to be employed at state level, where the resources, both technological and human, are more readily available.

But even those experts in AI and cybersecurity won’t have it easy. It’s one thing to understand AI’s impact on cybersecurity now, but it’s no exaggeration to say that in just a few months the processes involved may have moved on. I often read the latest industry white papers on AI and cybersecurity on my commute, because it’s remarkable how out of date they already are by the time they are published. That’s worrying because the industry leaders lack the depth of knowledge and skills to plan for any future attack.

In the longer run, quantum computing will help to defend against AI-based attacks. We are already seeing some larger organisations and governments using quantum systems. That makes sense because we’re talking about ever-growing complexity for defence and attack.

But the widespread commercial use of quantum is some way off. That allows me to come to this conclusion: if I had to bet right now on whether the good guys or the bad guys are going to win the early stages in this AI ‘war’, I’d have to put my money on the bad guys.

> “The fact is that whatever line of defence might be put in place, AI malware is finding a way around it

> “Our defences are simply going to be that much more sophisticated”

Amanda Finch, CEO of the Chartered Institute of Information Security

There are, of course, valid reasons for concern about the advent of artificial intelligence in the cybersecurity world. In some regards, our problems will get bigger. But I think there are many reasons to regard this as a boon too.

For one, AI will usher in a whole new set of technologies which, by enabling increased automation, will do away with a lot of the repetitive tasks that are currently necessary.

That automation will also bring a much greater level of observation – both continuous and global, but also deeper, giving us the ability to spot suspicious patterns that are much trickier to identify. Our defences will simply be that much more sophisticated, and vulnerabilities will come to light that much faster. At the moment we deal with a lot of false positives, but deep learning tools will help to reduce the likelihood of their occurrence.

I think the arrival of AI will encourage security professionals to think differently, too. It’s one thing to introduce new technology, but ultimately it’s about finding innovations in terms of how that technology is harnessed. At the end of the day, AI is just machine learning. It matters, though, because it will open the doors to greater successes in cybersecurity and lead to a flurry of start-up creation from those who see unrealised potential in AI’s application in cybersecurity, or who see the need for greater protection from AI-based attacks for smaller businesses and organisations that don’t have the resources. That will be good for the economy. We are already seeing some amazing firms emerging in the UK.

Of course, we’re still facing massive shortages of expertise in cybersecurity. AI won’t improve that; quite the contrary. But it will generate demand for new types of expertise. I think that will make cybersecurity a more attractive sector in which to work – and more interesting work at that. It will generate a need for a varied kind of workforce too, from analytical thinkers to risk managers and communicators, to explain the new threats.

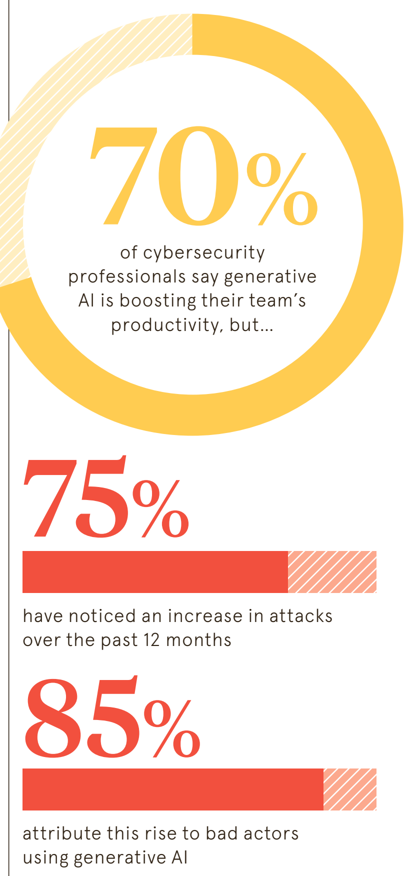
That could be good, for the employment of neuro-diverse people, for example, whose particular ways of thinking could prove invaluable. But I think it’s primarily going to be good for the health of the cybersecurity industry at large. It may even be able to help with burnout, which is a major issue in the industry.

The bad guys only have to get their attack right once, whereas the good guys on the defence have to be right all the time. And since AI will usher in more complex attacks, we can expect that it will also require greater cooperation between businesses, organisations and friendly states. There will be less territoriality. We’re already seeing a greater sharing of data ahead of AI’s impending impact on cybersecurity.

Can AI bring enhanced levels of compliance to the cybersecurity profession? That’s a tricky question. Obviously, the bad guys don’t follow the rules, but AI will help the good guys to stay good. It will encourage more widespread adoption of best practice guidelines, and that for me is more important than implementing further laws and regulations.

So, there’s an opportunity here for all sorts of progress. We can’t pretend that the implementation of AI in cybersecurity isn’t another big escalation in the arms race between the defenders and attackers of cyberspace. But there never really was any end to that arms race in sight. Cyber changes every year, and AI is just the latest thing.

That may sound casual, but perhaps there’s even a positive in that: it has put cybersecurity on the map. When I started out, people didn’t know about firewalls. Now, in part because of this conversation around AI, most people have a basic understanding of the need for cybersecurity. The problem may be bigger, yes. But we’re all that much more savvy about it, too. Now we just have to get on with things and deal with it. ●



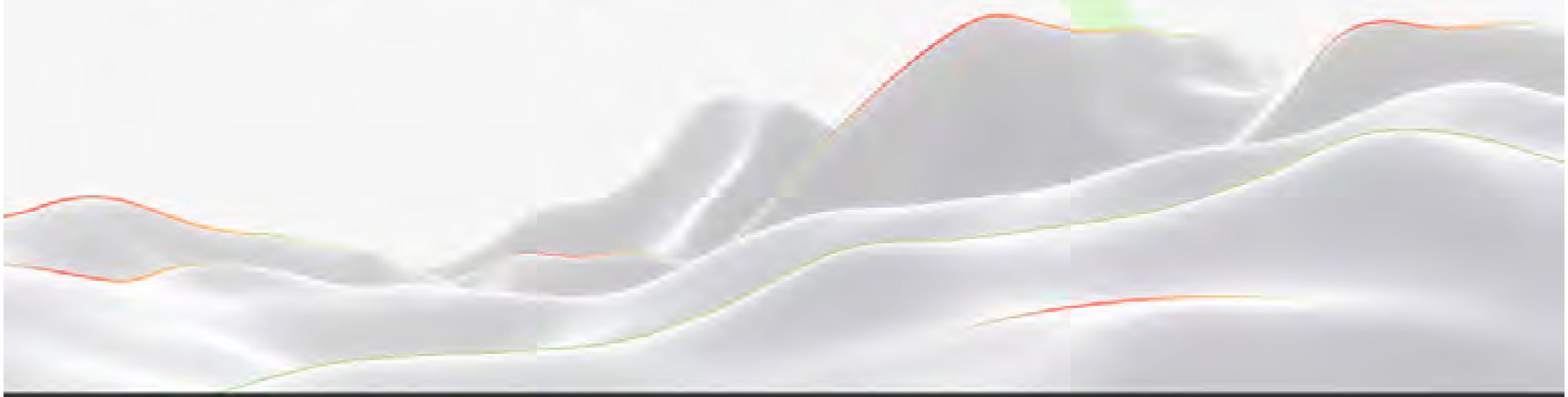
Sapio Research, 2023

Cantium in partnership with tenable

Enhance your cyber security posture

Improving your vulnerability management with:

- **Tenable One** platform implementation
- **Tenable One** ITSM integration
- Streamlining your **vulnerability management** processes
- Prioritising and remediating vulnerabilities



Cantium

Redefining the outsourcing model for the public sector and its supply chain.

cantium.solutions