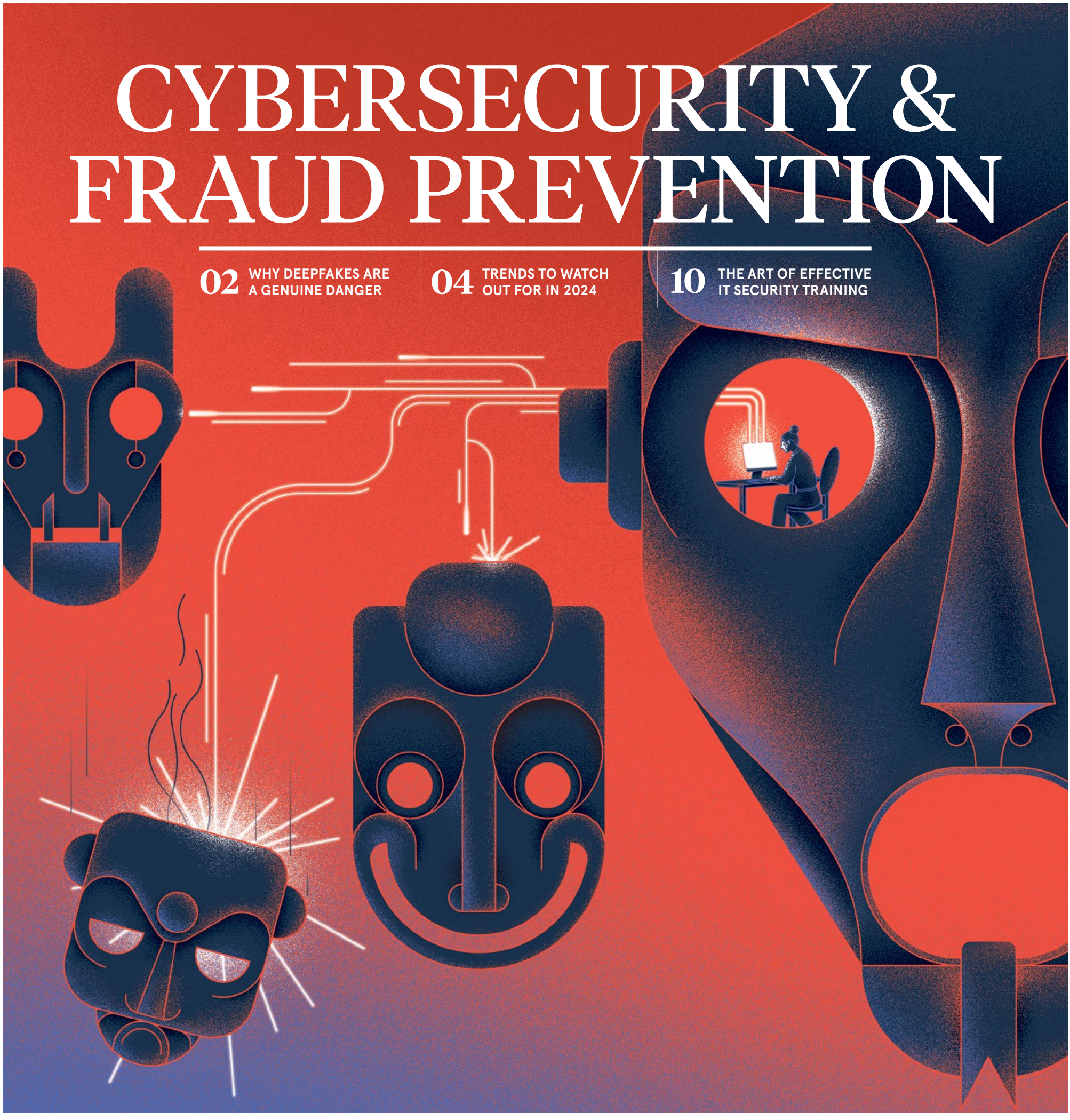
CYBERSECURITY & FRAUD PREVENTION



CYBERSECURITY & FRAUD PREVENTION

Distributed in
THE TIMES

Contributors

Ben Edwards
A freelance journalist who has been writing for more than a decade about business, finance, technology and the law.

Kate O'Flaherty
An award-winning journalist who specialises in covering data security issues that matter to businesses, governments and IT users.

Rosalyn Page
An award-winning writer who specialises in covering technology, innovation and digital lifestyle matters.

Jonathan Weinberg
A freelance journalist specialising in technology, the social impact of business and the future of work.

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
Kellie Jerrard
Harry Lewis-Irlam
Colm McDermott

Illustration
Sara Gelfgren
Samuele Motta

Design director
Tim Whitlock

Certified B Corporation

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 enquiries 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.

@raconteur raconteur-media @raconteur.stories

raconteur.net /cybersecurity-dec-2023

ARTIFICIAL IMPERSONATION

Why business genuinely has to worry about deepfake fraud

The rapid advance and increasing availability of AI-powered technology is making it ever more easy for criminals to dupe unsuspecting companies by impersonating senior executives

Ben Edwards

When fraudsters made off with $35m (£28m) from an unnamed US firm in early 2020, all it took was one telephone conversation and a few emails.

To execute the heist, the criminals used artificial intelligence to clone the voice of a director at that company, convincing a manager that the call was a genuine one coming from HQ, according to court documents. Posing as the senior executive, they instructed their victim to transfer the money as part of an acquisition the firm was supposedly making.

The emails, designed to look like they were coming from a corporate lawyer, backed up the deception.

In another case, reported by the *Wall Street Journal*, the CEO of a British energy company was tricked into thinking he'd been phoned by the boss of the firm's German parent company. When instructed to send €220,000 (£190,000) to the account of what he thought was a Hungarian supplier, he duly complied.

Both are examples of so-called deepfake fraud, a scam that uses artificial intelligence to impersonate another person on a phone call or even a video conference. While documented cases remain relatively rare, fraud experts report that the threat is increasing as advanced AI tech becomes more accessible.

"We're on the cusp of seeing these situations more and more," observes David Fairman, chief information officer at cybersecurity company Netskope. "With the rise of generative AI over the past year, it has become much, much easier to gain access to these capabilities. These services are more widely accessible to the masses – you don't need to be a data scientist or have a strong technical background to start using them for malicious purposes."

Security experts are also seeing examples of such technology being used in extortion attempts. Fairman has heard about cases in which criminals created deepfake images portraying senior executives in compromising situations to blackmail the victims into granting them access to their firms' resources.

This technology is not only being used as a vehicle for stealing money. Mike LaCorte, co-founder and CEO of investigation agency Conflict International, points out that "it could be used for competition research, industrial espionage or even efforts to spread disinformation or damage a competitor's reputation".

Photo illustration by Getty Images

As the two aforementioned cases of fraud highlight, the deepfakers will typically try to impersonate someone in a senior position because their subordinates are less likely to question their requests.

"When employees think they are dealing with someone in the C-suite, it applies an element of pressure and urgency that can almost force the situation," Fairman notes.

Deepfake technology can also make it easier for criminals to mount so-called social engineering attacks, typically targeting new starters or lower-level employees and building their trust over time, gradually creating opportunities to commit fraud.

"Each time you interact with someone remotely, you could be at risk of thinking that you're dealing with a real person but it's actually a deepfake," warns Sabrina Gross, regional director at digital ID authentication platform Veridas.

Although the deepfakers may be attracted by the greater potential rewards of targeting a large corporation, smaller businesses are just as vulnerable to attack, if not more so, given that they're less likely to have robust governance processes in place, Fairman warns.

While the risks are clear, it's hard to gauge the true scale of the problem, partly because organisations are unlikely to broadcast that they have been hoodwinked. Depending on the nature of the attack, companies may not even realise that they have become victims.

"There aren't lots of statistics on this, unfortunately, because no one really wants to share where they have been super-vulnerable," Gross says. "Much of the time, a business wouldn't necessarily know that it has been hit unless someone in the organisation were actively seeking a security breach."

Corporate boardrooms are becoming increasingly concerned about the broader dangers associated with the rapid advance of AI. Research by cybersecurity firm Kaspersky indicates that 59% of C-suite members are worried about the potential security threat presented by generative AI. Despite this, only 22% have discussed establishing safeguards in leadership meetings.

"It's quite concerning to me that they recognise the potential problem, yet haven't got the capability to meet the challenge," says David Emm, principal security researcher at Kaspersky.

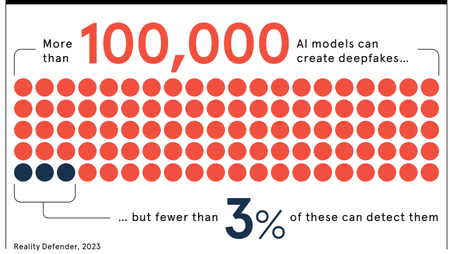
But there are some basic hygiene techniques that any enterprise can adopt to spread awareness of the deepfake threat across the organisation. For instance, while bogus audio can be hard to detect, there are other non-technical warning signs that people should be alert to, as Emm explains.

"With deepfakes, it makes more sense to consider the behavioural context," he says. "This less a matter of asking yourself: 'Is this speech a bit jittery or is this image suspiciously shaky?' It's more a question of: 'Was I expecting this person to get in touch and are they pressuring me into doing something that's out of the ordinary?'"

In such cases, companies could establish a call-back procedure so that the authenticity of a request can be verified. They would also be well advised to cover the threat of deepfake attacks in their broader IT security training.

As Fairman stresses: "All organisations have a responsibility to ensure that they have established a strong control framework and put suitable processes in place."

As sophisticated deepfake tools become ever more accessible, firms must therefore ensure that all staff understand that the caller on the other end of the line, however genuine they might seem, might not be the person they're claiming to be.



Reality Defender, 2023

Commercial feature

Q&A
Awareness is not action

Employees broadly understand the implications of cybersecurity and how their behaviour could impact their company's safety – and yet still take actions that could put it at risk. Mimecast EMEA field CTO, **Johan Dreyer**, explains that employees need better support to maximise their cyber hygiene and how businesses can provide it

Q Why do so many organisations struggle to have a culture of cybersecurity?

A It's quite simple. Business leaders do understand the potential risks associated with lax cybersecurity. Quite apart from their regulatory commitments, there are significant costs incurred as the result of an attack, from systems recovery to business downtime. Business owners are acutely aware of the need to make their organisations as cyber secure as possible.

Findings from our *State of Email Security 2023* report have shown that almost every business (99%) offers some form of cybersecurity awareness training to its staff. And yet, in the past 12 months, three out of four have seen an increase in email-based threats, two-thirds have been harmed by a ransomware attack and 80% believe their company is directly at risk as a result of careless or negligent employees.

This negligence is not down to laziness, a devil-may-care attitude or even malice. On the whole, employees are as keen as their bosses to be safety conscious when it comes to cybersecurity. The problem is that cybersecurity training as it stands is rarely tailored to the needs of the employee. Our *Collaboration Security: Risks & Realities of the Modern Work Surface* research found that one in five employees skip all the cybersecurity reviews before responding to a private message on a business collaboration tool with a link or an attachment, for example.

Q How do we bring employees' understanding of cyber risk closer to that of the business?

A The same logic that you might apply to clicking on a dodgy ecommerce or social media link needs to apply to the corporate culture. As a consumer, you know you can find yourself in a position where your personal life is severely impacted if you're not thinking about what you're clicking on. The more we can bring that consumer understanding into a work context, the more we'll have the empathy and understanding of colleagues who may otherwise not have been cyber aware.

We aren't expecting employees to become cyber experts, but that shouldn't mean they're ignorant of good security practice or what a good standard looks like. When we deliver awareness training, we need to design engaging content that connects those personal experiences to the behaviours we would like to promote.

Say an employee is working remotely at a coffee shop. Do they go to get more hot water for their coffee and leave their laptop unattended with the screen open, meaning someone could gain access to sensitive information? In the same scenario, would they leave their personal banking signed-in? These are things we need people thinking about.

Q Good cyber hygiene isn't just a defensive measure. How do businesses with actively cybersecure employees gain competitive advantage?

A Organisations with great cyber risk posture, a strong security culture and demonstrable accreditation in protecting their people, value chain and shareholders are well positioned to outperform their counterparts. For example, many organisations will ask to review a potential supplier's cyber credentials and this will play into the ultimate award of contracts.

Impacts of cyber attacks on an organisation can include business interruption resulting in loss of production, direct financial impact as a cost of recovery and loss of reputation within your customers, suppliers and shareholders. These are serious consequences.

Q Cybersecurity is a highly regulated, complex set of policies. How do we translate that to the average employee so they can absorb and understand their role?

A It's our responsibility as an organisation to create links between action and consequence – and showcase them. This goes back to company culture. There is a policy-and-compliance approach where you're presented with a long document with lots of dos and don'ts and a space to sign at the bottom. It covers compliance and audit requirements.

The reality is that people have information overload. The likelihood that someone has fully read through and understood that document is low. Also, the speed the world moves at means these documents struggle to stay current.

It's important to use relatable, storytelling-driven approaches. There is much more demand today for impactful, engaging commentary than there might have been five or 10 years ago. Content that is topical and relatable and contains a personal experience that is still connected to the world of work is key.

We can't get away from a compliance-driven approach entirely. We must make sure our reports to the market are accurate and safe. Agreements won't be going away any time soon. But above all, we have to connect with the employee's sense of purpose – their 'why' – and that means connecting their personal safety online with that in the workplace. Making them aware of how good digital decision-making can have a positive impact on the organisation and how the reverse can also be true.

Q When threats are evolving and becoming more sophisticated, how can a business create a culture that is safe but accepting of the fact that no one and no policy is 100% bulletproof?

A Business owners must foster an environment where speaking openly is encouraged. I've seen organisations that have managed to turn a potentially negative situation into a positive. Blaming, shaming and whistleblowing are counterproductive – fear doesn't drive good cultural behaviour and that creates poor outcomes. By encouraging openness and accountability without blame, the business can learn, fix and move on.

Q How can businesses promote their cybersecurity preparedness as a positive brand attribute?

A I'd love to see accreditation similar to the Red Tractor for British produce or the B Corp certification for ongoing ESG commitment. We do have some level of this with programmes such as the ISO 27001, SOC2 Type 2, TISAX and various other accreditations. But most of these are controls focused, require certification on a periodic basis and the scope can vary drastically from organisation to organisation. These are all great starting points but don't always accurately represent the culture of cyber risk awareness that you've worked hard to promote.

However we approach cybersecurity – and we must because the costs involved in not doing so are too great from multiple angles – we must do it with our employees at the heart of the process. We can't remove all risk; mistakes will be made. But if we invest in our people, put the right training in front of them and remove barriers to compliance, our employees will feel empowered to make the right decisions and feel supported throughout their careers and cybersecurity journeys.

> Organisations with great cyber risk posture, a strong security culture and demonstrable accreditation in protecting their people, value chain and shareholders are well positioned to outperform their counterparts

1 in 5

employees skip all the cybersecurity reviews before responding to a private message on a business collaboration tool with a link or an attachment

Mimecast, 2023

To find out more, visit mimecast.com/this-is-personal

mimecast

EMERGING TRENDS

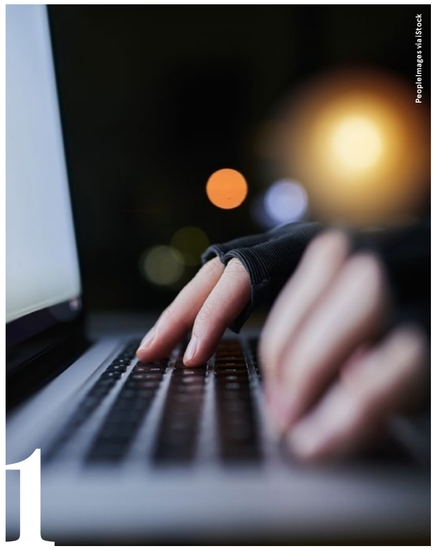
5 cybersecurity predictions for 2024

The battlefield and its tactics never stop evolving, so business leaders can't afford to ignore any emerging developments. Here are the trends they will need to know about next year

Kate O'Flaherty

The cyber threat landscape is changing constantly, with criminals taking advantage of the latest advances in IT to mount increasingly sophisticated attacks. Trends concerning the use of tech such as artificial intelligence and ransomware have dominated the headlines in 2023 – and these are set to cause even more disruption over the coming year.

As experts in the field will testify, businesses wishing to maintain effective defences need to be proactive, so what should their leaders be looking out for in particular?



1

AI will pose a growing threat, but it will be used more in defence too

Artificial intelligence has featured in a relatively small proportion of reported incidents over the past year, but this will change as cybercriminals start using the technology to "personalise and slowly scale up attacks", predicts Phil Venables, CISO at Google Cloud.

"By using AI-based large-language-model algorithms, attackers can make malicious content that looks, flows and reads like genuine material, making it even harder to detect phishing attempts," he warns.

More broadly, the use of generative AI to create fake news and related material on the internet could hugely increase the spread of disinformation, thereby "reducing public trust in online content".

But, while AI presents a clear danger in the wrong hands, the technology's capacity to process and contextualise huge volumes of data also has the potential to reinforce firms' cyber defences.

"This will come to fruition in 2024, with AI enabling defenders to strengthen detection and accelerate analysis," Venables says. "This will equip them to respond quickly and at scale."

Criminals will probe weak links in supply chains

One of the biggest supply chain data breaches of 2023 was the attack on a popular file-transfer application called Moveit. Criminals exploited a vulnerability in the software to break into thousands of organisations.

Supply chains will remain prominent targets in 2024, according to Tristan Morgan, managing director of cybersecurity at BT.

"Events such as the Moveit vulnerability affected many businesses, including international airlines and large retailers," he says. "Globally, this single hack cost businesses more than £7.9bn, affecting more than 1,000 companies and 60 million people."

Such incidents illustrate how easy it can be to break into big companies via their suppliers. Morgan believes that the success of this attack will encourage more criminals to attempt similar exploits. His opinion is supported by Gartner, which has predicted that 45% of all organisations will have experienced attacks on their software supply chains by 2025.

As the risk of cyber attacks grows and supply chains are increasingly threatened, Morgan forecasts that there will be a shift next year towards so-called zero-trust models – a security strategy based on the 'never trust, always verify' principle.

"Zero-trust architecture aims to protect the back door from supply chain attacks by requiring verification from anyone trying to connect to your systems," he says. "This helps to block unwarranted access."

2

Ransomware gangs will turn their attentions to smaller businesses

Any enterprise can be targeted by cybercriminals, whatever its size. Quentyn Taylor, senior director of information security for Canon in EMEA, predicts that smaller firms will increasingly bear the brunt of ransomware attacks in 2024.

This is partly because the decreasing cost of so-called ransomware-as-a-service offerings has made this data-locking weapon so accessible, reports Dr Tiffany Harbour, senior cybersecurity adviser at tech consultancy Access Partnership. She says that small businesses and local authorities "will be more at risk than ever" next year, given that they have relatively little money to spend on shoring up their defences.

Taylor expects that a growing number of firms will put plans in place next year to mitigate the risk of ransomware attacks as part of their efforts to reassure shareholders and attract new investment.

"Businesses are reporting net-zero claims in their statements and I wouldn't be surprised to see similar disclosures about their cybersecurity measures," he says.

3

4

The shortage of security skills will worsen

The well-documented cybersecurity skills gap is set to widen in 2024 as companies struggle to find the talent they require to repel ever-more sophisticated attacks. With experienced defenders so thin on the ground, companies are more likely to commit basic errors that criminals will be quick to exploit, warns Ian Thornton-Trump, CISO at security firm Cyjax.

The shortfall "may also impede the security improvements that organisations want to undertake, such as addressing their technical debt and legacy systems exposure", he says.

"Those working in cybersecurity must ensure that they remain relevant and able to support digital transformations," Thornton-Trump adds, noting that expertise in fields such as zero-trust architecture, AI and the transferral of legacy solutions to the cloud will be particularly in demand.

If they're to solve this skills shortage, businesses need to "establish processes for talent progression, offering more effective training and higher salaries", he argues. "Workforce development prioritising women, people with disabilities and under-25s is required."

Plugging software holes will become more difficult

Software holes were constantly appearing in 2023, often leading to supply chain breaches such as the Moveit attack. New vulnerabilities are being announced and fixed all the time – most organisations have heard of Microsoft's Patch Tuesday. But keeping abreast of them all will become an increasingly daunting task, according to Sean Wright, an independent security researcher.

He describes the challenge for businesses: "As soon as you've asked a team to patch one set of vulnerabilities, they'll need to address more issues, often with a limited time in which to do so."

To exacerbate matters, a significant proportion of firms aren't responsive enough to the warnings they receive. Even after a security problem is disclosed along with the appropriate fix, they will often ignore the alert or be "incredibly slow" to apply the patch.

Wright predicts that more companies will be scrutinising their suppliers next year to check whether they're taking the appropriate action quickly enough. With this in mind, he would strongly advise firms to focus on their asset management and vulnerability programmes.

5

Commercial feature

What CISOs need to consider in a post-AI world

ChatGPT and other generative AI tools have changed the game when it comes to work, but how do CISOs avoid the major headaches that come with this new brand of shadow IT?

A little over a year since the release of Open AI's groundbreaking ChatGPT, organisations and their employees are harnessing the power of generative AI tools with largely positive outcomes. Goldman Sachs forecasts that productivity growth could rise by 1.5 percentage points from this new wave of generative AI over the next decade.

The change is being felt institutionally, with companies rapidly rewriting processes to include artificial intelligence. But it's also happening from the bottom up, with individual workers adopting these tools in their day-to-day jobs in a far broader way.

What appeared to be the ultimate silver bullet for workplace productivity challenges has now emerged as the newest shadow IT concern (a device, software or application that sits outside the IT department's control) for CISOs.

"Most practitioners are talking about us entering the AI age," says Neil Thacker, chief information security officer EMEA at Netskope, an organisation that helps others protect their data and defend against cyber threats. Based on data from millions of enterprise users globally, Netskope found that generative AI app usage is growing rapidly, up 22.5% in just two months earlier this year.

Employees are becoming unbridled in their use of the tools to improve their workflows. "This gives us lots of opportunity to leverage and harness new technology," says Thacker. "But CISOs also have to consider the risks generative AI brings."

Where data goes

IT leaders and CEOs, mindful of their business's reputation and continuity, rightfully harbour concerns regarding the data that is fed into generative AI tools. Organisations with 10,000 staff members or more use an average of five AI-powered apps daily. ChatGPT leads the pack, receiving over eight times the number of daily active users compared to any other generative AI application, according to Netskope research.

With big names in the tech world, like Samsung, banning the use of ChatGPT by employees after sensitive data was accidentally leaked earlier this year, the million-dollar question emerges: how safe are company secrets in the hands of AI applications?

Netskope's analysis reveals that the source code for proprietary apps and services is posted to ChatGPT more than any other type of sensitive data, at a rate of 158 incidents per 10,000 users per month. Caution is vital when using AI, and the rules need to be understood by everyone. "For the workforce, it's all about performance and productivity," says Thacker. "Workers may not be aware of the risks. They may have interpreted the app's terms and conditions slightly differently to someone in the legal team – or more likely, they didn't read them at all."

Some employees may be better informed about the dangers than their peers. Yet, after weighing up the potential pitfalls of getting caught against the productivity benefits, they may decide it's a risk worth taking. So, how do you stop the misuse of AI from becoming a concern before it rears its head? "It really comes down to education," says Thacker.

Beyond educating staff on how generative AI tools operate, how they manage data, and the economic dynamics of providing services for free or at a low cost to users (and understanding the implications for the data they process), Thacker suggests introducing real-time or point-in-time education. Pop-up banners can be coded to insert a warning when an employee is about to post sensitive data into an unapproved generative AI application. "That is a perfect time to educate somebody," he says, "Then and there, you can explain the risks and why you have that oversight in place."

The guidance from Netskope includes building a continuous inventory of which apps and services are being used by employees and for what purpose, and, fundamentally, what data is being used. In addition, organisations need to align with the many new AI risk frameworks that have cropped up in the past year or more.

Take a page from cloud

Personal cloud storage, messaging apps, collaboration tools – the bevy of shadow IT infiltrating workplaces is no new thing, and it's ever-growing.

Often, Thacker notes, decision-makers worry that instituting AI policies, education systems, and advice will take a lot of time, effort and resources – things that, in an increasingly competitive landscape, businesses don't have.

> Workers may not be aware of the risks. They may have interpreted the app's terms and conditions slightly differently to someone in the legal team

Leaders recognise the risks: alongside source code, employees are putting regulated data, intellectual property, and, in worrying cases, passwords and crucial keys into generative AI tools. But they also know the realities of running their organisation.

Instituting good working practices in a post-AI world doesn't need to be onerous, says Thacker. Instead, tech teams can draw strategies for safe and secure integration from their past efforts against cloud threats and repurpose them for the post-AI environment. He adds that the challenge of securing new technology without impeding its benefits is one that CISOs have been successfully overcoming for years.

Safeguarding may be simpler than business leaders think, then. "They need to apply the same controls to AI services as they did to cloud applications. That means using technology to automatically see which apps or services are being used inside their organisation and applying policy controls and advisory notes within the workflows," says Thacker.

Being forewarned is being forearmed. Knowing which services workers are using means businesses "can build out inventory and ensure that they have monitoring in place for those services," he says. But simply knowing what tools the business is using now is no good unless they're regularly updated.

Netskope has a database of 75,000 cloud-based apps to which it assigns risk scores, enabling security teams to determine easily whether using an app is safe or not. By that token, it has begun ranking hundreds of generative AI apps on the same system, all of which receive a risk score. The database will continue to expand as more new products enter the market.

When in doubt, and as AI becomes more ubiquitous across the business world, immediate insight into the risks associated with each new iteration of the chatbot or virtual assistant will provide those securing the business with peace of mind.

For more information, visit netskope.com

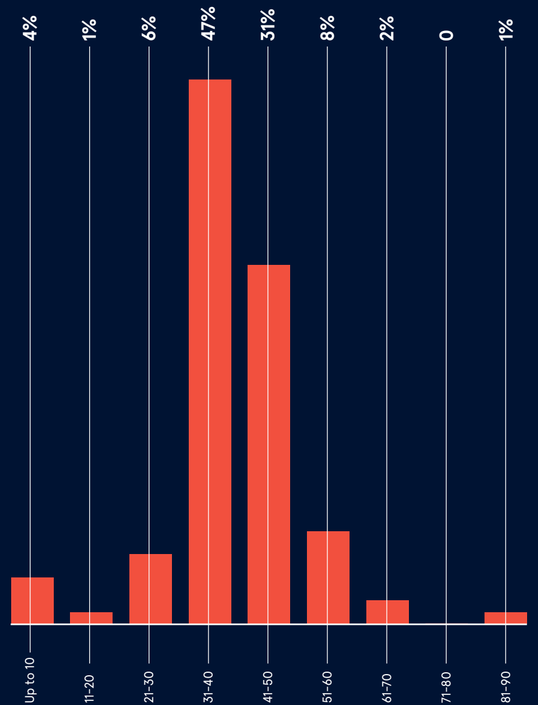
netskope

STRETCHED TOO THIN?

Cybersecurity teams play a vital role in defending their companies from potentially crippling attacks. It's quite the responsibility, which is bound to take its toll – in terms of both the resources required and the strain placed on cybersecurity professionals themselves. Given that maintaining consistently high levels of security is business-critical, why are so many employers allowing the people whose task this is to burn themselves out?

THE AVERAGE CYBERSECURITY SPECIALIST WORKED 41.3 HOURS A WEEK IN 2022, COMPARED WITH A UK MEAN OF 36.4 HOURS

Share of cybersecurity professionals working the following hours each week

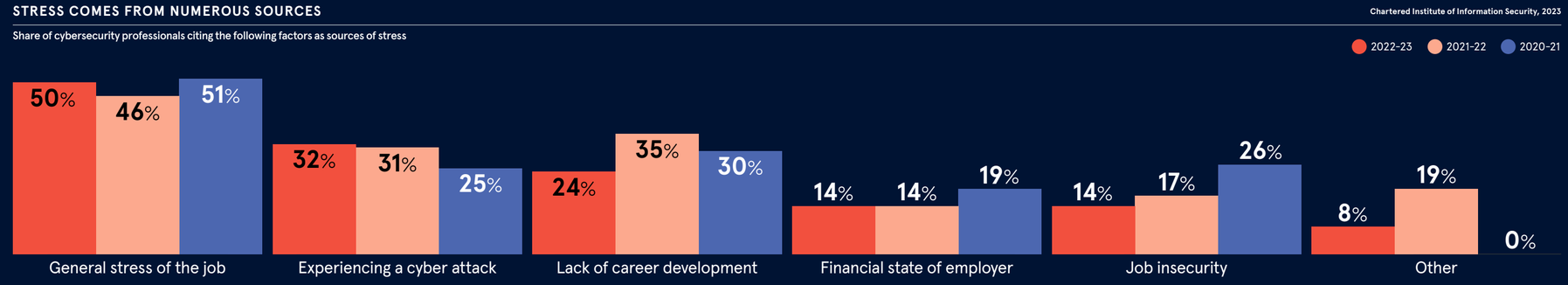


Chartered Institute of Information Security, Office for National Statistics, 2023

STRESS COMES FROM NUMEROUS SOURCES

Share of cybersecurity professionals citing the following factors as sources of stress

Chartered Institute of Information Security, 2023



HR-RELATED CONCERNS ARE BY FAR THE BIGGEST HEADACHE

Share of cybersecurity specialists citing the following as the biggest source of difficulty for their profession

Chartered Institute of Information Security, 2023

CYBERSECURITY PROFESSIONALS ARE SPLIT ON WHAT EXTRA INPUTS WOULD MAKE THEIR WORKING LIVES EASIER

Chartered Institute of Information Security, 2023

Is the industry short of resources or skills?

Is the industry short of experience or new entrants?

A CYBERSECURITY PROFESSIONAL'S AVERAGE TENURE IN A JOB IS ABOUT THREE YEARS

Time spent in current cybersecurity role, versus UK average employment tenure (years)

Chartered Institute of Information Security, Chartered Institute of Personnel and Development, 2023

INTERNAL RISKS

Inside job – the insidious rise of internal data threats

IT chiefs focused on maintaining corporate defences against cybercrime cannot afford to ignore the substantial – and increasing – danger posed by their firms' own employees

Jonathan Weinberg

The increasing sophistication of cybercriminals is prompting CISOs to devote ever more attention to protecting their firms' systems from attack. But security experts fear that, in doing so, they may risk overlooking a growing number of internal security threats.

According to research conducted by IT security company Imperva in 2021, "58% of incidents that negatively impact sensitive data are caused by insider threats". Of these incidents, 61% can be attributed at least partly to abuse or malicious intent, rather than innocent human error. The study also found that 60% of IT and data security professionals across EMEA prioritise preventing infiltration by outsiders over addressing internal threats, while 72% of organisations lack any strategy to deal with insider risks.

The three main reasons they cited for this laissez-faire approach were a shortage of funds, a lack of expertise and the belief that employees do not constitute a "substantial threat" to data security. But, given that the cost of insider criminality can run into millions of pounds, data security experts agree that firms generally need to manage this risk more proactively.

Manoj Reddy, security researcher at the Trellix Advanced Research Centre, reports that 70% of insider attacks are never disclosed by the firms targeted, adding: "Based on recent industry analysis, insider threats have increased by 47% over the past two years. This threat undermines the confidentiality, integrity and availability of the organisation, while aiding adversaries in gathering intelligence, carrying out sabotage and using subterfuge to achieve their nefarious objectives."

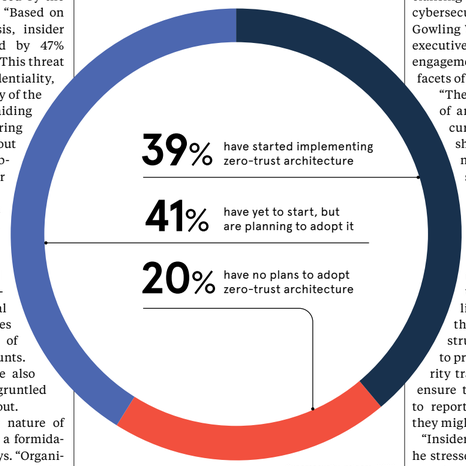
Analysts suggest that the cost-of-living crisis is driving more employees to copy sensitive corporate data and sell their companies' intellectual property to rival companies. Other cases involve the extraction of funds from client accounts. Beyond fraud, there are also destructive acts by disgruntled employees on their way out.

"The rapidly growing nature of insider threats presents a formidable challenge," Reddy says. "Organisations must prioritise security measures to retain stakeholder confidence. It's essential to identify, evaluate and manage such risks."

Not all insider threats have malicious intentions behind them, of course. It's often a case of employees simply ignoring their IT team's policies for their own convenience. For instance, research by cybersecurity company Armis suggests that employees in more than two-thirds of UK firms are putting their businesses at risk by downloading non-approved software from the web to their work devices without clearance from their IT teams.

BUSINESSES ARE INCREASINGLY TURNING TO ZERO-TRUST METHODS TO DEFEND AGAINST ALL KINDS OF SECURITY THREATS

Share of businesses planning (or not) to implement zero-trust architecture



Cybersecurity Insiders, 2022

Dr Igor Baikalov, chief scientist at cybersecurity firm Semperis and a former senior vice-president of global information security at Bank of America, suggests that the fact that remote working has become far more common could be "further eroding corporate security controls and supervision".

He believes that the insider security threat is being exacerbated by the increasing complexity of enterprise systems and the pressure on businesses to adopt new and often poorly understood technologies.

Baikalov adds that the abuse of system access privileges by employees "is a common element in insider attacks. Organisations need to implement a comprehensive identity threat detection and response solution that can prioritise and remediate vulnerabilities and misconfigurations in ID systems comprising several identity providers."

One key method of tackling insider risks is to apply the zero-trust security model, which grants employees what is known as least-privilege access. This is when system users are given just enough access to enable them to complete the task they have been assigned.

"This significantly reduces the attack surface and limits your potential exposure," explains Lewis Duke, threat intelligence lead at cybersecurity software developer Trend Micro. "The model challenges the traditional notion of a trusted network, recognising that any user or device could be compromised."

Helen Davenport, a partner specialising in data protection and cybersecurity matters at law firm Gowling WLG, believes that senior executives need to make board engagement and governance key facets of managing insider risk.

"The risk applies to businesses of any size, especially in the current economic climate," she warns. "It is therefore necessary to properly consider the cost-benefit aspects of all steps that can be taken to ensure a proportionate approach."

Duke also has advice for the C-suite. He argues that referring to system users as the "weakest link" could do more harm than good. A more constructive approach would be to provide more effective security training for employees and ensure that they are empowered to report any suspicious activity they might observe.

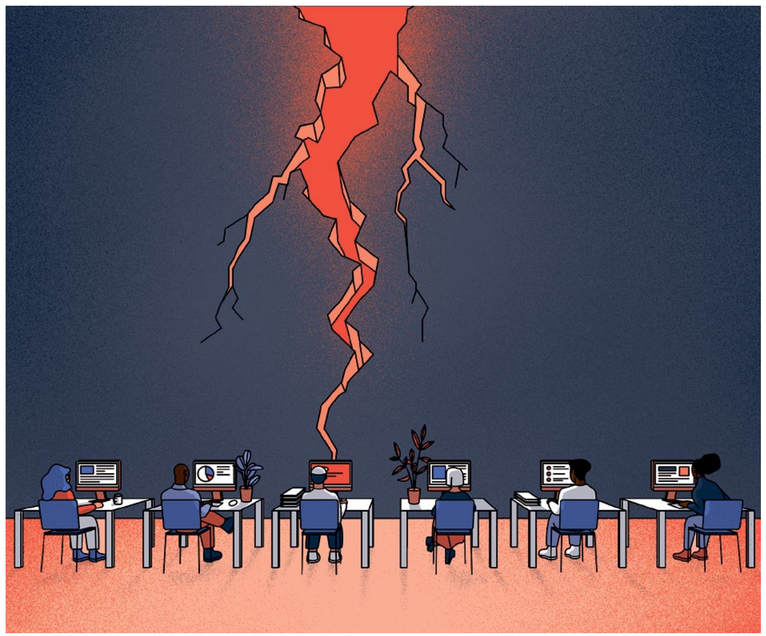
"Insider attacks are manageable," he stresses. "A proactive and user-centric approach to cybersecurity can effectively mitigate such risks and create a more secure digital environment. Armed with the right knowledge and tools, users can become valuable assets in the fight against insider threats, effectively turning the 'weakest link' into a strong line of defence."

The monitoring of employees is a particularly sensitive aspect of managing insider threats. Companies considering surveillance as an option should think carefully about its potential ramifications. That's the view of Ian Thornton-Trump, CISO at threat intelligence firm Cyjax. He says that monitoring can be a tricky measure to introduce, not only because of the legal implications but also because of the negative psychological effects it could have on those under observation.

While he believes that government bodies or firms operating in particularly sensitive fields may have a genuine case for using surveillance, Thornton-Trump warns: "Insisting on monitoring without the right reasons is going to damage morale, trust and loyalty."

He offers a piece of advice that firms should not overlook in their eagerness to use tech to combat insider threats.

"I would argue that psychology is what pushes people over the edge to create an insider threat," Thornton-Trump says. "Treating your people well will go a long way towards preventing them from becoming disgruntled and contemplating any malicious act. A happy employee is less likely to become a turncoat."



> I would argue that psychology is what pushes people over the edge to create an insider threat

How can AI help keep your business secure?

Much has been written about the offensive potential of artificial intelligence for hackers – but it's a tool like any other that can be used defensively too

Artificial intelligence has risen to the forefront of technological innovation, particularly in the past year. Although AI has been around for decades, it has only been in the past 12 months or so that generative AI has garnered global notoriety.

"With the advent of ChatGPT, and the competitors that came out shortly after, it basically dropped this idea into the consciousness of everyone," says Casey Ellis, founder and chief strategy officer at Bugcrowd. A multi-solution crowdsourced security platform, Bugcrowd is a member of the Hacking Policy Council, which works with the UK's National Cyber Security Centre and GCHQ.

By seeping into our collective consciousness, AI – the good, the bad and the ugly – is now at the forefront of people's minds. It's the nefarious uses of AI that regulators have focused on, with executive orders governing AI published in the US, an AI Safety Summit held in the UK and collective action taken by the G7 countries.

Regulators' focus on the threats posed by AI has crystallised thinking for businesses. "There's been a really sharp reaction from the regulatory and policy-making cycle," says Ellis. Because the focus has been so centred on the bad, rather than the good, business executives are more likely to worry about the offensive capabilities of AI in the hands of hackers.

This fear has been fuelled in part by headlines highlighting how the speedy automation of AI can enable those with ill will to launch a barrage of attacks against would-be victims.

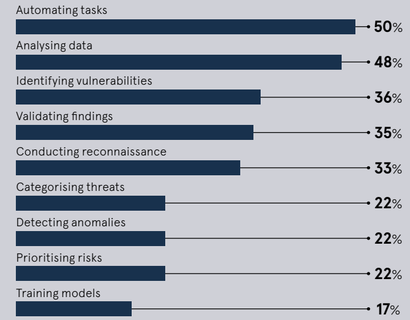
However, these headlines are not reflective of the full picture, says Ellis. "AI is a tool," he says. "And it's definitely powerful. And that's true in the hands of folks who are malicious. But it's equally true when AI is in the hands of folks who are benevolent and trying to help."

That includes Bugcrowd, which capitalises on the wisdom of the global community of white-hat hackers, who mimic what threat actors might do to leverage gaps in businesses' computer systems and highlight the risks. "The bad guys have got access to all this stuff," Ellis says. "But the good guys do, too."

TOP THREE AI CHATBOTS USED IN HACKING

TOP USE CASES FOR AI IN SECURITY RESEARCH

% of hackers who say they use AI for the following



Bugcrowd, 2023

Bugcrowd shifts the paradigm of thinking around the use of AI for evil to the idea that AI can be used for good. Generative AI is a tool that can be used defensively as well as offensively. "What these tools do is they give people really easy access to all that knowledge in a very simple way," says Ellis. "And it basically decreases time required to reach success." Solutions to a problem that may have taken hours to research can now be devised in a matter of minutes with the aid of large language models (LLMs). "It's democratised access to that kind of knowledge and made consumption and use a lot simpler," he says.

> Generative AI has democratised access to knowledge of AI and made consumption and use a lot simpler

An example of how Bugcrowd has used AI to keep its customers' businesses secure is in harnessing its power to corral and accurately match its diverse database of white-hat hackers from around the world. "It basically creates more opportunity for defenders. We can bring together all the ethical hackers we work with, every one of whom potentially has an answer to a problem a business has that it wouldn't otherwise solve," says Ellis.

Using AI in this way means that no challenge is insurmountable for businesses worried about the onward march of AI and what it means to put that power to automate tasks in the hands of threat actors. That's because an equal amount of power is being put in the hands of those standing alongside businesses, ready to defend them. "The barrier to entry has become a whole lot lower," says Ellis. "Folks don't necessarily need to learn technical skills to the same degree that they used to. They can more easily just get on with the job of whatever they're trying to achieve."

To find out more, visit Bugcrowd at Black Hat, Europe 2023 booth 315: www.bugcrowd.com

bugcrowd

EXPERT GUIDANCE

How to provide effective cybersecurity training

Attacks are on the rise, yet too many employers aren't giving their staff even the most basic education in mitigating the risk. Here, three experts in the field offer their tuition tips

Rosalyn Page

Cyber attacks on UK plc are becoming ever more prevalent, yet most employers appear reluctant to provide their staff with training in the latest IT security principles and practices.

According to the *Cyber Security Breaches Survey 2023* report published by the government April, only 18% of companies said that they had organised such tuition for employees over the preceding 12 months.

How should businesses looking to redress that shortcoming go about providing an effective training programme? Three experienced CISOs share their advice on this key element of cybersecurity best practice.

'Senior leaders' involvement will show everyone in the organisation how important this subject is'

Anthony Green

Manager of IT security operations and compliance, the Chartered Professional Accountants of British Columbia

Having educated hundreds of people in data security principles and practices, Green is convinced that such training must not be treated as a single standalone intervention.

Rather, it needs to be an "ongoing process that includes regular drills, updates and discussions on the evolving threat landscape. The goal should be to build a risk-aware mindset across the organisation," he says. "Regular engagement is key to that."

Green, who also creates academic programmes in cybersecurity at the University of British Columbia, recommends that employers take advantage of the free or low-cost frameworks offered by industry groups such as the Information Systems Audit and Control Association (ISACA) or the US National Institute of Standards and Technology. In the UK, there are government resources such as the National Cyber Security Centre's online training platform.

"These resources, including user-friendly infographics, can be shared to keep the subject near the top of everyone's minds," Green says. "HR and/or privacy teams can lead the way in making cybersecurity training part of the overall employee development process."

A firm believer in the value of frequent refresher sessions, he stresses the usefulness of activities such as 'lunch and learn' seminars and discussions about the latest cyber incidents to hit the headlines.

IT teams also need to run exercises such as phishing simulations, which help employees to get better at spotting and handling such threats. The idea is that cybersecurity becomes part of a company's daily operations as well as its culture.

Last but not least, senior leaders have a vital role to play in promoting the importance of effective security practices, as Green explains.

"Their involvement will show the whole organisation how important this subject is," he says. "This can only help to create a culture in which everyone takes cybersecurity – and their contribution to it – seriously."

> **HR and privacy teams can lead the way in making cybersecurity training part of the overall employee development process**

'Courses should present real-world scenarios that help to illustrate consequences of lapses and highlight the importance of best practice'

Pam Nigro

Vice-president of security, Medecision

Training programmes have to recognise the pivotal role of employee behaviour in keeping the cybercriminals at bay, stresses Nigro, who is also a board director at the ISACA.

"This means setting clear security objectives, conducting risk assessments and understanding people's knowledge gaps," she says, adding that courses need to be engaging and use different formats, such as live sessions and interactive modules, while avoiding tech jargon.

The examples they present should be "real-world scenarios that help to illustrate consequences of lapses and highlight the importance of best practice".

Programmes should be structured to incorporate ongoing training and updates with the aim of embedding cybersecurity into an enterprise's culture, adds Nigro, who likes to see courses that involve senior leaders and highlight exemplary practice.

She believes that the overriding goal of such interventions should be to empower people, because encouraging "openness and transparency helps to create a culture in which employees feel comfortable reporting potential threats".

Because the use of mobile devices for work purposes has become so prevalent, it is crucial to incorporate specialised training with specific advice on securing this equipment, according to Nigro.

Given the ubiquity of such devices in professional settings, "addressing their security is paramount in fortifying the overall resilience of a company", she says. By providing targeted training in how to secure mobile devices, an enterprise can mitigate the risks associated with their particular set of vulnerabilities.

"Emphasising the unique considerations associated with mobile device security helps to mitigate those risks, ensure a more robust defence and strengthen the organisation's overall cybersecurity posture," Nigro adds.

> **Emphasising the unique considerations associated with mobile device security helps to mitigate those risks**

'Employers must regularly update their training, at least annually, based on employee feedback, adoption rates and risks exceeding agreed tolerance levels'

Kayne McGladrey

Field CISO, Hyperproof

Training should be tailored to specific cyber risks in each learner's role, monitored and regularly updated, according to McGladrey, whose company provides a platform offering risk, security and compliance assurance.

For instance, "while all employees should be made aware of phishing techniques, specialised training in, say, incident-handling procedures should be delivered to the incident-response team only", he explains. "Similarly, organisations should provide training only if it's intended to reduce a specific risk, as it's unreasonable to expect employees to become knowledgeable about every possible topic in this field."

McGladrey adds that employers "should provide annual training at the very minimum, supplemented by micro-training modules after policy violations or incidents".

While a company's CISO and their team will typically lead the training, there are other options. These include engaging external expertise such as dedicated cybersecurity consultancies or a virtual CISO to develop a tailored programme.

Designing and delivering targeted courses is only half the battle for firms seeking to improve employee awareness. It's vital to assess their effectiveness to ensure that they're having the desired effect.

McGladrey suggests that, instead of relying solely on the training provider's dashboard for evaluating uptake, internal compliance teams should gather and assess evidence of effectiveness independently.

"This enables organisations to show to their leadership teams the effectiveness of their training in risk mitigation," he says, adding that Hyperproof automatically monitors progress in KnowBe4, a popular cybersecurity training platform.

"A KnowBe4 module on phishing completed by 95% of staff within a month, for instance, will be more impactful than one with only 50% adoption in reducing that risk," McGladrey says. "This also removes the need for the second line of defence to manually request and verify training completion."

Third-party verification will also enable boards of plcs to describe their cybersecurity training controls in line with regulatory requirements. McGladrey notes that this can also be used alongside evidence of other cybersecurity control operations to negotiate favourable premiums with insurers.

He adds that employers "must regularly update their training, at least annually, based on employee feedback, adoption rates and risks exceeding agreed tolerance levels".

> **It's unreasonable to expect employees to become knowledgeable about every possible topic in this field**

Hey imposter

Ever feel like you're pretending?

Like you're always faking it without ever making it?
That's normal. Today's business world is so complex that the more you grow in your career, the less you know about your job. Raconteur clarifies the complexities of modern business with stories that help you make more informed decisions and build more successful companies.

So, stop pretending.
Live up to your true potential.

Become a better leader at Raconteur.net

Raconteur

Stories that connect modern business.