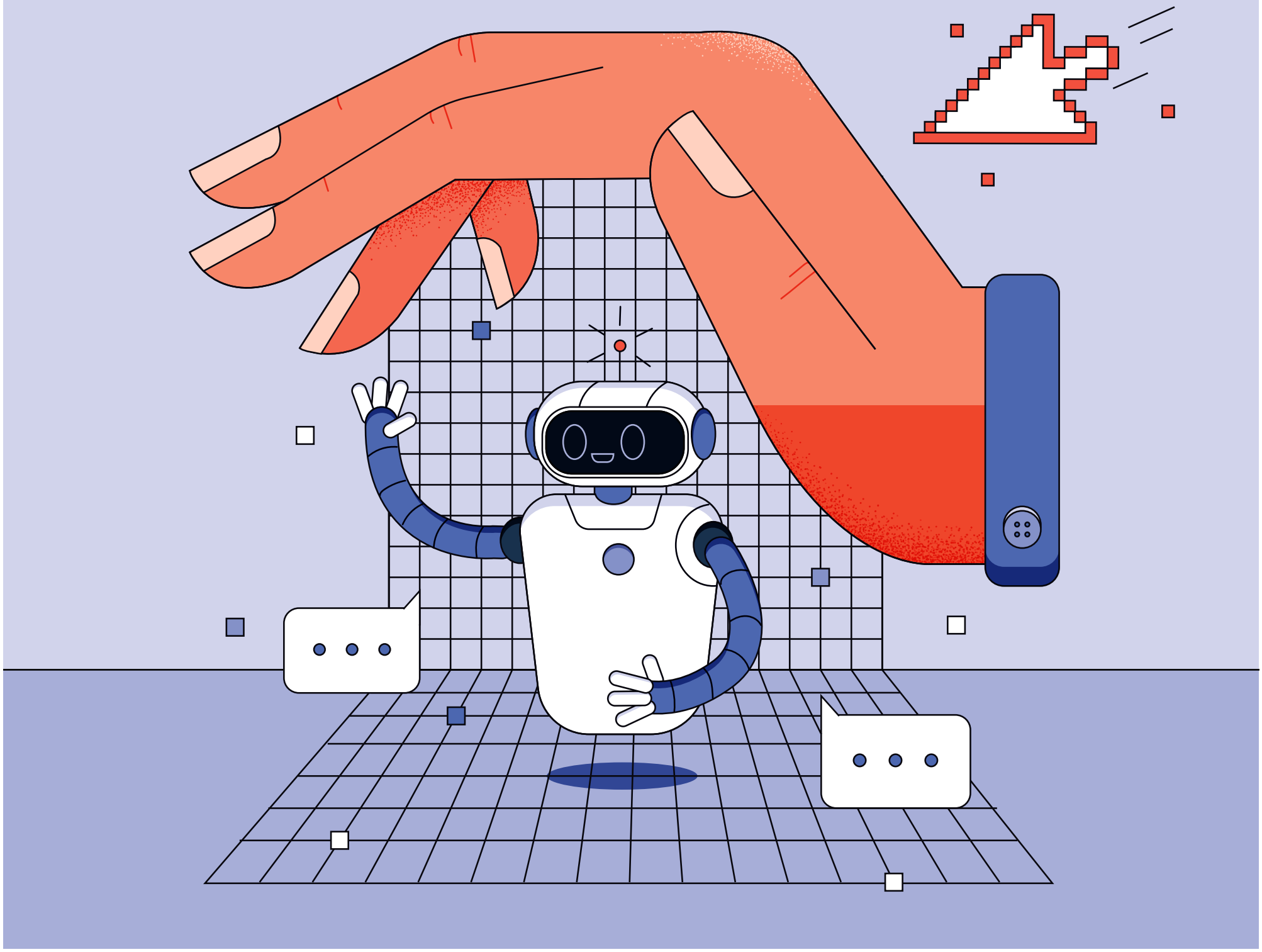
CYBERSECURITY & DIGITAL THREATS



CYBERSECURITY & DIGITAL THREATS

Distributed in
THE TIMES

In association with
Infosecurity Europe
4–6 June 2024, ExCeL London

Contributors

Jon Axworthy
A freelance journalist, specialising in health, tech, science and the future, with work published in *T3*, *Wareable* and *The Ambient*.

Tamlin Magee
Senior technology writer at Raconteur. He's interested in big ideas shaping business tech and its impact on people and society.

Morag Cuddeford-Jones
A freelance journalist with 20 years of experience covering commercial and transformation issues impacting businesses.

Mark Walsh
A New York-based freelance writer. His work has featured in *The Guardian* and *New York Magazine*.

Nick Easen
An award-winning writer and broadcaster, covering science and tech for *BBC World News* and *CNN*.

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

Raconteur

Special projects editor
Ian Deering

Contributing editor
Neil Cole

Commercial content editor
Laura Bithell

Commercial content executive
Jessica Lynn

Commercial production manager
Emily Walford

Production executive
Sabrina Severino

Design and illustration
Kellie Jerrard
Colm McDermott
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 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.

@raconteur raconteur-media @raconteur.stories

raconteur.net /cybersecurity-may-2024

POLICY

Is the government failing UK plc on cybersecurity?

Experts believe that Westminster could – and should – do far more to encourage companies of all sizes to strengthen their defences against a substantial and growing threat

Jonathan Weinberg

© Photography42/stock.adobe.com

Protecting British business from cyber attacks is not just the responsibility of CEOs and their tech chiefs. The government must also play its part – which should be more prominent, according to experts in the field.

A poll conducted on behalf of US cybersecurity firm Armis in Q4 2023 found that 52% of corporate IT decision-makers in the UK felt that their government wouldn't be able to protect its businesses and citizens adequately from an act of cyber warfare.

The government's own research, published in April 2024, revealed that half of all British businesses – and 74% of large companies – had reported a cybersecurity breach over the previous 12 months.

It's not as if policy-makers have been sitting on their hands. Later that month, for instance, the UK became the first jurisdiction to ban manufacturers from having easily guessable default passwords such as 12345 on smart devices. In 2022, the Cabinet Office published the Government Cyber Security Strategy, setting out a detailed eight-year plan to improve the public sector's resilience. The same year, the government updated the National Cyber Strategy it had previously published back in 2016.

Nonetheless, Westminster should be doing more to protect businesses and the providers of critical services, which are becoming ever more prone to attacks by "state actors". That's the view of Sabeen Malik, vice-president of global government affairs and public policy at Rapid7, a US network security specialist. She points out that these entities are "increasingly being targeted for data exfiltration, ransomware and state aggression".

Malik, a former senior tech adviser at the US Department of State, suggests that the government should "invest in providing more context-specific knowledge on why they are being targeted and pool private sector resources as a public-private partnership to provide a defined level of protection based on their risk profile".

Dr Andrea Cullen is the co-founder and CEO of Capslock, a state-backed training provider for people seeking careers in cybersecurity. Given the scale of the risk facing the private sector, she would like to see the government building on initiatives such as the community-interest company known as the UK Cyber Cluster Collaboration.

Westminster's cyber strategy "has to allocate sufficient resources – and it could benefit from the inclusion of incentives for implementing its objectives", Cullen argues. "But a strategy alone is not enough to address the complex and evolving threats this country faces. Its implementation must involve more cooperation and coordination among the stakeholders: government, business, academia and society in general. Securing buy-in at all levels is vital. This can be time-consuming, but the details are important."

Another positive step, she suggests, would be to develop an independent organisation providing "certification and advice", much like those that exist in the energy, telecoms, financial services and healthcare sectors.

Cullen acknowledges the efforts of the UK Cyber Security Council, an independent state-funded body working to boost professional standards in the sector. But she adds: "The strategy so far appears to be to sweep up the resources and capability within other organisations to deliver on objectives. It makes things difficult to navigate."

While the Armis poll indicated a general lack of faith among UK tech chiefs in the government's ability to shield their firms from an act of cyber warfare, it also found that only 27% of respondents had established a plan to address that threat, even though 56% said it was a concern.

Adam Marrè, chief information security officer at US cybersecurity firm Arctic Wolf, believes that the government should do more to encourage businesses to reinforce their defences – and quickly.

"It should incentivise the adoption of best practices and security certifications through tax incentives, enforce mandatory reporting of cyber incidents and establish baseline security standards," he says.

Marrè, a former FBI special agent who spent 12 years investigating cybercrimes, argues that the government also needs to start "fostering public-private partnerships for information-sharing, running awareness campaigns and providing financial support and consultancy services for small and medium-sized businesses".

He adds: "Investing more in cybersecurity education, workforce development and advanced R&D, as well as promoting cybersecurity insurance, would further bolster the nation's defences."

Other steps that experts have suggested the government could take include expanding the National Cyber Security Centre's mandate and stiffening the Network and Information Systems Regulations 2018 to raise standards of corporate governance, possibly by imposing greater legal burdens on directors.

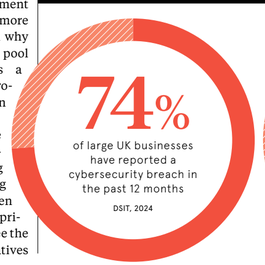
Robert Hannigan is a former GCHQ director who led the creation of the National Cyber Security Centre in 2016. Now head of international business in Europe and the Middle East for US cyber consultancy BlueVoyant, he believes that the government should take a more systematic, risk-based approach. Whenever credible threats from state actors are detected, it should react quickly by sharing clear guidance for businesses to follow.

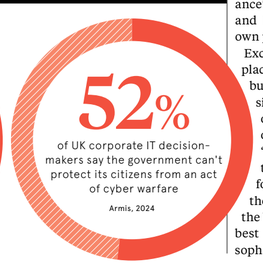
Hannigan adds that the government "can also help to identify, support and incentivise new companies that may not have attracted private sector funding but are addressing emerging challenges. Advanced work on the security of AI systems would be an obvious example."

He highlights procurement as another area where it could take positive steps. The government has significant buying power, which would enable it to mandate minimum cybersecurity standards that the many companies supplying it would have to meet.

Hannigan acknowledges that Westminster has a "difficult balance" to strike between intervening and letting businesses take their own path.

Excessive intervention would risk placing "bureaucratic burdens on businesses without achieving significant security gains, while over-detailed regulation can go out of date quickly", he notes. "But governments and regulators could enforce a baseline for security practices to help those that aren't yet addressing the basics – and then point to what best practice looks like for more sophisticated organisations." ●





Commercial feature

Q&A

Why leaders must prioritise mitigating human risk in the age of AI

The risk of artificial intelligence in the field of cybersecurity is an increasingly pressing concern. Mimecast's senior manager of product management, **Dr Kiri Addison**, explains how firms can better manage human risk in the age of AI

The human element of cyber risk is emerging as the biggest cybersecurity strategy gap in the age of AI. A Forrester report predicts that 90% of data breaches in 2024 will have a human element, up from 74% in 2023. Yet, Mimecast's 2024 *State of Email & Collaboration Security* report found that employees' ability to recognise cyber threats was a notable concern for organisations. Businesses must take a proactive approach to mitigating human risk and invest in employee training to ensure their defences are strong against cyber attacks. Dr Kiri Addison explains why it's important to remember humans remain the most likely victims of, and tool against, AI-powered cyber attacks.

Q Where does the issue of AI and cybersecurity currently sit?

A AI in cybersecurity is something that we've spoken about for a long time, but in the last couple of years, the explosion of generative AI (GenAI) and ChatGPT has really brought it back to the forefront. You've got the positive side of it, which is that it's going to have a beneficial impact on cybersecurity, but there's also the negative side.

There's a lot of talk about the negatives and what may happen in the future. But we're not necessarily seeing everything people seem to be talking about, like the vast amounts of phishing emails generated by AI or a surge of malware developed by AI.

Q What are the real and present risks?

A There was a takedown recently of a group in the UK that was reportedly using GenAI to create a vast library of phishing web page templates. Security has always been a bit of a cat and mouse game, but GenAI can assist criminals in terms of scaling up their operations, helping them evolve even more quickly.

The other trend on the rise is the use of deep fakes in cyber attacks. The technology hasn't been quite good enough to launch a serious financial attack – but now it is. There was a recent incident in Hong Kong in which criminals utilised deep fake technology via a Microsoft Teams call to persuade an employee into making a huge wire transfer using fake footage of their CFO.

We're seeing an explosion of ransomware attacks, extortion, phishing, deep fakes, all increasing alongside each other. It's all part of the same threat landscape, which was already getting more complex.

Q It's a tricky time to be a CISO. What are they looking for?

A I think it's all about risk. People don't have endless budgets, especially at the moment. So, it's making the most of the budget that you do have. A priority is understanding why your organisation would be attacked. What is that attack going to look like? How would that play out? And how likely is it to happen? You need to have a good understanding of your own organisation, but also the threat landscape as well. That's where the threat intelligence element comes into it.

Then, you need to understand your defences. What do you already have in place to address some of these risks and mitigate them? Where are the gaps that exist? And what would the impact on your organisation actually be if one of these attacks were to succeed? Once you have that information, you can prioritise and focus on the areas you've identified. This requires reliable data and information to help you take a risk-based approach.

> **Businesses must take a proactive approach to mitigating human risk and invest in employee training to ensure their defences are strong against cyber attacks**

Q Where are those risks most commonly seen?

A The human element is a significant one. Whether that's opening a malicious file or a link you've just been sent in a new collaboration tool, these actions may ultimately end up leading to a ransomware attack on the system. Or maybe you've been sent a compromised email spoofing your boss and it's asking you to respond with some sensitive data. There's a whole range of different attacks that could happen, but a lot of them require a human to be tricked into taking a certain action.

For a long time, humans have been blamed for making mistakes, but actually I think we need to look at them as a very critical part of a strong defence strategy. You can see them as a risk, but you can also see them as a control. With ongoing comprehensive training, they can recognise and be suspicious of the increasingly sophisticated attacks they will encounter. Then, you can rest assured your human firewall is all set and working. But like any tool, if it's misconfigured or not switched on properly, then it isn't going to do as good of a job. The approach that we're encouraging is to identify which individuals need the most support and tailoring your training towards that.

Q How can organisations form a comprehensive cybersecurity strategy to protect both employees and businesses?

A Mimecast offers customers an awareness training product that interacts with end users, testing their ability to recognise and avoid risks. Mimecast can help companies send out test phishing campaigns to employees to see who will interact with them positively and negatively. This identifies which employees are in need of further support to avoid falling victim to real attacks.

Being proactive, rather than reactive, is the necessary response to human risk in the age of AI. This plays into the risk-based approach: identifying your areas of weakness upfront and thinking about how you're going to prevent and also recover from this. Nothing is 100% certain, so you still have to think of the element of recovery. In the uncertainty of the AI-driven cyber threat landscape, human risk is one factor businesses can take a combative approach towards, by addressing weaknesses ahead of time and investing in regular training to help employees remain vigilant, should they encounter a threat.

Learn more at mimecast.com

Visit Mimecast at InfoSecurity Europe 2024 at Stand E55

mimecast

Commercial feature

AI and digital resilience: is cybersecurity actually getting easier?

Cyber attacks are changing on a daily basis, but many organisations are still making the same mistakes when it comes to protection. And these mistakes often come from the top

The cyberthreat landscape is rapidly evolving, and organisations can often struggle to keep up with the more sophisticated attacks that are levelled at them every day. Yet, business leaders are still failing to understand the importance of keeping systems secure.

In a recent roundtable hosted by data insights and organisational resilience firm Splunk, cybersecurity experts from different industries discussed how, despite constantly moving threats, some things never change – such as the motivation behind attacks.

"Their motivation – financial gain – is always there, and they're prepared to keep at it," says Simon Viney, cybersecurity financial services sector lead at BAE Systems Digital Intelligence. "New groups will spring up and there will be some successes from law enforcement [...] But that motivation isn't going away."

Another constant is that, no matter how advanced threats become, the targets are still similar – from compromised emails to that weak link in your supply chain. According to Mark Woods, chief technical advisor for EMEA at Splunk, "some things will just be accelerated". He says: "If you look at the common compromises, it's still most likely your business email or some low-level system being compromised, or someone being extorted, or the supply chain has messed up."

Of course, there's a lot that organisations can do to tighten up security internally and with their direct suppliers and vendors, "but the second and third-line supply chain is vitally important too", says Rigo Van den Broeck, executive vice-president in cybersecurity and innovation at Mastercard.

"Fixing that has been an increasingly important topic, both from a security perspective, but also from a compliance and regulatory perspective, because there are a lot of regulations, especially in Europe, around this in the financial industry," adds Van den Broeck.

It is not just the private sector facing these indirect threats however. Many public institutions are also at heightened risk of cyber attacks, with criminals often targeting – or operating from within – businesses further down the supply chain – in what might be called an organisation's 'soft underbelly'.

Dealing with threats

Perhaps surprisingly, recent research published by Splunk found that many people believe keeping businesses cyber-secure is actually becoming easier, with four in 10 security leaders saying cybersecurity is much or somewhat easier in 2024 than it was in the year before.

On the one hand this may reflect better technology and respondents finding it easier to identify and neutralise threats. However, on the other it's a finding that may be cause for concern, suggestive of a possible lack of understanding of threats and the levels of disruption that can be sewn across a business.

"One big issue facing organisations today is that the threat landscape continues to evolve, and technology is now so complex, it can feel impossible to find a solution that's able to deal with all of these disparate problems. This can result in companies not knowing what to do, and lead to decision paralysis in the boardroom," according to Viney.

"The challenge is you pick any [provider], even with integrations, then 18 months go by, and you need to keep on top of the constant pace of change, and redo your approach all the time. Even in large organisations, doing that effectively is a real challenge," he says.

"I'll admit it's surprising to see a suggestion that cybersecurity is trending easier over time," adds Woods. "However, it's key to understand that it's security leaders who say they're starting to find security easier. This group is most likely to have good foundations and a consolidated system in place – a company's cyber posture will clearly benefit from this."

Convincing the board

Business leaders tend to want a quick fix that will magically protect the entire organisation – one that doesn't require thinking about. But cybersecurity is something that you need to continuously iterate on, says Woods. "So, you've got a two-year transformation programme to make you more cyber resilient? Great. What happens after that? Well, the central budget suddenly disappears."

Leaders may want to shut their eyes to an increasingly complex environment, but boards ought to be given a sense of agency in protecting their organisation – and encourage this across the business. In effect, this means the chief people officer should have as much to do with cybersecurity as the chief financial officer does.

One suggestion from the roundtable was to give the board more practical solutions to help them understand the importance of cybersecurity. This may require fostering a sense of what they can do – such as increasing employee engagement so that people feel a stake in the business that they're protecting. Encouraging this level of engagement is key to keep the whole business aware of potential threats.

The AI threat

When it comes to artificial intelligence, there's a fear that generative AI tools are helping attackers stay ahead of the curve, leaving organisations scrambling to keep up. Some may feel that AI tips the scales in favour of the attacker over the defender – though some would speculate that AI has not yet been fully utilised to defend systems, or assist with governance or regulatory burdens.

One thing that would help the fight against cybercriminals using AI is greater collaboration between companies, according to Van den Broek. Without the open sharing of data, cybersecurity is limited to systems based on what comes in and out an organisation, rather than wider sets of data that can be used to create predictive defence models run by machine-learning.

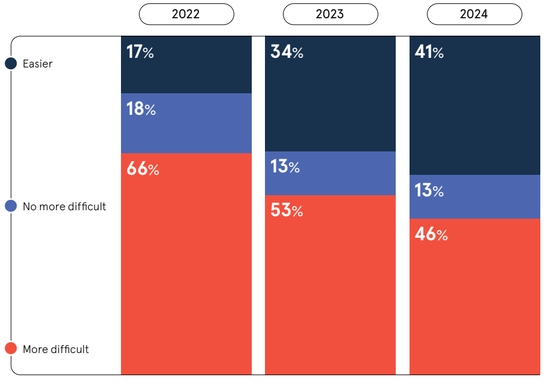
"Co-operation between industries, between companies, both public and private focused, is so crucial," concludes Van den Broek. "Because, if we don't share data on the defence side, we cannot build AI-based systems to do the defence for us."

For more information please visit splunk.com

splunk>

RESEARCH SUGGESTS SECURITY LEADERS BELIEVE CYBERSECURITY IS GETTING EASIER OVER TIME

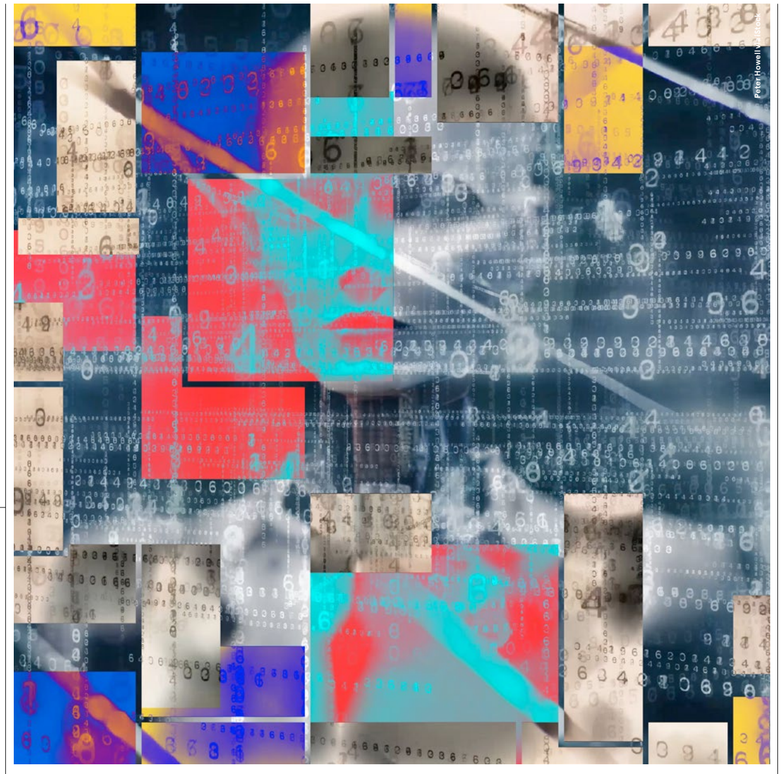
Splunk, 2024



ARTIFICIAL INTELLIGENCE

Prompt injection: AI's covert combat zone

Industry observers debate whether AI will be more useful to cyber attackers or defenders. But underlying vulnerabilities in LLMs may pose an even greater threat to organisations than AI-powered attacks



Jon Axworthy

Artificial intelligence has opened up a new frontline in cybersecurity, with the technology being used to both attack and defend corporate operations.

But while much discussion has focused on the ability of AI to fuel attacks on the one hand and bolster defences on the other, AI systems themselves could be a chink in cyber armour of UK organisations.

One in six businesses in the UK have deployed at least one AI application in their operations, according to research commissioned by the Department for Culture, Media and Sport. Such applications have unique security requirements and firms that neglect these will be vulnerable to cyber threats.

Organisations most commonly use AI in customer-service chatbots, which are underpinned by large language models (LLM) that generate humanised responses when prompted. According to Kevin Breen, director of cyber threat research at Immersive Labs, these models are particularly vulnerable to cyber attacks.

"Prompt injection is currently the most common form of attack observed against LLMs," he explains. "The focus is on tricking the model into revealing its underlying instructions or to trick the model into generating content it should not be allowed to create."

Another potential weakness stems from AI's inability to access data and information that is more current than the system's most recent training update. To counter this limitation, LLMs have an added capability to incorporate functions into the AI context through a process known as function calling.

Breen explains that accessing up-to-date weather information is a common example of such an operation. "Asking an application what the weather is like in London, for instance, will prompt the AI to tell the application what function to use and what data to send. As these functions are sent to the AI, they become part of the context."

> **Teams should realise that they're probably not starting from zero. The security tools that they already have in place can help to monitor AI applications**

Malicious users can modify the context with a prompt injection and force the AI to list all of its functions, signatures and parameters, warns Breen. "If developers aren't properly sanitising these results, this can lead to attacks like SQL injection or even code execution, if some functions are able to run code."

And, since LLMs are used to pass data to third-party applications and services, the UK's National Cyber Security Centre has warned that malicious prompt injection will become a growing source of risk in the near term.

For this reason, any business training LLMs on sensitive data such as customer records or financial information must be especially vigilant, explains Dr Peter Garraghan, a professor of computer science at Lancaster University, as well as chief executive and chief technology officer at Mindgard AI. He adds that the risks of improperly secured AI extend beyond data leakage.

"Malicious actors are able to manipulate model outputs, which can lead to incorrect decisions and biased results. This could have severe consequences in high-stakes applications such as credit scoring, medical diagnosis or content moderation."

Understanding the potential attack surface is essential. Generative AI has unique characteristics that exacerbate security challenges, according to Herain Oberoi, general manager, data and AI security, governance, compliance and privacy at Microsoft.

"Its high connectivity to data makes data security and governance more challenging than ever and its use of natural language means that the technical barrier for bad actors is lower, as a simple sentence can be used to attack AI applications. Plus, because it is non-deterministic, it is susceptible to manipulation."

Security teams must therefore ensure that their existing cybersecurity frameworks and risk management processes are extended to cover AI systems.

"Firms should include AI assets in asset inventories, data flow diagrams, threat models, red teaming, pen testing, incident response playbooks and so on," explains Garraghan. "In one sense, AI is just another software tool and incorporates a lot of standard IT thinking. But it also has very significant differences and requires specialist skills and tools to secure properly."

Security-operations teams must also treat AI security as a continuous task. This starts with an organisational culture that emphasises the importance of responsible and secure AI development and deployment, says Garraghan

"This means establishing clear policies around data handling, model testing and deployment approvals. It also means training everyone interacting with AI, from data scientists to business users, on the risks and best practices. AI security is a highly dynamic field, so continuous education is essential."

While ensuring effective security measures may seem like a daunting task, the good news is that some AI vulnerabilities might already be covered, according to Liam Mayron, staff product manager for security products at Fastly.

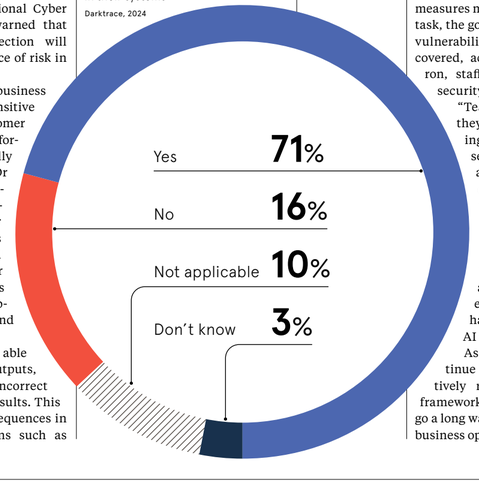
"Teams should realise that they're probably not starting from zero. Some of the security tools that they already have in place can help to monitor newly deployed LLMs and AI applications, even if they're not built for it," Mayron adds. "The key is to ensure and verify that these existing security tools have visibility into your AI applications."

As these applications continue to proliferate, proactively reviewing the security frameworks that protect them will go a long way towards safeguarding business operations.

DON'T NEGLECT CYBERSECURITY IN THE RUSH TO IMPLEMENT AI

Share of firms that have taken steps to reduce the cyber risk of using AI in their systems

Darktrace, 2024



SUPPLY CHAIN

Supply and ransom demand

Cyber criminals are increasingly gaining access to protected data via third-party suppliers. Businesses and their supply chain partners must remain vigilant

Morag Cuddeford-Jones

First there were viruses, trojans and worms; then, ransomware and phishing. It would appear that there is no limit to the creativity of hackers intent on infiltrating institutions.

And, while well-resourced organisations may be able to adapt their security frameworks to combat direct attacks, cyber criminals have identified potential weak links in third-party partners.

Cyberattacks originating in the supply chain increased by 68% in 2023 and now account for 15% of reported breaches, according to Verizon's most recent *Data Breach Investigations Report*.

The race to modernise operations has led more businesses to develop software-based supply chains, while budgetary pressure encourages firms to outsource a greater share of services. But more outsourcing inevitably means less direct oversight of security practices.

It's a point made by Chris Novak, managing director of Verizon's Threat Research Advisory Center and advisor to President Joe Biden's Cyber Safety Review Board. "As businesses outsource more and more services to third-party organisations, they increase the potential attack surface that threat actors can exploit."

And, in the race to stay ahead of the competition, it's all too easy for security precautions to fall by the wayside. Tayo Dada, head of cybersecurity and international professional investigator at Conflict International, warns: "We are hyper-connected and there are a multitude of vendors. We are very reliant on them, so when we see some 'best-of-breed' software, available off the shelf, it can be tempting to subscribe without considering all of the potential risks."

Dada adds that no one is immune. Alluding to the 2020 SolarWinds supply chain attack, he admits that even he, a cybersecurity expert, used the company's software as a remote management and monitoring platform. Quite simply, he says, "we need to be a lot more wary".

Private sector organisations could learn from the UK's public sector, where there is considerable pressure to maintain a 'gold-standard' approach to supply chain security.

Since 2014, the government has required all partners and suppliers bidding for contracts involving the handling of sensitive information to be certified through the Cyber Essentials scheme.

Although certification does not guarantee that every vulnerability has been addressed or even identified, it provides companies with a minimum-standard framework to guard against the most common digital security threats.

Jude McCorry, CEO of the Cyber and Fraud Centre – Scotland, a non-profit, says this certification is only a starting point when considering partners and suppliers.

Getty Images via iStock

> **As businesses outsource more and more services to third parties, they increase the potential attack surface that threat actors can exploit**

"We then send out a questionnaire asking, for instance, how often they do security training and whether there is an incident-response plan in place," she explains. "The last thing we want is to have a cyber attack originate from someone that we've given money to."

But despite these safeguards, firms must accept that there is no such thing as total security. "Organisations currently spend an average of 55 days patching 50% of their critical vulnerabilities," Novak reveals. "This means that, after almost two months, they are only about halfway towards fixing their issues. Compare this to threat actors, where the typical time to develop exploit code and attack is about five days."

Dada acknowledges that investment in cybersecurity is viewed by many as a cost rather than a value-add. So when it comes to securing clients in a highly competitive market where every penny matters, it can be tempting to take shortcuts.

Cyber Essentials certification, for instance, can be granted with external verification but can also be gained through a self-assessment. Suppliers could complete a self-assessment as a tick-box exercise to appear compliant because it will help them to secure the contract.

"You have to start somewhere," McCorry says. "Plus, it's not that easy to fill out the questionnaire. If you're a small company, you'll probably need someone to help you with it."

Moreover, while the Cyber Essentials scheme does not guarantee absolute security, it does indicate a supplier's dedication to cyber hygiene. McCorry adds, however, that she still wants to see that a partner is making additional investments on top of their certification.

"Healthy paranoia" is the first step to avoiding exposure to critical vulnerabilities, she says. Purchasers of software, or software-enabled suppliers, must be willing to put their vendors under scrutiny – and it's not a quick process.

Martyn Wallace is chief digital officer at the Digital Office, which supports the digital transformation of Scottish local authorities. In 2025, analogue telephone services will be switched off in Scotland, but healthcare providers must ensure continuity of telecare.

He explains the rigmarole surrounding the transition to digital care services: "The Digital Office, the Scottish Government, Digital Health, Digital Health and Care Directorate, Technology Enabled Care and others have worked on a collaboration for the past six years. We have taken two years to purchase a contract for a shared alarm receiving centre. A massive part of that was due diligence on the cyber-security risk and cyber credentials."

Procuring mobile devices was especially problematic as these tend to be particularly vulnerable to breaches. Wallace recalls one supplier who suggested that their products were secure because a special screwdriver was needed to access the devices. "People who make devices have to step up their game," he insists.

Once a company falls victim to an attack, how badly they're hit depends on their level of preparation. Wallace suggests that companies should conduct a 'pre-mortem'. This means "determining the absolute worst that could happen and identifying steps that could be taken now to prevent it."

Novak agrees: "Implementing processes such as cyber risk quantification (CRQ) can help. There is a risk scoring system against potential avenues of attack, including physical devices as well as cloud environments and applications. Security teams can use the estimated costs generated by CRQ to prioritise fixing flaws based on the potential damage that could be inflicted, rather than attempting to patch hundreds of vulnerabilities at the same time."

Understanding and managing the vulnerabilities in your supply chain, then, is less like building a fortress around your business and more like putting your finger in the dam. You can't protect against every eventuality, but with uncompromising standards and a robust due diligence process you can stop the dam from bursting.

71%

of small businesses have not been asked to prove their cyber posture by supply chain partners in the past 12 months

54%

of organisations have insufficient visibility into the vulnerabilities in their supply chain

41%

of firms that suffered a material impact from a cyber attack say that it originated from a third-party partner

World Economic Forum, 2024

Commercial feature

Breaking down barriers: transforming data security in the cloud

Without a unified approach to security, organisations will struggle to reap the benefits of the data revolution

Data is revolutionising how businesses operate, enabling them to better understand their customers, achieve operational efficiencies, and drive innovation and growth.

Yet the sheer amount of data present within organisations can make it extremely challenging to track and manage – a problem complicated by the fact data is often locked in silos and scattered between channels, cloud apps and internal systems. Redundant, obsolete, or trivial data (otherwise known as ROT) can account for up to 80 percent of an organisation's data lingering on systems, presenting an unknown level of hidden risk.

Not surprisingly, many companies struggle to unlock the full power of their data, meaning investments go to waste and opportunity costs are incurred. More worryingly, poor data security governance makes it harder to remain compliant in an increasingly complex regulatory landscape, or defend against data breaches which can lead to serious financial costs and reputational damage.

So how can companies protect their data "in the wild" and make comprehensive data security the business imperative it should be?

Visibility is key

In an ideal world, firms would have full visibility over their data in order to mitigate risks and gain the insights they need, says Karl Triebes, who is chief product officer at Forcepoint, a market leader in the data security space. In reality, insufficient personnel, time constraints, high costs and other barriers make safeguarding data tougher than ever.

"Many companies are at a point where they are working harder but not necessarily smarter to stay safe," Triebes says. "Security leaders are doing the right thing but getting poor results, which isn't an option when it comes to data security."

Part of the problem is that the average company deploys between 50 and 75 cyber technologies at any given time, which all need to integrate well to be successful. But when managing so many technologies this is rarely the case, leading to frustrating false positives and error-ridden reporting.

Firms need large data teams with varying specialties to manage so many conflicting technologies, and that requires significant investment.

> **The shift toward hybrid and remote work has become the new normal, requiring a fresh approach to cybersecurity that prioritises data security wherever it resides**

"With privacy regulations now covering more than 70% of the world, enterprises are under increasing pressure to enhance security measures," says Triebes. "But their data teams face a near-impossible task in ensuring the myriad technologies in play remain compliant as each new version or reversion is launched."

Unified approach

The fact that data breaches – both intentional and accidental – are becoming more common only compounds the problem. Sensitive company data is increasingly managed by third parties in the cloud, expanding the attack surface faced by organisations. And the rise of remote working means data is now regularly accessed outside the office on unmanaged and personal devices, further increasing the risks.

"Dispersed teams are working from anywhere with data everywhere, but not always safely – especially as new and unknown technologies come into play," says Triebes. "The shift toward hybrid and remote work has become the new normal, requiring a fresh approach to cybersecurity that prioritises data security wherever it resides."

Firms must adopt a unified approach to data security to simplify the task of securing their workforces beyond office premises, prioritising data security irrespective of its location. This in turn will help security leaders prevent breaches and simplify compliance by safeguarding information wherever people work, access and use sensitive data.

Yet many conventional data security tools fail to offer a truly unified approach, because they do not account for the contextual significance of business data, meaning potential security gaps remain.

'Data security everywhere'

Forcepoint helps organisations overcome this problem with a "data security everywhere" approach that protects sensitive company data wherever it resides. The firm, which supports 12,000 businesses around the world, across multiple industries, recently launched two new solutions that are transforming the way organisations deal with data blind spots.

The Forcepoint Data Security Posture Management (DSPM) solution uses artificial intelligence to deliver real-time visibility, ease privacy compliance and minimise risk for data stored across cloud applications or on premises.

It finds and identifies whether data such as personally identifiable information (PII) or health records are stored in an organisation's network folders, cloud directories and devices, then classifies and catalogues that data based on user parameters.

"Forcepoint DSPM allows users to find and prioritise the most important vulnerabilities in their data while gaining real-time insights," says Triebes.

"The contextual awareness garnered allows security leaders to be both proactive and reactive to eliminate the risk, depending on what makes the most sense for the business. Risk remediation is truly one of the elements of Forcepoint DSPM that makes it so unique – and this wouldn't be possible without AI."

Forcepoint ONE Data Security meanwhile is a fully cloud-native data loss prevention solution that provides unified security management, helping organisations simplify security. It covers key channels including cloud applications, web, email and endpoints, while providing a single dashboard to see all data and a single security policy to protect it all.

It also offers more than 1,700 predefined policies, templates and classifiers to streamline companies' compliance efforts globally, making it easier to navigate regulatory risk.

This unified approach to data security management eliminates many of the headaches and potential gaps that security leaders face with legacy solutions, says Triebes. It also cuts costs, with Forcepoint customers typically achieving efficiency savings of up to 31% by reducing complexity and improving productivity.

"In a world where everything is connected yet everyone is dispersed, there has never been a more opportune or critical time to safeguard sensitive data," he concludes. "By executing a comprehensive Data Security Everywhere strategy, firms, regardless of size or industry, can truly safeguard the usage of data wherever it resides."

For more information please visit forcepoint.com

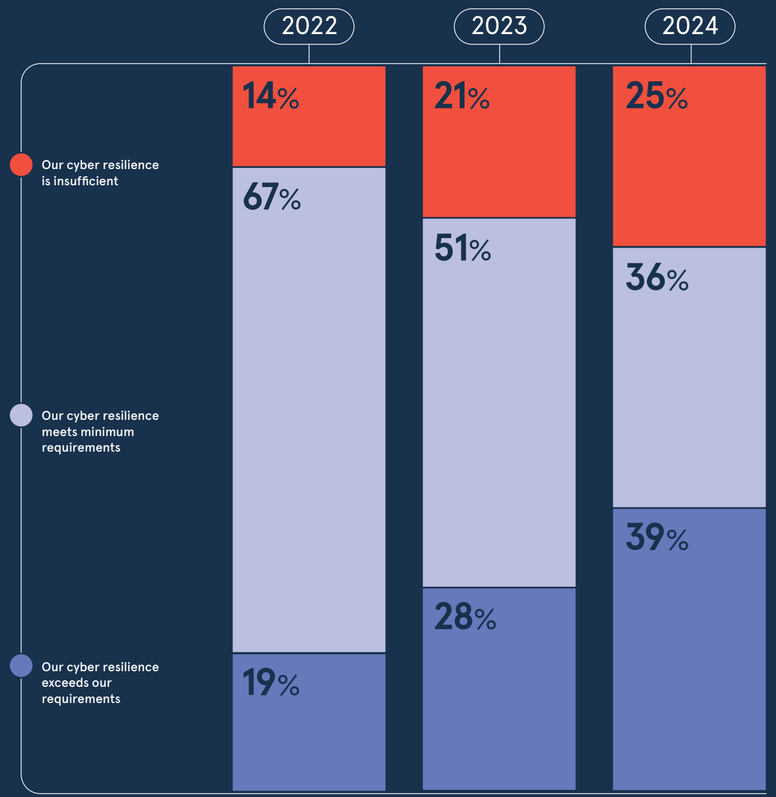
Forcepoint

CYBER INEQUALITY

Large organisations are much better prepared for cyber attacks than smaller organisations – and the gap between them has grown considerably over the past two years. Low-revenue organisations are more than twice as likely as high-revenue firms to say that their cyber resilience is insufficient. Smaller enterprises are far less likely to be covered by cyber insurance than large enterprises and they're also bearing the brunt of the cyber skills gaps. While 95% of high-revenue businesses say that they have the necesary skills to achieve their cybersecurity goals, only 49% of low-revenue firms say the same

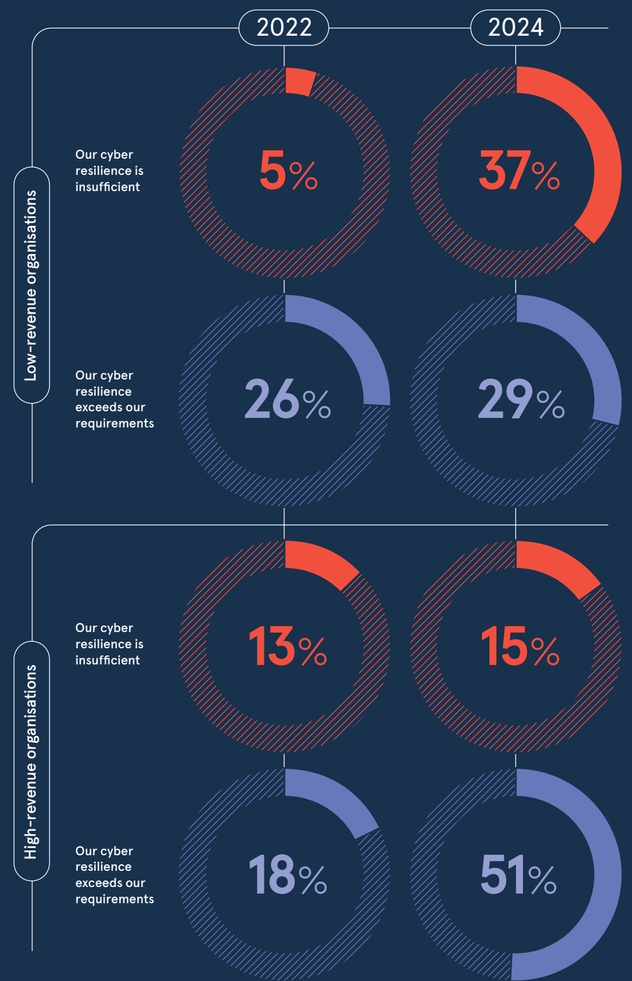
FIRMS ARE FEELING INCREASINGLY VULNERABLE TO CYBER THREATS

Organisations' evalutation of their cyber resilience



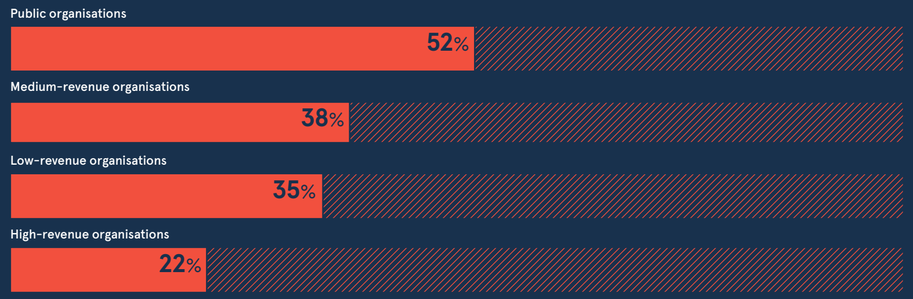
LOW-REVENUE ORGANISATIONS ARE PARTICULARLY UNPREPARED FOR CYBER ATTACKS

Organisations' evalutation of their cyber resilience, by company size



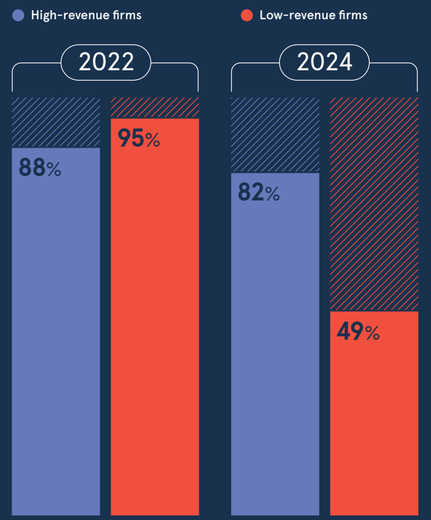
MANY ORGANISATIONS SAY SKILLS AND RESOURCES ARE THE GREATEST BARRIER TO CYBER RESILIENCE

Organisations reporting that skills or resources are their biggest barrier to achieving cyber resilience



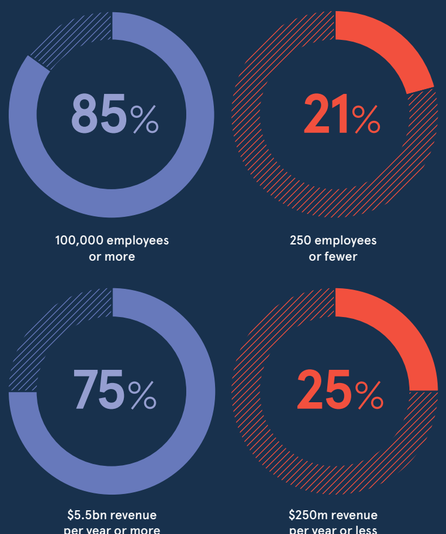
BUT LARGER FIRMS ARE LESS IMPACTED BY CYBERSECURITY SKILLS GAPS

Share of organisations reporting that they have the skills necessary to achieve cybersecurity goals



LARGE ENTERPRISES ARE ALSO MORE LIKELY TO BE PROTECTED BY CYBER INSURANCE

Share of organisations with cyber insurance, by company size



World Economic Forum, 2024

Charday Penn via iStock

DATA PROTECTION

Wide-open source: how to train and protect LLMs

The models being used to train GenAI systems can leave data exposed to cybercriminals. How can corporate users best protect the sensitive information they hold?

Nick Easen

Foundation models, the bedrock of the much-hyped tool that is generative AI, are data-hungry. If businesses want to differentiate themselves, they must feed these models with proprietary information, including customer and corporate data. But doing so can expose this sensitive material to the outside world – and the bad actors operating in it – potentially contravening the General Data Protection Regulation in the process.

Dr Sharon Richardson, technical director and AI lead at engineering firm Hoare Lea, sums up the situation: "From day one, these models were a very different beast from a security standpoint. It's hard to bake security into the neural network itself because its strength comes from hoovering up millions of documents. This is not a problem we've solved yet."

The Open Worldwide Application Security Project, a not-for-profit foundation working to improve cybersecurity, cites data leakage as one of the most significant threats to the large language models (LLMs) on which most GenAI tech is based. This risk drew considerable public attention last year when employees at Samsung accidentally released sensitive corporate information via ChatGPT.

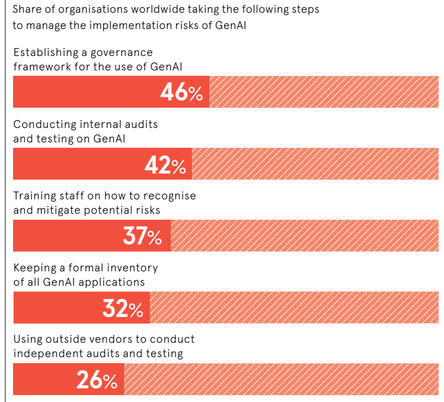
The task of safeguarding the data being used takes on a new meaning with the latest GenAI tools, since it's hard to control how the information is processed. Training data can get exposed as these systems work to organise unstructured material. It's why some businesses are focusing their efforts on securing inputs. Swiss menswear company TBô, for instance, carefully labels and anonymises information on customers before feeding this into its model.

"You want to ensure that your AI doesn't know things it's not supposed to know," advises Allan Perrottet, the firm's co-founder. "If you don't prepare your data properly and just throw it straight at OpenAI, Gemini or any of these tools, you're going to have issues."

> **For a brief moment, data can be sitting on a server outside your control, which is a potential security breach**

WHAT STEPS ARE FIRMS TAKING TO PROTECT THEIR AI TOOLS?

Share of organisations worldwide taking the following steps to manage the implementation risks of GenAI



Deloitte, 2024

Smart organisations are taking a multi-pronged approach to managing the risk. One measure is permissions-based access for specific GenAI tools, under which only certain people are authorised to view classified data outputs. Another control is differential privacy, a statistical technique that allows the sharing of aggregated data while protecting individual privacy. And then there is the feeding of pseudonymised, encrypted or synthetic data into models, with tools that can randomise data sets effectively.

Data minimisation is vital, stresses Pete Ansell, chief technology officer at IT consultancy Privacy Culture.

"Never push more data into the large language model than you need to," he advises. "If you don't have really mature data-management processes, you won't know what you're sending to the model."

Understanding the attack surface that an LLM might expose is also important, which is why retrieval-augmented generation (RAG) is growing in popularity. This is a process in which LLMs reference authoritative data that sits outside the training sources before generating a response.

RAG users don't share vast amounts of raw data with the model itself. Access is via a secure vector database – a specialised storage system for multi-dimensional data. A RAG system will retrieve sensitive information only when it's relevant to a query; it won't hoover up countless data points.

"RAG is really good from the perspectives of both data security and intellectual property protection, since the business retains the data and the library of information the LLM is referencing," Ansell says. "It's a double win, ensuring that your strategic assets are kept closer to home."

But he adds that "best practice around identifiable personal information and cybersecurity should also apply to business-level data".

Such techniques don't just protect sensitive material from cybercriminals. They also enable businesses to lift and shift learning from one LLM to another since, in practice, it's not possible to trace the data back to its original source.

There is no doubt that data security problems posed by the training of LLMs are linked to data maturity and managing information assets with the utmost integrity. In many ways, the issues surrounding GenAI are like the challenges of GDPR compliance on steroids.

"If GDPR's the big stick, the race to utilise AI is a big carrot," Ansell says.

Other measures that a business can take to improve its AI-related data security include creating a multi-disciplinary steering group, conducting impact assessments, providing AI awareness training and keeping humans in the loop on all aspects of model development.

One of the biggest challenges facing the sector is that sensitive corporate data still has to leave localised servers and be processed in the cloud at data centres owned by one of the tech giants, which control most of the popular AI tools.

"For a brief moment, data can be sitting on a server outside your control, which is a potential security breach. There's still a weakness there," Richardson says. "The reality is that we're still in the Wild West phase when it comes to GenAI. There will be unintended consequences. You may think that you've got it all under control, but you probably haven't."

This is why open-source models are becoming increasingly popular. They enable IT teams to externally audit LLMs, identify security flaws and have them rectified by a trusted developer community.

Yash Raj Shrestha, assistant professor in the department of information systems at the University of Lausanne, argues that open-source AI is "more secure and trustworthy than closed-source AI. That's because, when things are open, a large number of people can work together to find bugs, which can then be fixed. It's the future." ●

INSIGHT

'It's a learning and development experience for everyone'

Vicky Aitken, conference manager, Infosecurity Europe, highlights key themes for this year's event and explains why there's no substitute for in-person knowledge sharing

From 4 to 6 June, cybersecurity professionals will gather at Infosecurity Europe's annual conference in London to share their experiences and hear insights from some of the leading voices in the industry.

The themes for this year's event are inspired by a 2024 research report compiled by the Infosecurity Group, highlighting the obstacles and opportunities presented by a rapidly evolving technology landscape. The research surveyed more than 200 security professionals and revealed five key challenges: coming to terms with AI, maintaining cyber resilience, managing staff workloads and combatting burnout, compliance with incoming legislation and preparing for future digital threats.

These topics, plus countless others, will be covered from all angles across nine stages at the conference.

The keynote stage kicks off each day with a celebrity speaker. Henry Ajder will cover the latest in generative AI and the dangers of deepfakes; Jake Humphrey and Damian Hughes will explain what security leaders can learn from their High Performance podcast; and Claire Williams, of Formula 1 fame, will explore the challenges of leading a vast workforce and provide pointers on embedding cybersecurity into your company's culture.

Other centre-stage speakers will be discussing, among other topics, whether or not to pay ransom demand, developments in cyber insurance, crisis management in the event of a breach and how firms of all sizes can best prepare for legislation including the NIS2 directive.

In addition to everything happening on the main stage, we'll also have areas devoted to startups and technological innovation, as well as a lot of practical workshops and roundtable discussions; and, of course, a bustling exhibition hall.

There will be some exciting new presentations this year, too. We're thrilled to have moved Stephanie Hare's discussion on women in the cyber industry to the main stage. This topic was originally slated for the South Gallery, but was given a keynote slot because of high levels of interest among attendees. It's encouraging that so many in the industry are taking issues relating to diversity and inclusion seriously.

Also new this year, we will be organising some analyst sessions with business consultancy Frost & Sullivan and have partnered with non-profit Every Child Online to bring awareness to the problem of digital exclusion.

And that's really why events such as Infosecurity Europe exist: to bring awareness to the problems facing this industry and provide a space in which the ideas and experiences of those on the frontline can be shared. It's a learning and development experience for everyone.

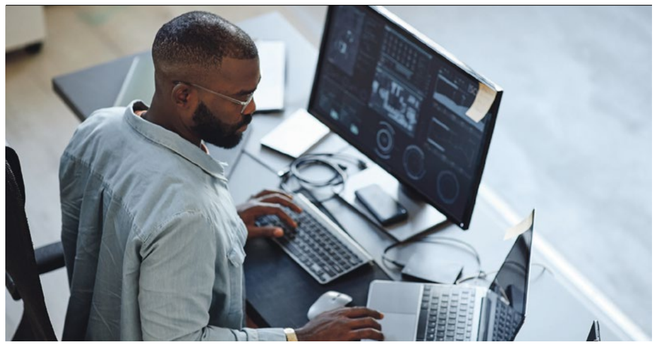
In many ways we're still feeling the effects of Covid lockdowns, which forced the cancellation of all these events and massively limited interactions among industry peers. We have some catching up to do. Considering how quickly things evolve in this industry, it is essential that we create these knowledge-sharing opportunities again – and that cybersecurity professionals take advantage of them.

Everyone is very busy. But there's tremendous value in getting out there, interacting with others and learning from one another's experiences. There really is no substitute for that in-person interaction.

The variety and expertise on display at Infosecurity Europe, the chance to build your network, the first-hand learning experiences; these are invaluable for cybersecurity professionals, who are running to keep pace with the changes in the industry. We're very confident that our attendees will come away from this conference with a better understanding of how to do their job. ●

Vicky Aitken
Conference manager
Infosecurity Europe

Commercial feature



CISO priorities must shift in a heightened threat landscape

Having a more nimble response to cybersecurity issues as they arise is becoming vital – but how do you do that safely?

For chief information security officers (CISOs), the world is looking increasingly dangerous. The cyber threat landscape appears less secure than ever – putting the onus on CISOs to try and step in to shore up defences. "The cost of the attacker to compromise you is going down," says Rob Demain, CEO and founder of e2e-assure, Threat Detection and Response Specialists. "The adoption of new tech has meant that it's less expensive for attackers," he says. "When it's less expensive, that broadens the targets, which means more people are brought to the attention of hackers."

Those overseeing their organisation's cybersecurity are well aware of the risks, but they're also conscious that their investment and security often can't keep up. In all, 42% of cybersecurity decision-makers said their operations were underperforming, according to a recent e2e-assure survey.

The problem is often that security professionals agreed security operations centre-as-a-service (SOC-as-a-service) contracts with service providers years ago when cybersecurity became a risk. Those initial agreements, which often lock in customers for years at a time, were ill-suited to adapt to the changing security environment. "What's happening is that attackers are moving quicker," says Demain. "They're using attacks in different areas. And a lot of organisations are finding that they aren't prepared for that in terms of the outsourcing arrangements, which are quite inflexible."

> **The cyber threat landscape appears less secure than ever – putting the onus on CISOs to try and step in to shore up defences**

This gap between what CISOs need and what they can currently access is exemplified by e2e-assure's 2024 threat detection research, which shows CISOs are seeking greater speed, more control and better resilience as the main priorities they look for in a provider. The problem is that existing SOC-as-a-service providers often don't offer those key components that businesses now seek out. "Traditionally, it can be slow," says Demain. This, naturally, causes frustration among decision-makers.

Beyond that, the way that SOC-as-a-service traditionally works is to be reactive, rather than proactive, in defending organisations from cyber incursions. Demain compares it to a fire alarm, where outsourced providers usually inform customers that they're being attacked, but don't always explain what to do about it. "It's very much a passive arrangement this way," he says. At the point at which an organisation is attacked, it's arguably too late to do anything about it – something CISOs who find themselves falling victim are increasingly conscious of.

"A lot of traditional services function by responding to the actual encryption or the ransomware events," Demain says. That's far too late to make a meaningful difference. "By the time that's happened, it's too late to fix it. So, what we should be doing is looking for the spark, which is what we call initial access techniques," he says. "What we try to focus on is detecting the early stages of attacks. It's much easier to take action to stop them at that stage."

A proactive approach is what e2e-assure offers its customers. Rather than locking in businesses to long-term, inflexible contracts, the company offers flexible, agile contracts suitable for the modern workplace. The firm also offers modular services that can be adapted to a business's needs, rather than what the provider wants to sell them. "Change costs a lot of money," says Demain, and e2e-assure's modular approach means it's possible to do so without breaking the bank. The company works with clients to assess their specific needs and develop a solution that works for them and their requirements.

And rather than being impenetrable, e2e-assure offers its automated, always-on security operations in a way that is simple to understand, with a dashboard available through its Microsoft Teams app. This easily allows businesses to review, respond and remediate any issues that may arise. Having a continuous security assessment can make the difference between keeping your business secure, says Demain, or falling victim to the latest cyber attack.

"CISOs need to be in control," says Demain. "It's their business they're protecting. They can keep in touch with us, but they want to be informed and have authority over decisions that impact the safety of their business."

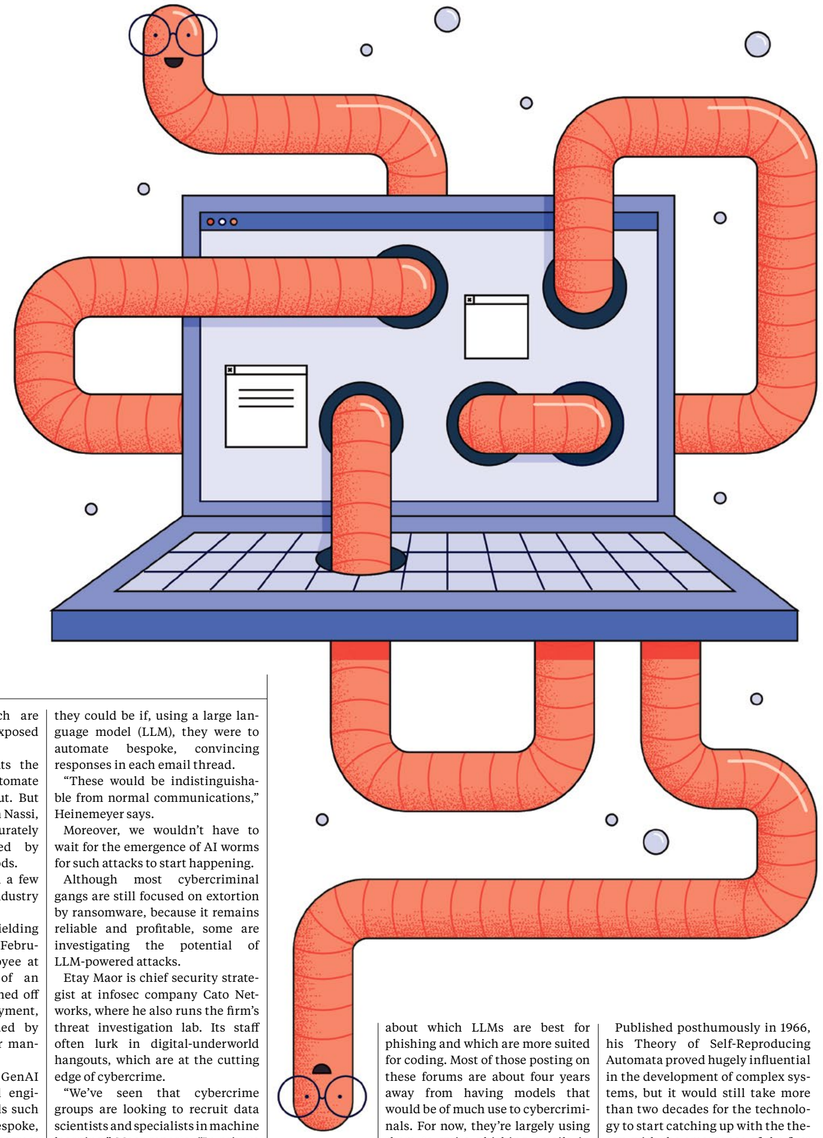
For more information please visit e2e-assure.com

e2e — assure —

MALWARE

The worm that turned intelligent

An eye-opening experiment introducing Morris II, a proof-of-concept worm, shows that corporate cybersecurity teams must become vigilant for AI-powered versions of classic attack methods



Tamlin Magee

The appearance of the first computer worms was a watershed in the history of cybersecurity. Unlike traditional viruses, they could replicate themselves, spreading their digital larvae across networks without human assistance. From the primordial worms of the internet's formative years, such as Morris in 1988, to the ransomware cryptoworm WannaCry nearly three decades later, this sneaky genus of malware has left a trail of destruction in its tracks.

Innovations in wormery often appear in tandem with new technologies. And so it has happened with the dawn of democratised AI. Named after its ground-breaking forebear, Morris II is a new worm that uses generative AI to clone itself and proliferate.

An experiment by researchers from Intuit, Cornell Tech and the Technion Israel Institute of Technology recently enlisted Morris II to use so-called poison prompts to break the defences of email assistants powered by GenAI. Emails stuffed with these poison prompts caused the assistants to comply with their commands.

The prompts compelled them to send spam to other recipients and exfiltrate personal data from their targets. They then cloned themselves to other AI assistant clients, which mounted similar attacks.

The researchers hope that their proof-of-concept worm will serve as a warning that might prevent the appearance of similar species in the wild. They have alerted the developers of the three GenAI models they'd successfully targeted, which are working to patch the flaws exposed by Morris II.

This experiment highlights the potential of AI systems to automate attacks without human input. But one of the researchers, Dr Ben Nassi, suggests it's too soon to accurately estimate the threat posed by GenAI-powered attack methods.

"I believe we'll find out in a few years, based on how the industry reacts," he says.

Criminals are already wielding other AI-aided weapons. In February, for instance, an employee at the Hong Kong branch of an unnamed multinational signed off a fraudulent £20m scam payment, believing instructions issued by deepfake imitations of their managers via a video call.

Fraudsters are also using GenAI to supercharge their social engineering attempts, using tools such as ChatGPT to create more bespoke, targeted and grammatically correct phishing emails.

Max Heinemeyer, chief product officer at cybersecurity firm Darktrace, believes that the use of AI to develop existing attack methods and scale them up will continue, but he adds that GenAI is still too erratic to be relied upon by criminals.

Picture a scenario where hackers gain access to an email server and hijack email threads by posing as a recipient or a sender. They then attach a convincingly disguised PDF file containing malware.

Hackers are actually doing this sort of thing already, but now imagine how much more effective they could be if, using a large language model (LLM), they were to automate bespoke, convincing responses in each email thread.

"These would be indistinguishable from normal communications," Heinemeyer says.

Moreover, we wouldn't have to wait for the emergence of AI worms for such attacks to start happening.

Although most cybercriminal gangs are still focused on extortion by ransomware, because it remains reliable and profitable, some are investigating the potential of LLM-powered attacks.

Etay Maor is chief security strategist at infosec company Cato Networks, where he also runs the firm's threat investigation lab. Its staff often lurk in digital-underworld hangouts, which are at the cutting edge of cybercrime.

"We've seen that cybercrime groups are looking to recruit data scientists and specialists in machine learning," Maor reports. "In private channels, they've mentioned creating their own malicious LLMs."

His team members have read discussions on Russian hacking forums about which LLMs are best for phishing and which are more suited for coding. Most of those posting on these forums are about four years away from having models that would be of much use to cybercriminals. For now, they're largely using them to write phishing emails in languages they don't know.

> **Cybercriminals are prioritising the lower-hanging fruit for now, but they're definitely looking into scaling up**

While Maor hasn't yet seen self-governing, self-replicating malware that criminals can just "fire and forget", he warns that they "are trying to get there. They're prioritising the lower-hanging fruit for now, but they're definitely looking into scaling up."

While lecturing in the late 1940s, pioneering mathematician John von Neumann led a thought experiment about self-replicating technology. What would it take, he wondered, to create a machine that could reproduce and evolve like humans do?

Published posthumously in 1966, his Theory of Self-Reproducing Automata proved hugely influential in the development of complex systems, but it would still take more than two decades for the technology to start catching up with the theory, with the emergence of the first computer worms.

It would also require a lot of R&D work to create an aggressive, autonomous AI worm that works in a repeatable way. If cybercriminals are content with their current hacking armoury, they probably lack the incentive to dedicate the necessary time, effort and resources. Furthermore, Heinemeyer notes, anyone letting loose such a beast would be targeted by every law enforcement agency in the world, which is what happened when the WannaCry and NotPetya cryptoworms were unleashed.

Malware of this type would therefore be more likely to originate from state-sponsored groups waging international cyber warfare.

"I'm sure that nation-state actors could cook AI worms up in a lab behind closed doors. They might have done so already – I think all the ingredients are in place," he says. "But, if you pull the trigger on this kind of weapon, you can do it only once. Once it's out in the wild, people will immunise themselves against it by creating counter technologies."

> **If you pull the trigger on this kind of weapon you can do it only once. People will immunise themselves against it**

Early proof-of-concepts such as Morris II, indicating the devastating potential of more advanced weapons to come, highlight the importance of looking ahead. Intelligent malicious worms would seem a logical next step, especially given the increasing sophistication and availability of AI tooling and the growing professionalisation of the cybercriminal underworld.

Businesses must therefore keep track of the emergence of new attack models – and, perhaps even more crucially, adopt a more proactive approach to combatting them.

Heinemeyer argues that corporate cybersecurity teams should prioritise reducing the attack surface, returning to the "people, processes and technology" framework to prepare for the unexpected.

"I think it would do us good as an industry to not just focus on that Whac-A-Mole game and start shifting more activity towards anticipating attacks before they happen," he says.

Dr Jason Nurse, reader in cybersecurity at the University of Kent, suggests that organisations should proceed cautiously with their own AI implementations.

"AI has immense potential but, like any other technology, it needs the appropriate review and assessment as it relates to cyber risk," he says, recommending the US National Security Agency's recent guidance on secure AI (see panel, p13) as "a good place to start. It centres thinking about the deployment environment, continuously protecting the AI system and securing AI operations and maintenance."

Thankfully, the descent into a William Gibson-esque dystopia where autonomous worms stalk their victims in cyberspace is unlikely, but such AI-powered malware could surface sooner than you'd think. A friendly garden worm will tend to bury its head in the sand, but that doesn't mean that we should.

The US National Security Agency's guidance on secure AI usage

Manage deployment governance
Any organisation deploying or operating AI should work closely with the IT function to identify the deployment environment and ensure that it meets security requirements. It should ask the developer of the AI system to provide a threat model and use this as a guide to implement best practices, assess potential threats and plan mitigation strategies. All teams, but especially cyber and data departments, should be empowered to raise concerns.

Ensure a robust deployment environment architecture
Security protections should be established as boundaries between the IT environment and the AI system. Teams should identify and address blind spots in these protections using the AI threat model as a guide. Identify and protect any proprietary data sources organisations plan to use in model training or fine-tuning – and examine the list of data sources when available for models trained by others.

Harden deployment configuration
All security best practices apply to AI too. For example, sandbox your environment running machine learning models with containers and virtual machines. Continuously review and patch hardware and software updates. Secure sensitive AI information such as outputs and logs by encrypting this data and placing the encryption keys in secure physical storage.

Commercial feature

Beyond the blind spots: why CISOs must embrace deep observability

An increasingly complex digital environment poses risks to CISOs that must secure data and networks. Zero trust and deep observability offer resilient solutions against new and complex cyber threats

Cyber attacks are increasing, and despite global infosecurity spending expected to reach a projected $215 billion in 2024 according to Gartner, organisations are losing ground in the security arms race to threat actors. Cybercriminals are spending more time hidden on corporate networks, and pressure is growing on CISOs to ensure the security of hybrid cloud infrastructure and organisational data.

Failure to secure an organisation can have devastating consequences, with a host of operational, financial, regulatory, reputational, and legal ramifications. At the same time, CISOs are faced with managing huge volumes of data traffic, a proliferation of endpoints, many of which are 'un-managed', and an increasingly complex hybrid cloud IT environment. This is all alongside managing cost reductions. It's no surprise that cybersecurity is now a core boardroom topic.

In addition to economic and environmental pressures, new regulations around disclosure and minimum-security standards are bringing accountability to the cybersecurity debate. New regulations assign personal responsibility to those at the top of a business for mitigating a breach. Executives have even faced legal charges for failure to report high-profile data breaches in the United States.

As such, boards are seeking reassurances from the CISO: how secure is our organisation? What are we doing as a business to be more secure? What key business processes are in place that will support this level of accountability?

Zero trust, better network visibility

For an increasing number of organisations, adopting a zero trust approach to security is a powerful means to achieve resilience and protect hybrid cloud environments from cyber attacks. This is substantiated by more than 1,000 security and IT leaders in the Gigamon *2023 Hybrid Cloud Survey* which revealed on a global scale, Zero Trust discussions at board level increased from 58% to 87% across the last year.

"Zero trust means that no one person or thing is trusted by default, whether inside or outside the network," says Stephen Oliver, senior director, EMEA North at Gigamon. "It's an approach that is gaining traction, even among those struggling to cope with increasing IT complexity and a proliferation of tools."

The inevitable 'tool sprawl' of digital transformation can introduce another element of risk to the organisation – which is exacerbated if security leaders don't have real-time visibility into all data in motion across their hybrid cloud IT infrastructure. The same applies to governance and risk; it's impossible to comply with regulations if you can't see what's going on in your environment, or where all your data traffic is coming from or going to.

Deep observability is key here, and its tie to zero trust has been reaffirmed in studies, including how critical it is in securing and managing hybrid cloud IT infrastructure.

Observability vs. deep observability

Observability is often used to describe this insight into what's on a network. But when it comes to zero trust, organisations need to think beyond surface level visibility. Security and observability tools must bring together log-based data with network-derived intelligence if they are to provide deep observability across a company's hybrid cloud – one that spans the data center, private and public cloud, along with virtual and container workloads.

"A true zero-trust approach rests on a foundation of real-time, network-level visibility, and this includes monitoring East-West (lateral) traffic for behavioural anomalies and insight into all traffic in transit, even encrypted traffic" says Oliver.

Instead, deep observability provides 360-degree visibility into the hybrid cloud IT infrastructure, applications, and systems that go beyond existing MELT (Metrics, Events, Logs, and Traces)-based approaches, incorporating real-time network-derived intelligence and insight.

Deep observability, as enabled by Gigamon, can serve as a foundation element of successful security initiatives, be it maximizing tooling investment, or charting a path to zero trust.

"Zero trust demands exceptional visibility across your entire network," says Oliver. "This deep observability is powered by the combination of data and insights collected by existing security, observability tools, and network telemetry. It's this combination that provides the real-time intelligence and insights that can help drive a zero-trust approach."

Alexandr Mucic via iStock photo

97%

of global IT and Security leaders believe that deep observability is an important element of cloud security

52%

of global IT and Security leaders claim their boards don't understand a shared responsibility security model

Gigamon, 2023

> Being able to see everything in your IT environment is the first and foundational pillar of a zero-trust-based strategy

The pillars of zero trust

Understanding how to achieve zero-trust and what it requires is therefore paramount for CISOs. The CIS Critical Security Controls (CIS Controls) is a set of best practices for organisations looking to strengthen their security posture. The first step? A commitment to visibility.

"It's important for CISOs to have visibility of all network traffic flowing within their IT infrastructure for security and performance monitoring, and the way to achieve that is by deploying a deep observability strategy," says Oliver. "Being able to see everything in your IT environment is the first and foundational pillar of a zero-trust-based strategy – and it's one that cannot be overlooked."

Zero trust is here to stay. The adoption of zero trust has even been mandated for government organisations in the United States, and it is likely to expand to other regions. In the UK, the national cyber security centre's cyber essentials scheme is now completely aligned with a zero-trust architecture.

"It is critical that CISOs, given their evolving responsibility and increased accountability, have deep observability across networks and cloud environments, to enhance security outcomes and mitigate risks and costs," says Oliver. "At Gigamon, we deliver a foundational pillar that provides complete visibility into all data that runs across an organisation's hybrid cloud IT environment."

Deep observability clears a path for successful journeys towards zero-trust. Think about how a fully-lit street is safer than a dark one – your networks are no different. Gaining complete visibility into the network is the equivalent of lighting up the whole street.

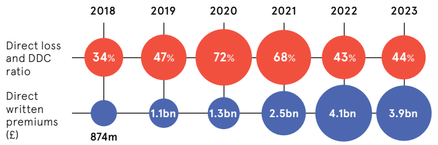
Learn more about why Deep Observability is foundational to Zero Trust: gigamon.com/campaigns/zero-trust

Gigamon®

Nikolay Pandev via iStock

THE VALUE OF DIRECT WRITTEN PREMIUMS DECLINED FOR THE FIRST TIME IN 2023

Cyber coverage direct loss and defence and cost containment ratio and value of direct written premiums



Fitch Ratings, S&P Global Market Intelligence, 2024

CYBER COVER

The underwriting on the wall: insurance costs ease, but for how much longer?

Premium inflation has abated, courtesy of greater competition in the market and a general improvement in cybersecurity. But the recent resurgence of ransomware attacks – and other threats – may change that

Mark Walsh

On 2 May, the US director of national intelligence, Avril Haines, warned a Senate panel that cyber warfare waged by foreign adversaries such as Russia and China, had become one of the "most pernicious transnational threats" to the security of the country. She noted that the number of international ransomware attacks – a large proportion of which target US entities – had risen by 74% year on year.

Yet the global cyber insurance market doesn't seem to share Haines's sense of alarm. Most providers have barely upped their premiums since early 2023, while some have even reduced theirs. Indeed, the average price of cyber coverage fell by 6% in Q1 2024 after edging down by 2% and 3% respectively in the last two quarters of 2023, according to international brokerage Marsh.

It's a significant shift from the so-called hard insurance market of 2020-22, when premiums more than doubled, hitting historic peaks after a surge in ransomware claims during the depths of the Covid crisis. The ransomware epidemic of that period, coupled with the ever-present spectre of a catastrophically far-reaching cyber attack, led some observers to conclude that the risk was becoming virtually uninsurable.

So why has there been no replay of that sky-is-falling scenario? Experts in the field suggest several reasons, ranging from increased competition among insurers to improved cyber resilience among their clients.

One such expert is Kara Higginbotham, head of professional liability and cyber at Zurich North America. She reports that the market "looks slightly different" this time. For instance, "the risks are dispersed differently across a wider number of carriers".

Nonetheless, the apparent resurgence of ransomware and other cyber threats may start pushing premiums back up before the end of this year. The cost of providing cover remains far greater than it was before the Covid crisis – and insurers cannot absorb further increases indefinitely.

Reinsurance giant Munich Re has estimated that premiums collected by cyber insurers worldwide rose from about £7.5bn in 2021 to £11.2bn in 2023.

Such a significant increase may have helped to keep premiums in check more recently, according to Tom Johansmeyer, global head of index classes at reinsurance broker Inver Re.

"Ransomware is always a concern, but what should make this year different is the fact that the global premium base is much larger than it was in 2021," he says, explaining that this should give insurers more scope to absorb losses and so make the market less volatile than it otherwise could be.

> The bar has been raised. Businesses are doing a better job of securing themselves

And, while US entities still contribute about 60% of this market's total premiums, Johansmeyer notes that uptake of cyber insurance in other territories has grown significantly since 2021. Research published last year by the Howden brokerage, for instance, reported especially strong growth in France, Germany, Israel, Scandinavia and the UK. Such diversification "should provide some amount of overall industry resilience", he predicts.

Johansmeyer estimates that the five largest cyber insurers still account for as much as a third of the global market. But more entrants have arrived in recent years, which has put downward pressure on the price of cover as these newcomers seek to establish themselves by offering more competitive premiums.

Higginbotham says: "There are new entrants and new capacity entering the market. Because premiums were going up, there was more willingness on their part to jump in and insure these risks."

These recent entrants have included not only traditional insurance and reinsurance firms but also newer industry entities such as managing general agents. These have teamed up with carriers to handle underwriting in specialised markets including cyber insurance.

Besides competing on price, insurers are going to greater lengths to tailor policies to fit clients' risk profiles, according to Howden. This has also helped to make cyber insurance more of a buyer's market.

But there is a downside to this increase in competition, warns Daniel Woods, a cybersecurity lecturer at the University of Edinburgh. He reports that anecdotal information compiled over the past six months indicates that some irresponsible insurers are undercutting rivals on underwriting standards.

"This risks undoing the gains in cyber resilience seen during the hard market between 2020 and 2022," he argues.

Indeed, improvements in clients' cybersecurity practices over that period, partly in response to new requirements imposed by underwriters, helped to stabilise the insurance market and get premiums under control.

"The bar has been raised. Businesses are doing a better job of securing themselves," confirms Adam Harrison, a cybersecurity expert and managing director at FTI Consulting.

He notes that making such improvements has paid off for mid-sized businesses in particular. These have attracted a large proportion of ransomware attacks because criminals view them as softer targets than large companies but consider them cash-rich enough to be worth hitting.

Peter Hedberg, vice-president, underwriting, at cyber specialist Corvus Insurance, reports that clients aren't paying ransoms as often as they were because they're better prepared to withstand attacks. When they're using processes such as multi-factor authentication and ensuring that all backup data is encrypted or immutable, it means that "restoration is a far more viable option than it was before", he says.

While such precautions have helped to stabilise the cyber insurance market, insiders acknowledge that volatility could return. That's in part because of a lag effect on premiums, because policies are typically renewed annually. This means that an uptick in prices reflecting the latest ransomware surge may well lie ahead.

Moreover, other threats, including IT supply chain attacks, have hardly gone away, while a growth in claims stemming from litigation over wrongful data collection has become a key concern.

In the US, alleged violations of laws such as the Biometric Information Privacy Act – introduced by the state of Illinois back in 2008 – have led to costly class actions against firms including Facebook, TikTok, HR software provider ADP and theme-park operator Six Flags.

A more recent privacy litigation trend concerns the use of pixel tracking, whereby companies use code embedded in their websites to gather information about visitors. Because such cases may take years to resolve, that only adds to the uncertainty about the likely scale of future losses.

"It is very possible that rates could increase, given what happens when carriers come to realise what losses they're holding on their books," Higginbotham warns.

And that's without even considering the impact AI could have in helping hackers to wreak havoc on IT systems.

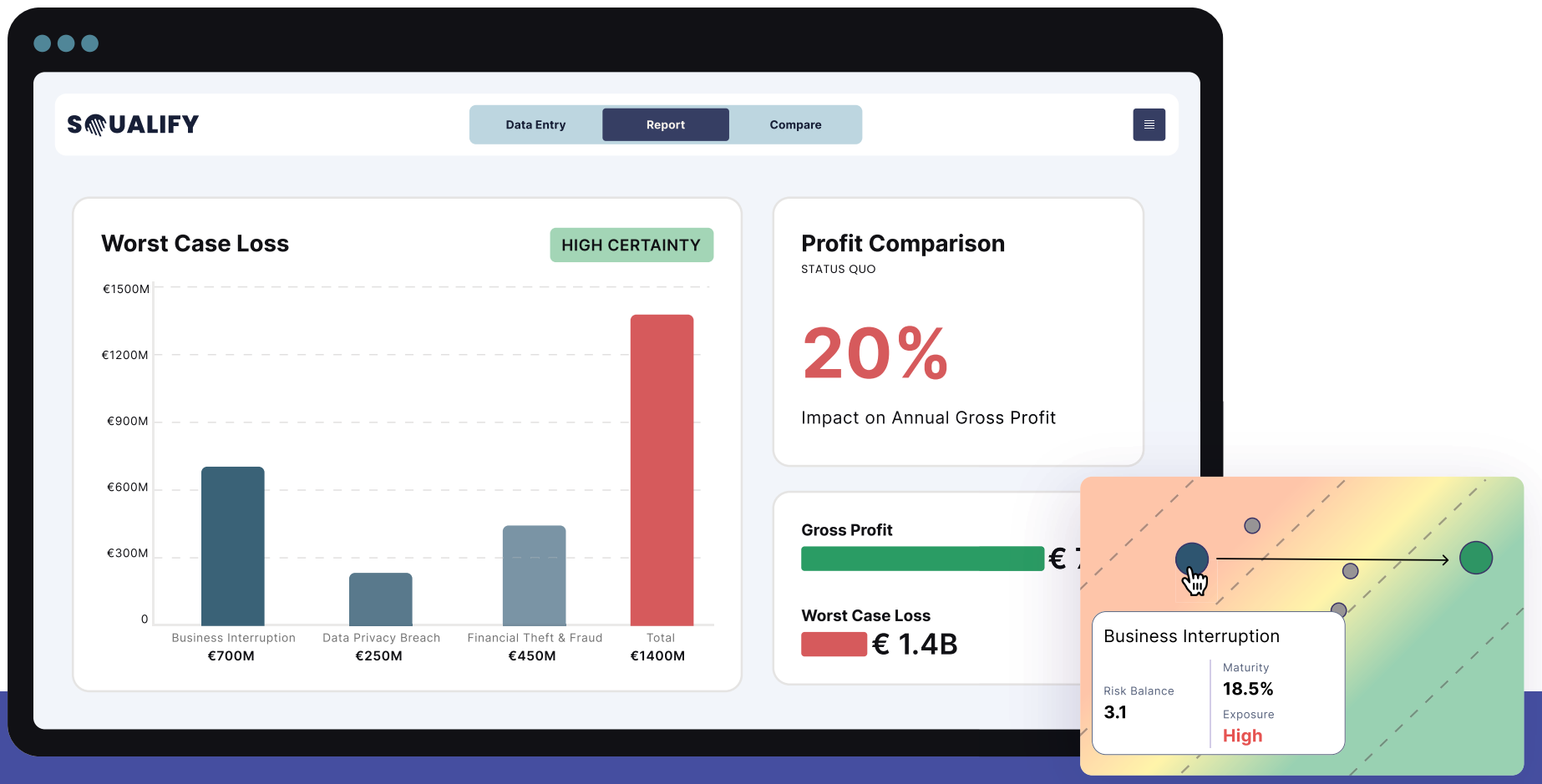
"We take AI very seriously. We're very scared," Hedberg admits. "The best we can do as underwriters is offer a reactively priced product and protect our insurance."

TOP-DOWN CYBER RISK QUANTIFICATION

Cyber Risk Management for the Boardroom.

Find out how much money your organisation could lose in the next cyber attack.

- **Lean implementation**: Worst Case Loss in 48hrs. Full quantification in few days.
- **Superior data**: We leverage 9+ years of historical cyber loss data.
- **Reliable**: Our risk model is trained on 4,500+ quantifications.
- **Scalable**: Seamless enterprise-wide risk aggregation.



Quantify your full cyber risk in few days.

Understand the financial impact of your cyber risk and make strategic decisions for the entire organisation.

REQUEST A FREE DEMO AT SALES@SQUALIFY.IO

SQUALIFY
A Munich Re Venture

www.squalify.io