CYBERSECURITY

02 CAN THE UK BOLSTER DIGITAL RESILIENCE?

04 WHY DIGITAL TRUST IS AT A RECORD LOW

11 TRUMP'S CYBER CUTS PUT US ALLIES ON EDGE

CYBERSECURITY

Distributed in
THE TIMES

Published in association with
Infosecurity Europe | 3-5 June 2025 | ExCeL London

Contributor

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

Raconteur

Special projects editor
Ian Deering

Commercial content editors
Laura Bithell
Larnie Hur
Jessica Lynn

Commercial production managers
Alex Datcu
Ellen Newsome

Production executive
Sabrina Severino

Design and illustration
Kellie Jerrard
James Lampard
Celina Lucey
Samuele Motta

Design director
Tim Whitlock

Certified B Corporation

POLICY

How Westminster plans to bolster digital resilience

The government has revealed details of the cyber secuirty and digital resilience bill, which aims to protect the UK's critical infrastructure

Tamlin Magee


Nicola McCombe via Getty Images

The UK government has released a policy paper revealing further details of the upcoming cyber security and resilience bill, which was first teased in the King's Speech in July 2024.

The bill, which will enter parliament later this year, has three primary goals. One is to strengthen the cyber defences of IT providers supplying government or public services. Most suppliers for the public sector are subject to certain cybersecurity reporting obligations under the NIS Regulations 2018.

Westminster plans to extend these regulations to include IT providers for public sector organisations. It estimates that up to 1,000 IT suppliers would be redefined as 'critical national infrastructure' and therefore subject to certain cybersecurity safeguards.

The designation will be applied to IT suppliers of any critical public services, as a cyber attack or similar disruption at these firms could significantly impact public services. Suppliers that fail to comply with the additional requirements could face fines of up to £100,000 per day.

These plans come in response to an observed increase in supply-side attacks, which enable attackers to access large organisations through vulnerabilities in their supply chain partners.

Also in the bill is a plan to strengthen "information-gathering powers" at the Information Commissioner's Office, with the aim of enabling the regulator to identify cyber risks more proactively.

Finally, the bill proposes giving the secretary of state powers to update cyber regulations without going through parliament. According to the policy paper, the aim is to enable the government to introduce regulation quickly in response to sudden changes in the cybersecurity landscape.

Three further measures are being considered, but are not yet included in the bill.

Data centres, which were redefined as critical national infrastructure in the UK in September 2024, could be included in the scope of the regulation. Under the proposal, public data centres with at least one megawatt (MW) capacity would be covered by the regulation. For enterprise data centres, the threshold would be 10MW.

Of the 224 colocation data centres in the UK, managed by 68 operators, the government expects 182 third-party sites and 64 operators to fall in scope of the regulation.

Secondly, the government may publish a "statement of strategic priorities for regulators". This would create a standardised cybersecurity framework for all regulators and a "unified set of objectives" for implementing regulations.

Lastly, the secretary of state may be given executive powers to demand regulated entities to take action against emerging threats, if doing so is deemed "necessary for national security".

Industry commentators welcomed the details of the proposals, which represent a "necessary course correction" according to Etay Maor, chief security strategist at Cato Networks.

"When attackers hit London hospitals by compromising a managed service provider (MSP), it wasn't just a breach, it was a failure in how we delegate trust," Maor says. "MSPs are deeply integrated in the organisation, and have privileged access and wide operational reach. Treating them like passive vendors ignores the fact that when one falls, the blast radius is massive."

Martin Lee, EMEA lead at Cisco Talos adds: "Critical services must be secured against a constantly evolving threat landscape. The government's proposals are a welcome step forward in boosting the nation's digital resilience."

But ensuring government and regulators work closely with industry on the detail and delivery will be a crucial next step, Lee emphasises.

The government announced the bill in July, promising to introduce mandatory reporting for ransomware attacks and grant regulators more powers to mitigate and respond to cybersecurity incidents.

The announcement came in the wake of a devastating cyber attack on Synnovis, a private company that provides pathology services to the NHS. After the attack, some patients were informed they may have to wait up to six months for blood tests.

Jamie Maccoll, a research fellow at RUSI, a defence think-tank, says mandatory reporting of ransomware will be particularly useful to better understand the cybercrime landscape in the UK.

"We know cybercrime is a really big issue," he says, "but we don't know the scale of it or the true cost of it to the UK, which makes it hard to design effective policy."

A bill focused on AI oversight was conspicuously missing from the government's latest announcement. The Labour Party promised in its election manifesto to direct more regulatory scrutiny to frontier AI operators including Google, Anthropic, Microsoft and OpenAI. When it comes to AI security, therefore, there are plenty of potential risks that industry and government must address. That's according to Julian David, CEO of TechUK, a tech industry group.

He adds that the government must work closely with industry when crafting AI policies to ensure that any new legislation does not inhibit growth and innovation unnecessarily. David says getting the balance right is important for the UK's AI and also for the prime minister's ability to achieve his goals for the government and the nation.

89 out of 430
total cyber incidents managed by the National Cyber Security Centre in the 12 months to September 2024 were deemed 'nationally significant'

11,000
acute outpatient appointments or elective procedures were postponed last year thanks to a cyber attack on an NHS supplier

DSIT, 2025

INSIGHT

'Quantum is not just a technical challenge'

This year's Infosecurity Europe will prepare security professionals for a wave of emerging threats

From 3 to 5 June 2025, London's ExCeL Centre will again host Infosecurity Europe, the most influential information-security industry event. This year marks our 30th anniversary, and we've curated a programme that reflects both how far the industry has come and how advanced technology is changing cybersecurity.

Among the biggest shifts on the horizon is quantum computing, which has the power to transform industry, society and, of course, cybersecurity. Once a distant concern, quantum computing now has real-world implications. The 2025 edition of Infosecurity Europe puts this issue front and centre, providing insight into potential consequences that cannot be ignored.

This year's keynote sessions address changing perceptions of quantum computing. The US National Institute of Standards and Technology (NIST) has already formalised the first set of post-quantum cryptography standards, which indicated that policymakers and researchers are taking the threat seriously.

On 3 June, we're opening the conference with a keynote session with the world-renowned physicist and communicator Professor Brian Cox, who will explore the intersection of black holes and quantum mechanics, and discuss the implications for the future of computing. In a session titled "Black Holes and Quantum Computers", he'll look at the science behind this emerging technology, the structure of black holes, how they store information and how this might redefine what's possible.

The session serves as a reminder that quantum is not just a technical challenge, it's a conceptual one that demands a broader conversation on science, strategy and ethics.

Following this is a panel featuring industry experts including Daniel Cuthbert from Santander, IBM's Anne Leslie, Karl Holmqvist from Lastwall and Joe Tidy, a cyber correspondent and author at BBC News. In a discussion titled "Quantum Computing versus Cybersecurity: The Next Arms Race", they will examine how advances in quantum computing will reshape cyber defences, explore the rising threat of 'harvest now, decrypt later' attacks and assess which industries are most at risk.

The session will also cover how the industry is responding through initiatives and what steps security leaders can take to integrate post-quantum cryptography into their existing systems.

More broadly, the event will explore the full scope of security challenges facing today's organisations, with eight content stages covering everything from ransomware and AI to regulation and geopolitics.

Education will take centre stage this year with the launch of Infosecurity Europe Masterclasses, powered by SANS Institute. These instructor-led sessions are designed to equip professionals with practical skills in digital forensics, cloud security and security culture. The masterclasses will feature live simulations, deep-dive techniques and actionable takeaways for immediate workplace implementation.

Also new to 2025 is the Infosec Hub, a dedicated space for strategic learning to support cyber professionals with selecting and buying the right solutions. It includes demos, peer discussion groups and a clinic where analysts such as Forrester and Frost & Sullivan will provide guidance on purchasing or implementing cyber solutions.

On 4 June, we'll welcome Abadesi Osunsade, the founder and chief executive of Hustle Crew, to the keynote stage with a discussion titled "Taking Up Space: How to Lead the Charge in Cybersecurity", a conversation aiming to help security professionals build their confidence, establish a personal brand and enhance their careers.

This year's Infosecurity Europe will have more than 380 exhibitors and countless opportunities to learn, connect and collaborate. The agenda is packed with speakers from across industry, government and academia who will share practical security strategies, provoke debate and bring the cybersecurity community together to build a safer digital landscape.

Brad Maule-ffinch
Event director, Infosecurity Europe

PRIVACY

Public trust in digital tech plumbs dismal depths

Privacy is an increasingly important feature in digital interactions. Why are so few businesses taking note?

Tamlin Magee

Zora Zhuang via Getty Images

Trust in digital services has plummeted as consumers feel that the onus is on them to protect their data. And companies that violate their users' privacy risk losing customers.

These are the findings of the 2025 Digital Trust Index, produced by Thales, the French aerospace and defence company. The report, which surveyed 14,000 consumers across 14 countries, paints a bleak picture of consumers' trust in most digital interactions.

News and media is the least trusted sector, according to the survey. Only 3% of consumers said they trust news and media organisations with their personal data. Respondents also labelled organisations in supply and logistics (4%), social media (4%), entertainment (5%), retail (5%), transportation (6%) and hospitality (7%) as particularly untrustworthy.

At the other end of the spectrum, people appear most willing to hand their personal information to firms in the banking sector (44%) and government organisations (41%).

"It's a pretty depressing state of affairs," says Rob Elliss, vice-president of sales for Thales across EMEA. Without trust, he explains, businesses will struggle to develop their digital capabilities.

It is perhaps little surprise that people distrust brands with their data, given the many stories of catastrophic data leaks and cyber attacks appearing in the media.

"Privacy is much more in the public psyche than it used to be," adds Elliss. "The majority of consumers expect a greater degree of transparency about what data is being collected and also a certain degree of sovereignty and ownership of their own data."

Although GDPR imposes restrictions on how organisations can use the data they collect, there is a sense that it is ultimately the responsibility of individuals to safeguard their own information.

Almost two-thirds (63%) of those surveyed believed that too much onus is placed on the consumer to protect their own data. More than a third said they only share data when it's absolutely necessary to access a product or service.

Anyone who has tried to regain control of their data from a data broker, the names of which are often hidden in the terms and conditions of any digital service, will know that the path to doing so is often circuitous and complicated, even though GDPR is meant to ensure this right.

"Trust is so low because consumers feel that privacy is an uphill battle," adds Elliss. "Many people don't know where to start. Do you reject or accept cookies? There's a fatigue that creeps in, in terms of getting things done."

He says a better balance is needed bewteen data privacy and security on the one hand and ease of use, access and reliability of services on the other.

Some brands understand that privacy is attractive to consumers. Apple has consistently developed new privacy features for its handsets since 2014, after its CEO, Tim Cook, highlighted the issue of consumer tracking in an open letter. Meta, which has been fined for violating data privacy rules in the EU, has since emphasised user privacy and introduced end-to-end encryption for chat services across Facebook Messenger and Instagram in 2023.

> **Trust is low because consumers feel that privacy is an uphill battle. Most people don't know where to start**

But, despite consumer demand, few companies are focusing on data privacy as a key selling point. "A lot of consumers are rejecting brands precisely because of the excessive amount of data they feel is being gathered and the absolute lack of transparency as to where that data is heading and what's being done with it," says Elliss.

The banking sector – the most trusted sector in Thales' report – might suggest a route forward. Finance is heavily regulated and banks have been incentivised to demonstrate their security credentials to customers. "That is very visible to the public," says Elliss.

He believes that companies could gain consumer trust by following the examples of firms in regulated industries. Organisations should demonstrate the steps they are taking to protect data, whether from cyber attacks or sovereign controls, and should offer customers ongoing access to their data, Elliss says.

Ironically, however, consumers are apparently bothered by basic data-protection measures. About one in six people surveyed by Thales said they have abandoned brands or service providers because of bothersome password requirements.

But organisations must govern access to data, systems and networks. And Elliss says there are many passwordless technologies that provide robust user protection, such as FIDO tokens, pass keys and biometric authentication.

"It's about using commonly available technologies and making it clear to your customers what you're using," he says. "Outside of highly regulated industries, I don't think companies make enough noise about the measures they're putting place to ensure your protection."

He continues: "If brands deployed more sophisticated authentication, security and privacy tools, that would rapidly lead to an increase in consumer trust."

So firms can strengthen privacy measures and empower users to access their data. But another way to earn trust is to simply keep less customer information.

There are plenty of companies holding and processing sensitive data with little knowledge of where it resides or whether it's protected, according to Elliss.

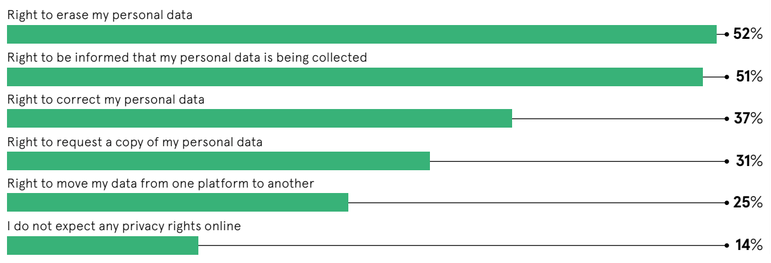
Sometimes removing data or opting not to request certain details is the simplest solution. "That's something we often overlook," Elliss says.

Organisations seeking to win customer trust should first understand where the data resides, then protect it or simply delete it.

Firms that do hold or rely on sensitive data ought to take "very visible" measures to protect and control access, Elliss adds. This is not yet commonly understood at the enterprise level, but given the dearth of digital trust among consumers, that may soon change.

WHAT KIND OF PRIVACY RIGHTS DO CONSUMERS EXPECT? Thales, 2025

Privacy rights consumers expect in interactions with brands and governments



Commercial feature

How to use AI to outpace tomorrow's cyber challenges

Cybercriminals are using AI to launch faster, more targeted identity attacks. To keep up, organisations must adopt proactive, AI-driven security strategies

Identity is the latest battlefield in cybersecurity, and credentials are prime targets for sophisticated threat actors armed with AI.

Cybercriminals have even developed autonomous attack frameworks that operate

without human direction, and are using sentiment analysis to craft highly targeted spear-phishing campaigns. What's more, AI is enabling more persistent, adaptive and scalable attacks, forcing security teams to defend against a wider range of threats at speed.

"Cybercriminals are weaponising generative AI for more convincing social engineering and using AI to identify attack paths through complex systems," says Dmitry Smilyanets, a senior director, product management and engineering at cybersecurity company Recorded Future.

"The attack timeline has become significantly shorter, with techniques that previously took months to develop now emerging in weeks or days," says Smilyanets. "The velocity of modern attacks also frequently outpaces humans' response capabilities, with automated attack tools able to compromise systems and spread laterally within minutes of gaining initial access."

Organisations using extensive software-as-a-service applications and digital identities are particularly vulnerable, as the expanded attack surface of these platforms provide threat actors with more opportunities to exploit identity weaknesses than ever before.

"As organisations grow their digital presence, they effectively increase the perimeter they must defend, creating more potential entry points for attackers," Smilyanets explains. "Many organisations struggle with visibility challenges, unable to track all their digital assets – and as security professionals often note, you cannot protect what you don't know exists."

The volume of exposed credentials has reached unprecedented levels, with credential theft per device rising 25% since 2021, according to Recorded Future's 2024 State of Threat Intelligence report. "Some organisations discovered more than 100,000 exposed credentials in our assessment – that makes manual remediation virtually impossible."

Last year, approximately 77% of web-application breaches involved stolen credentials, according to the 2024 Verizon Data Breach Investigations report. Traditional security tools often fail to stop identity-based attacks because they're designed to detect anomalies rather than valid credentials being misused. Even sophisticated behavioural-analysis tools struggle initially, as attackers using legitimate credentials can mimic normal user-behaviour patterns.

Recorded Future's research has also identified significant growth in supply chain credential compromises, where attackers target third-party service providers to gain access to multiple downstream organisations simultaneously. "A single compromised vendor led to data exposure across dozens of enterprise customers in several cases we analysed," says Smilyanets.

Sophisticated cyber attacks

No organisation is immune to these threats, which can cause tremendous damage. In February 2025, the GrubHub data breach exposed millions of customers' and drivers' identities. Attackers claimed to have stolen 70 million lines of data, including millions of hashed passwords, phone numbers and email addresses.

The intrusion was traced to a third-party service provider, which the threat actors used to access the contact information of campus diners, merchants and drivers who had interacted with customer-care services. "The attackers demonstrated sophisticated targeting by exploiting third-party partnerships and creating a domino effect where a single compromised vendor impacted an entire ecosystem," says Smilyanets.

"Security experts noted the attackers likely used AI-driven tools to analyse the network for vulnerabilities and automate data exfiltration, enabling them to access and harvest millions of identity records with minimal human intervention."

Recent breaches at Snowflake and Change Healthcare also revealed another new pattern: attackers using so-called infostealer malware to obtain credentials and bypass protections such as single sign-on (SSO).

Infostealer malware uses a multi-stage process that helps to circumvent modern security measures. "Initial infection typically occurs through phishing, malicious advertisements or compromised websites, followed by establishing persistence on infected systems," Smilyanets explains.

The malware then harvests credentials from multiple sources, including web browsers. "What makes infostealers especially dangerous is their ability to bypass SSO and multi-factor authentication by capturing authentication tokens and cookies rather than just passwords, and stealing browser session data that contains active, authenticated sessions," says Smilyanets.

Modern infostealers, such as Redline, Raccoon and Vidar, can even extract complete digital identities rather than just passwords, allowing attackers to fully impersonate legitimate users with all their authentication factors.

Another element that makes modern identity attacks particularly devastating is the criminal infrastructure supporting them. Initial-access brokers specifically sell authenticated access to corporate networks, and ransomware-as-a-service platforms have lowered the technical barriers for attacks. Communication channels such as Telegram and Discord also facilitate the trading of compromised accounts, while forums provide technical support and tutorials for using stolen credentials effectively.

"The criminal underground has evolved into a sophisticated ecosystem for credential trafficking and malware distribution," says Smilyanets. "Specialised marketplaces offer categorised, searchable databases of stolen credentials, while subscription-based services provide continuous access to newly compromised data."

Proactive security

All of these evolving threats demand a shift from reactive, perimeter-based security models to proactive detection of credential exposures before exploitation. Identifying compromised credentials in the early stages, especially if they are legitimate credentials, enables organisations to promptly reset passwords, implement additional authentication measures or place heightened monitoring on affected accounts.

"This creates a critical time advantage, allowing security teams to neutralise the threat while attackers are still in the reconnaissance and preparation phases," says Smilyanets. "Early detection essentially transforms a high-risk situation with minimal security visibility into a containable event where defenders have the upper hand."

Recorded Future's identity intelligence solution leverages advanced AI and machine learning to provide organisations with preemptive detection of compromised credentials before attackers can weaponise them. "Our platform collects and analyses exposed credentials in near real-time across an unmatched breadth of sources – including dark-web forums, paste sites, criminal marketplaces and botnet infrastructure – which traditional security tools do not have access to," says Smilyanets.

It also creates connections between compromised identities, threat actors and attack patterns that would be impossible to detect manually, providing critical context about the threat actors involved, their typical attack patterns and the likely timeline for exploitation. This enables security teams to understand not just which credentials are exposed, but which ones present the most immediate risk.

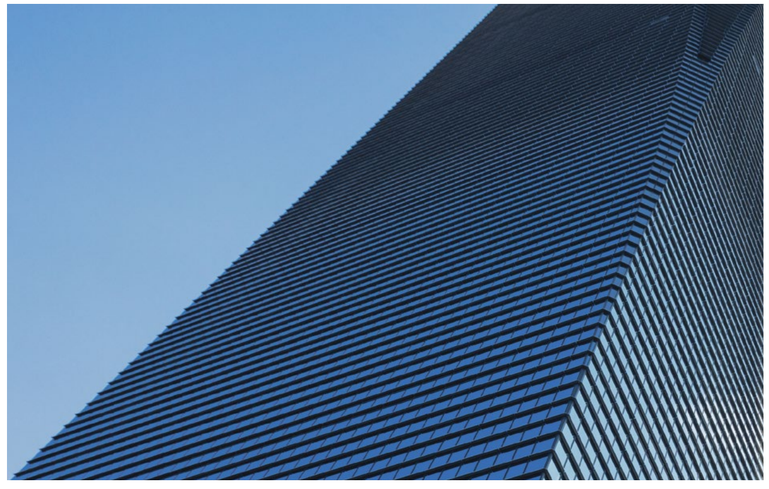
"We assign risk scores to entities such as IP addresses, using both rule-based and machine-learning systems, which helps analysts quickly determine which threats require immediate attention," says Smilyanets. "This scoring mechanism is critical for helping security teams focus on the most critical exposures rather than drowning in alerts."

An API-driven architecture also enables fully automated security workflows. This means security teams can automatically determine whether exposed credentials belong to their organisation and whether they're still active, identify the specific users affected and initiate password resets without manual intervention. This can reduce remediation time from days to minutes, and help to scale up protection as credential exposures grow.

Ultimately, Smilyanets concludes: "Proactive AI-driven identity intelligence provides the visibility, context and response capabilities needed to address the central role identities play in modern security architectures, making it not just beneficial, but necessary for contemporary cybersecurity strategies."

In today's threat landscape, identity is the primary target. Traditional defences can't keep up, so organisations need AI-driven identity intelligence to gain visibility, prioritise risks and respond quickly.

> **In today's threat landscape, identity is the primary target**



Scan the code or visit recordedfuture.com/identity-exposure-assessment to find out more about Recorded Future's Intelligence Graph

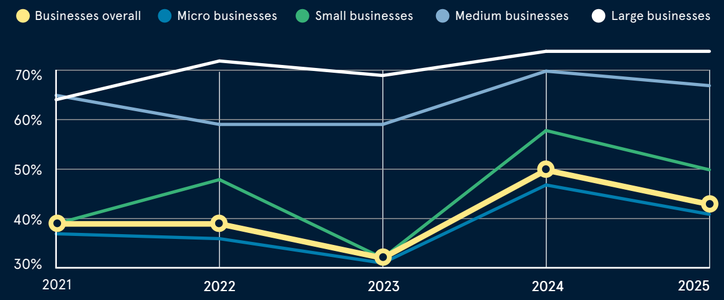
Recorded Future®

BOARDROOM BACKSLIDE

Board-level responsibility for cybersecurity is in sharp decline at UK firms. Only 27% of organisations today have a board member with responsibility for cybersecurity, compared with 38% in 2021. This is worrying, considering the threat of ransomware has doubled over the past year, according to DSIT's *Cyber Security Breaches Survey 2025*

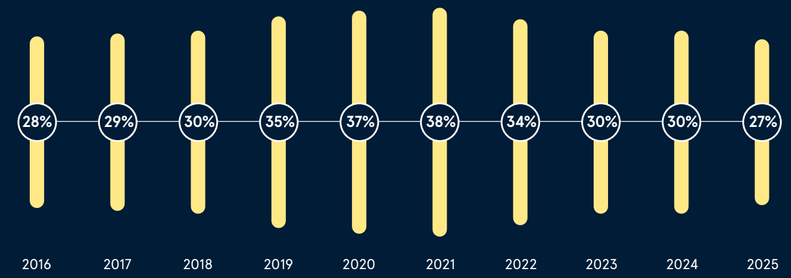
FEWER ORGANISATIONS IDENTIFIED ATTACKS IN THE PAST 12 MONTHS

Share of organisations that have identified a cybersecurity incident or attack in the 12 months prior to survey date



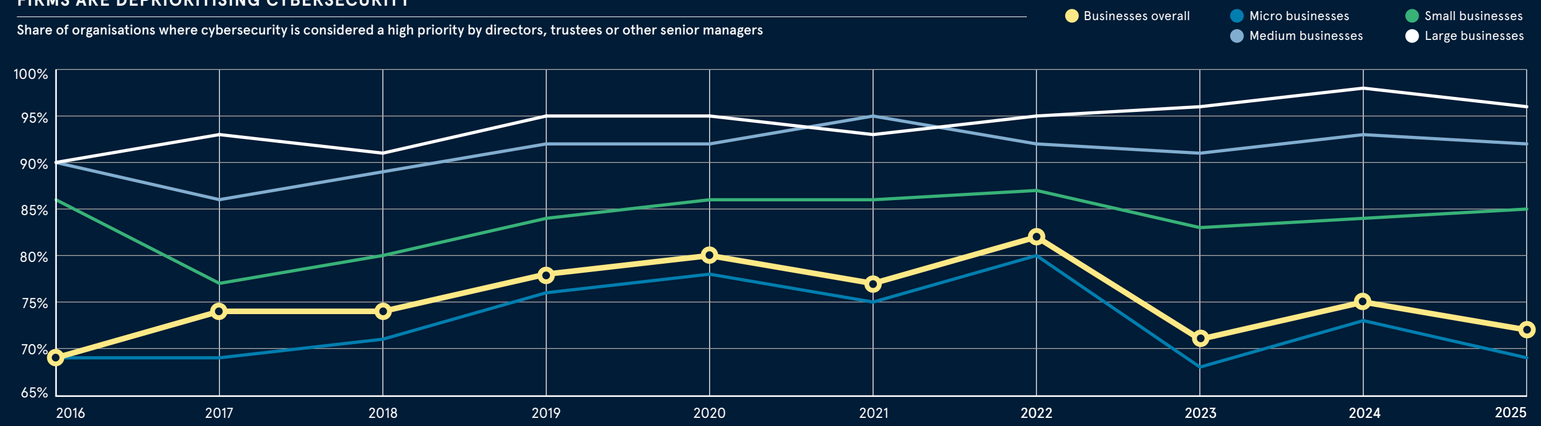
NEARLY THREE IN FOUR FIRMS HAVE NO DEDICATED CYBERSECURITY ADVOCATES ON THE BOARD

Share of organisations with board members or trustees with responsibility for cybersecurity



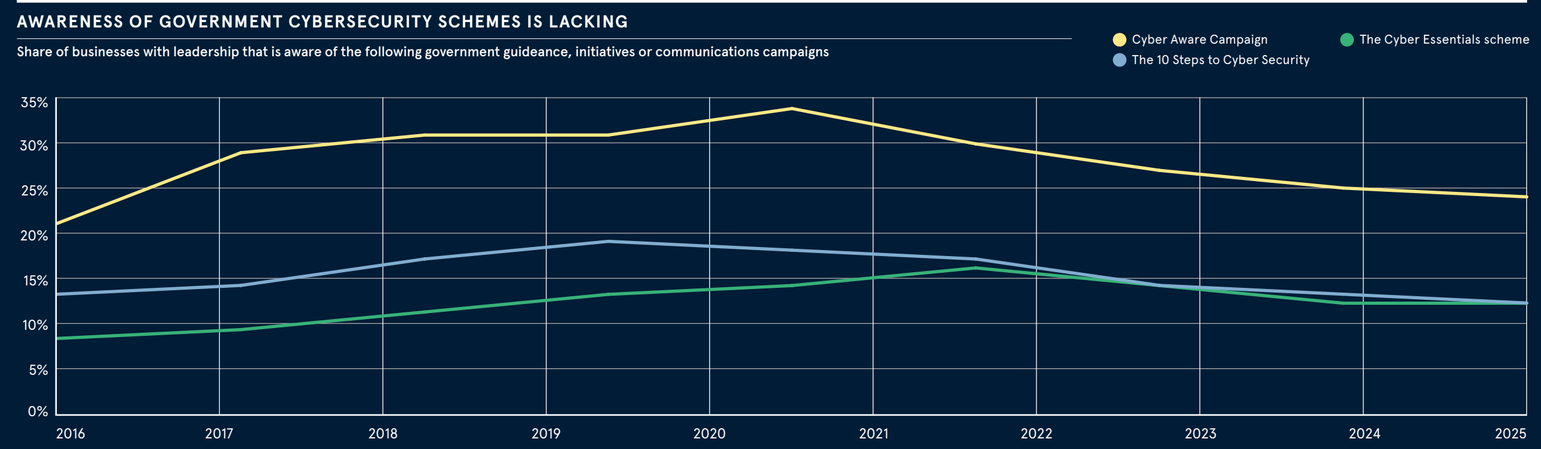
FIRMS ARE DEPRIORITISING CYBERSECURITY

Share of organisations where cybersecurity is considered a high priority by directors, trustees or other senior managers



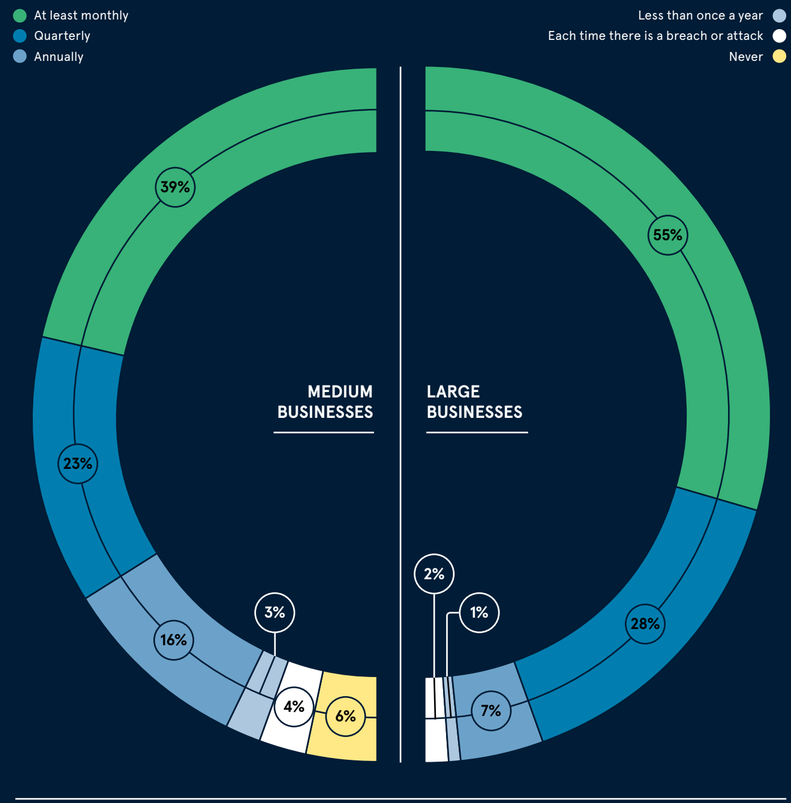
AWARENESS OF GOVERNMENT CYBERSECURITY SCHEMES IS LACKING

Share of businesses with leadership that is aware of the following government guideance, initiatives or communications campaigns



MOST SENIOR STAKEHOLDERS RECEIVE REGULAR CYBERSECURITY UPDATES, PARTICULARLY AT LARGE BUSINESSES

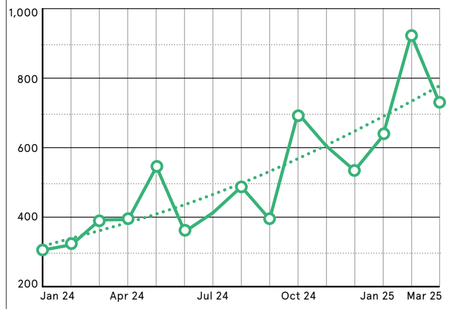
Frequency with which directors, trustees or other senior managers are updated on cybersecurity actions



Department for Science, Innovation and Technology, 2025

RANSOMWARE ATTACKS ON THE RISE

Number of ransomware victims reported on data-leak sites



Checkpoint, 2025

WORKFORCE

Ransomware's human costs: sleepless nights, strokes and PTSD

A new report shows that IT teams have been overworked, stressed and even hospitalised in the aftermath of ransomware attacks

Tamlin Magee

For all the chaos caused by ransomware attacks, conversations about their imact tend to focus on financial damage. Ransomware attacks cost organisations tens of billions of pounds a year and have even forced some victims into insolvency.

The average ransom demand in 2024 was $3.5m (£2.6m), the average ransom paid, $9.5m (£7.1m), and total ransoms paid throughout the year reaching $133.5m (£99.7m), according to Comparitech's 2024 end-of-year ransomware report.

But these cyber attacks affect more than a company's bottom line. They also take an emotional and physical toll on the people left dealing with the aftermath.

Two new reports, *The Ransomware Victim Experience* from RUSI, a defence think-tank, and an accompanying academic article for the *Journal of Cybersecurity*, outline just how devastating these attacks can be for those left to deal with the aftermath.

According to the reports, ransomware attacks impact everything from organisational wellbeing to victims' family lives and mental and physical health. One person in the report claims the stress of a ransomware attack contributed to a stroke that they suffered shortly afterwards. A senior executive, meanwhile, suffered from "a little bit of PTSD" every time they returned to the office and even reported feeling suicidal.

"There's so much that impacts the IT and security teams and other people across the business," says Jason Nurse, the reports' co-author and a reader in cybersecurity at the University of Kent. "Psychologically, it's significant. It really hits people quite hard. Often people aren't keen to return to work."

Many security professionals said they have been unable to sleep or eat properly during major attacks and would work extremely long hours to restore operations. Some staff attempting to restore systems were required to work together in small rooms for long stretches of time during the Covid pandemic, exacerbating their feelings of anxiety. One worker was sent to hospital with panic-induced heart palpitations owing to the stress of a ransomware attack.

"The reality is that security teams need to drop everything because the business cannot function unless the problem is addressed," adds Nurse. "There's pressure from other teams and external stakeholders and there is a limited number of people that have to think about how they'll respond. How do we engage? What do we say? How do we tackle this? Often the survival of the business comes down to just a few people."

Response teams often cannot leave work until any disruptions are resolved – they work around the clock, tired and stressed, and the pressure rises the longer the disruption drags on.

Some incident response firms, the researchers found, have developed in-house confidential trauma counselling for clients, and about 20% of victim organisations have used such services. Many individuals involved found that they could not return to the office after the attack and soon moved on to other roles.

> **The reality is that security teams need to drop everything because the business cannot function unless the problem is addressed**

Taking advantage of human fallibility is an essential skill for any cyber attacker. They must not only trick victims into opening malicious code, but also pressure people on the receiving end to pay the ransom.

With the advent of ransomware-as-a-service – where core teams develop malware, then affiliates pay to access and deploy it – criminals can target businesses more easily than ever before. Competition between cybercrime groups and law enforcement has led to an arms race to create increasingly effective tools and methods.

At the same time, cybercriminals are under pressure to devise new social engineering techniques to trick their victims and extort them more efficiently once their data is encrypted.

Criminals are increasingly extorting victims twice: first by encrypting their target's data and then by threatening to dump it in public channels if they are not paid. New groups such as Volcano Demon are even using high-pressure sales tactics to extort their victims. For instance, criminals will cold-call targets to discuss the options for restoring their data.

"Attackers have had to be more devious in their approaches to get people to pay, engage and respond," says Nurse. "They try to get under people's skin and into their minds to understand how they can extort people, how they can pressure them, how they can touch multiple pressure points to get people to pay."

Ransomware attacks work by exploiting weaknesses in human psychology. No wonder then that they take a psychological toll.

Employee wellbeing is rarely a consideration when assessing cybersecurity. Yet RUSI's research found that organisations with comprehensive wellbeing initiatives and high morale were among the most effective at protecting employees during an attack.

"High company morale made a big difference going into an attack," says Nurse. "Good, strong leadership is also important – thinking about preparation and things like key resiliency practices before an incident takes place."

Unsurprisingly, building a strong security culture helps staff to withstand the blows. But 'soft' measures can also help businesses bounce back from a ransomware attack. For instance, organisations with a set of trusted advisors internally – those who could be the calm voices in the room in a sea of understandable panic – were better able to withstand attacks. Setting up corporate communication channels and strategies before attacks occurred helped firms to recover quickly.

When dealing with an attack, it is important to plan ahead for continuity by introducing rota systems in case the issue is not resolved quickly, the report advises. While staff may have to work long hours to restor normalcy, small measures, such as bringing food carts into the room, allowing employees to go home for a couple of days before returning or paying for nearby hotels, go a long way to maintain satisfaction and wellbeing in the team.

The report also found that organisations that provided employees with access to psychological health or support services after an incident were able to recover from the attack more successfully. Promptly engaging with trusted third parties also helped victims to minimise damages and recover more quickly.

Implementing staff support measures can help to maintain wellbeing among IT workers and also contribute to greater workforce resilience, the report found. A financial services firm said it sould have prevented "months and months" f sick leave if it had offered its core IT staff gardening leave after a cyber incident was resolved.

A long-lasting challenge for security leaders is becoming integrated with the rest of the business. All too often, security or IT teams might feel siloed or that they are perceived as a blocker to business operations. This report underscores the fact that these security practices are essential to business continuity, especially in crisis situations. And in those situations, providing cybersecurity teams with additional support is essential.

Commercial feature

AI is rewriting the rules of risk management

With cyber risks and compliance demands increasing, automation is quickly becoming the smartest way for businesses to stay secure, agile and ahead of the curve

Organisations today face unprecedented challenges when it comes to managing risk. More applications, increased cloud migration and the proliferation of software-as-a-service solutions have dramatically expanded the threat landscape. Meanwhile, security teams are struggling with strict regulations, shrinking budgets and talent shortages.

At the same time, chief information and security officers are keen to demonstrate the business value that the security function provides, rather than just being viewed as a cost centre. They want to convey cybersecurity's role in mitigating risk, achieving compliance standards and helping to win new business.

It is against this backdrop that artificial intelligence (AI) presents a double-edged sword, often representing both a significant threat and a powerful solution.

Cybercriminals are using AI to create more convincing phishing attempts and generate more complex attack codes. But AI-powered tools are also providing unprecedented capabilities in risk management and compliance.

"We're seeing more vulnerabilities and attack vectors than ever before," explains Jeremy Epling, chief product officer at Vanta. "AI is being used by attackers to create new threats, whether through sophisticated phishing attempts or AI-generated attacks.

"But AI also gives us a capability we never had before: dealing with unstructured data. So much of compliance and security revolves around documents and screenshots, and now we have an entirely new way to understand and provide value."

The automation advantage

Vanta's most recent The State of Trust Report reveals a striking insight: 77% of IT decision-makers believe automation can relieve the manual burden of compliance, saving them time and money. Yet only 60% of business leaders agree. This gap likely stems from a fundamental misunderstanding of the manual burden faced by security teams, says Epling.

"It boils down to who feels the pain every day. Business leaders are looking at the numbers and the ROI and driving the business, but they're not living in these tools every day and building a deep appreciation for how many hours get sucked into these reviews," he explains. "Governance, risk and compliance has been underserved for a long time in terms of providing a high level of innovation and helping to drive efficiencies."

Businesses are spending more time than ever before on compliance. In the UK, companies already dedicate 12 working weeks per year to keeping operations compliant. Security teams in particular often dedicate far more time to compliance than to other value-adding activities, such as cyber strategy and threat mitigation.

Here, intelligent automation offers multiple operational benefits. "AI can help generate secure code, automate remediation processes and provide a single pane of glass for your entire security programme," Epling says.

> **Intelligent automation enables security teams to be seen as strategic business enablers rather than cost centres**

For example, AI can automatically respond to complex security questionnaires and analyse vendor documents, identifying risks and providing actionable insights. It can also ensure consistency around security policies, as AI can detect irregularities across multiple policy documents. Automated systems can also immediately identify documentation issues, which can help prevent last-minute audit complications.

"Instead of spending hours manually reviewing documents and copy-pasting responses, AI can take a first pass on these tasks," says Epling.

Turning compliance into a business benefit

Perhaps most importantly, intelligent automation enables security teams to be seen as strategic business enablers rather than cost centres. "When you achieve compliance standards, you can unlock new markets and win additional business," Epling says.

He continues: "Automation helps us clearly show time savings and improvements in efficiency. For example, when teams use Vanta's automated workflows, we can quantify how much faster they're completing tasks compared to before. That makes it easy for security leaders to go back to their management and explain the tool's value."

But it's not just security teams that benefit from automation tools, he explains; these systems can also help engineering and IT teams to work more efficiently. "Since they're not in the security trenches every day, giving them focused, actionable remediation guidance, along with context about why it matters, helps them prioritise effectively," Epling says.

And with Vanta's tools, such as automated questionnaires, customers are constantly providing feedback to help the firm improve its programmes.

"It's a way to turn security from a cost centre into a growth enabler," says Epling. "When you can show how your trust posture helps close deals faster or opens new opportunities, it becomes a clear business-value driver. And it bridges the gap between security teams and leadership, so they're finally speaking the same language."

First steps to intelligent automation

For organisations considering intelligent automation, Epling offers some practical guidance.

The first step is to start small – focus on specific areas such as supplier risk or questionnaire management. Then trial AI tools with existing documents and policies, and make sure the AI solutions provide clear citations and explanations.

Epling also advises organisations to consider comprehensive platforms that offer a holistic view of governance, risk and compliance.

"For startups and small businesses, there are tools designed to help you get your first certification," says Epling. "You don't need prior knowledge – the right platform will guide you step by step."

The future of risk management

As cyber threats become more sophisticated and the compliance burdens increase, intelligent automation isn't just a 'nice-to-have' – it's becoming a necessity.

Such automation marks a transformative approach to risk management. By embracing AI-powered tools, organisations can not only mitigate risks more effectively but also turn compliance into a strategic business advantage.

"The goal is to spend less time on paperwork and more time on deep, impactful security work that truly protects your organisation," says Epling.

As cyber threats continue to evolve, the message is clear: intelligent automation isn't just a technological upgrade – it's a critical component of your security strategy.

77% of IT decision-makers believe automation can relieve the manual burden of compliance

60% of business leaders agree

For more information please visit vanta.com

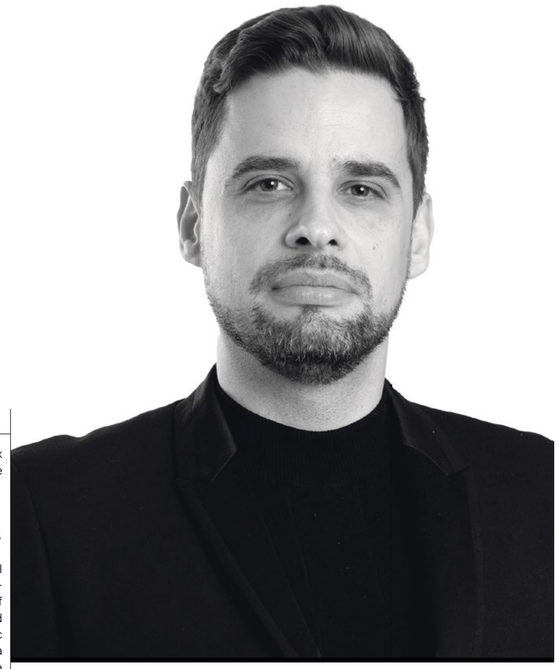
Vanta

Commercial feature

Q&A

Why digital identity needs a new baseline

As identity threats grow more sophisticated, trust is no longer a one-off check – it must be verified continuously and intelligently, says **Adam Preis**, director of product-solution marketing at Ping Identity



In the early days of digital identity, trust was a starting point: you logged in once, verified your credentials and got on with your journey. But in today's rapidly evolving threat landscape, where AI-generated deepfakes, identity fraud and third-party breaches are growing exponentially, trust must be earned continuously.

Adam Preis, director of product-solution marketing at Ping Identity, reveals how digital trust is evolving, and what it takes to build meaningful, secure digital relationships with customers, partners or AI agents.

Q How has the concept of digital identity evolved?

A Digital identity has transformed dramatically over the past two decades.

Initially, identity and access management (IAM) was simply about allowing the workforce to log into systems and applications. But around 12 years ago, the introduction of identity federation standards revolutionised access by enabling logins through third-party identity providers, such as Google and Facebook.

Put simply, users no longer needed to create, store and use unique credentials for each application. This shift enabled more seamless and secure access, paving the way for frictionless digital experiences and expanding the role of identity in consumer-facing applications.

Q How do you define 'verified trust' in today's digital landscape and why does it matter?

A Verified trust has shifted from a 'trust then verify' approach to a 'verify first, then trust' model.

With the emergence of sophisticated attack vectors – including fraud, deepfake content and AI-powered impersonation – organisations must be able to verify a user's identity with greater certainty, especially as risk levels fluctuate across the user journey. These evolving threats make fraud detection, response and prevention significantly more challenging.

In the age of AI, verification should involve matching identities against trusted 'anchors' – such as government digital identity schemes, bank ID systems or decentralised wallet-based verified-credential schemes – and implementing robust liveness detection. This means not only verifying credentials at onboarding but also continuously assessing risk signals throughout the user journey and introducing step-up identity verification when needed.

Today, identity is quickly becoming the security perimeter, whether you're a worker logging into secure corporate systems or a consumer accessing sensitive services such as banking or healthcare.

Q What role does identity play in customer retention and churn?

A IAM directly impacts customer experience because poor verification processes create friction that frustrates users. In fact, complex onboarding, multiple login requirements and inconsistent authentication across channels, such as mobile apps, web platforms, call centres and hybrid physical-digital touchpoints, can drive customers away. Businesses that can create smooth, secure and flexible identity experiences, with options for verification and clear data-privacy controls, are more likely to retain customers.

Q How do AI-generated deepfakes challenge traditional IAM strategies?

A AI-generated deepfakes have dramatically increased the sophistication and prevalence of identity fraud. Malicious actors can now create highly convincing fake identities, voices and even entire video-conferences. A notable example is a Hong Kong case where criminals used deepfake technology to convince executives to transfer $25m by impersonating company leadership.

Again, this means that traditional IAM strategies that rely on static credentials or simple multi-factor authentication are no longer sufficient. Organisations must instead consider advanced verification technologies that can detect, respond to and prevent AI-generated fakes, using a myriad of first- and third-party risk signals in real time across the entire user journey.

Q How should organisations approach the rise of AI agents with digital identities?

A Organisations must treat AI agents as entities with distinct identities that act on behalf of users, requiring clear, user-granted authorisation to access specific identity attributes and personal data for narrowly defined tasks within a limited timeframe.

This should include giving AI agents specific, time-limited access to defined data sets, implementing granular authorisation controls, securing API access for AI interactions and continuously monitoring and verifying AI-agent activities.

Customers should also have control, such as granting an AI agent access to only a limited portion of their profile for a specific task, for a period of time. As an example, identity-enabled AI agents in consumer banking will allow these agents to perform specific tasks, such as finding better mortgage rates or recommending savings products, all while respecting the customer's defined permissions.

More than anything, you should create a framework that enables AI agents to operate effectively while maintaining robust security and privacy controls.

Q How can businesses introduce verification without adding friction?

A The key is to understand that poorly designed identity experiences can drive customers away. Businesses that recognise this are the ones successfully finding the right balance – it's not about removing all friction but using it wisely and only where it adds value or trust.

Strategies such as introducing delegated authorisation and policy-based access control are helping to redefine this balance. For example, if I want to give my daughter access to my current account but limit her to a certain spending amount, I should be able to do that securely and seamlessly.

This concept can be extended to more complex scenarios, such as delegating authority through a power-of-attorney arrangement in healthcare or legal contexts. It also applies to, for instance, mortgage or insurance processes, enabling seamless identity delegation between customers, brokers and providers without requiring users to navigate cumbersome verification steps.

Q What's next for digital trust – are we moving towards a trust-as-a-service model?

A We're seeing the early signs of a shift in that direction. A lot of organisations, particularly in the financial sector, are starting to realise that their trust and identity-verification capabilities can be monetised.

Some banks in Europe are exploring decentralised identity, particularly wallet-based technologies. These systems enable users to hold verified credentials on their devices, proving their identity during transactions without relying on a centralised database. With a trust anchor in place, users can, for example, confirm their age or address, without revealing personal details. This provides them with greater control over how they share and revoke access to their credentials while reducing the risk of data breaches and fraud.

In this emerging model, banks and other trusted institutions can function as trust anchors. That means they can both verify a person's identity and offer those verification services to third parties. This enables new systems that deliver verification-as-a-service.

Regulatory momentum is accelerating this trend. In Europe, new regulations such as eIDAS 2.0 and the European Digital Identity Wallet will soon come into force. By November 2027, businesses must be able to accept the digital wallet for customer identification and authentication.

This is going to be a huge push towards decentralised identity and will likely open the door for trust-as-a-service models. Over the next three years, as both the public and private sectors align on this vision, we will see a shift towards more secure, seamless experiences. Verified trust will play a central role in safeguarding consumer, workforce and third-party identities, driving more secure and frictionless interactions across all digital touchpoints.

> Verified trust has shifted from a 'trust then verify' approach to a 'verify first, then trust' model

For more information please visit pingidentity.com

Ping Identity.

400tmax / via Getty Images

GLOBAL THREATS

Trump's cybersecurity cuts put US allies on guard

Global cybersecurity efforts risk being undermined as the US government enacts sweeping cuts and leadership shake-ups at its top cyber agencies

Tamlin Magee

With sweeping tariffs causing economic chaos and combative rhetoric flowing from the White House, the Trump administration is disrupting business-as-usual at home and abroad.

Cybersecurity operations have not been immune to the turbulence. In March, Pete Hegseth, the US defence secretary, reportedly ordered a pause to offensive cyber operations against Russia. The Pentagon denies this claim.

Meanwhile, Timothy Haugh, head of US Cyber Command (the military command in charge of cyber operations) and chief of the US' signals intelligence agency, the NSA, was dismissed in early April along with his deputy. And the government efficiency department, led by Elon Musk, is taking aim at the US cybersecurity and infrastructure security agency (Cisa), threatening to axe nearly half of its staff.

Cisa, which sits within the US department of homeland security, oversees cybersecurity and infrastructure protection across the government. It is responsible for evaluating cyber threats and coordinating proactive responses.

In an April memorandum, the Trump administration accused Cisa of leading "government censorship against Americans", alleged that it censored "election information" and called the former director, Chris Krebs, a "significant bad-faith actor who weaponised and abused his government authority".

The administraion also revoked security clearances for Sentinelone, a private sector cybersecurity vendor. The company had appointed Krebs as chief intelligence and public policy officer shortly after he was fired by the US president for contradicting his false claims of voter fraud in the 2020 US election.

This politicisation of cybersecurity in the US could prevent Washington and its allies from sharing essential security information and limit their abilities to combat emerging threats, according to Laura Houston, a partner at Slaughter and May, a law firm.

"Three months into Trump's second term, it's increasingly clear that cybersecurity is not a priority for the administration," she says. "They aren't denying the prevalance of threats, and they have extended the long-standing national emergency declaration concerning cyber risk. But there are still no Senate-confirmed cybersecurity leaders in the Pentagon, the head of US Cyber Command has just been fired and Cisa's workforce is being significantly reduced."

According to reports, Cisa plans to remove 1,300 employees from its payroll, motivated by the push for greater efficiency in the federal government. Plus, the Trump administration has proposed cutting $491m (£368m) of funding for the agency in the 2026 budget.

Brandon Wales is the former acting director of Cisa and now works at Sentinelone. He says that how such cuts could impact Cisa's work is unclear. But, if the numbers are anything close to those appearing in the press, the reductions in headcount or funding could hamper the agency's ability to support federal, state and private sector organisations through cyber incidents.

Most concerning, according to Wales, is what the cuts could mean for Washington's capacity to share cybersecurity information. "A lot of information on threats and best practices is critical to the way we collectively defend the country."

However, Wales admits that the man nominated to replace Krebs at Cisa, Sean Plankey, appears to be up to the task. He has plenty of real-world experience, having served as director for cyber policy in the first Trump administration.

Wales adds that despite the "policy turmoil", collaboration between international law enforcement organisations, such as the FBI, Europol, the Secret Service and Interpol, will remain strong. "That work is continuing and that's good because those relationships should be deeply institutionalised, so that no matter what else is happening, the important collaboration will continue," he says.

But others further from the US halls of power take a dimmer view. According to Matthew Hodgson, the CEO and co-founder of Element, a privacy company, the gutting of Cisa will "obviously compromise the US' ability to defend itself".

He believes that the administration's "attack" on US cybersecurity services undermine their dependability. "Concerns were raised last year about Cosy Bear [a Russian threat group] and other attacks on critical infrastructure. It really shifts the onus to individual countries to protect their own infrastructure and services," he says.

These moves by the US will push the rest of the world to ensure their own security, rather than depending on American tech services, Hodgson explains. Already, European nations are working to develop their own digitally sovereign tech stacks.

Although the US defence department denies reports that it has ceased offensive cyber operations against Russia, the news nonetheless rattled some figures in the European cybersecurity sphere.

Tom Vazdar, a cybersecurity professor at the Open Institute of Technology and former security adviser at Europol, says that if the reports are accurate, they could signal a significant policy shift, where old alliances disintegrate and new ones are created. He suggests the cyber diplomacy at play with Russia could usher in a reformulation of such alliances, redirecting the US' offensive capabilities towards China.

But a US withdrawal from engagement with Russia would "really reduce critical intelligence sharing," says Vazdar.

"Nato and European nations fear increased cyber aggression from Russia. This could prompt Europe to independently develop more robust offensive cyber capabilities," he explains. "It's obvious that the days of the US leading the free world are gone."

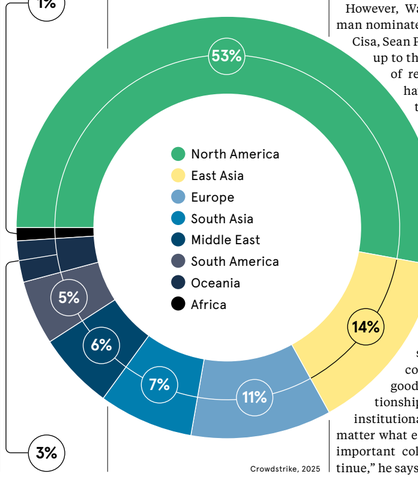
By repeatedly failing to condemn Russian cyber aggression, Vazdar says, the US has "undermined all international norms against cyber attacks" while simultaneously "diluting deterrent strategies" – something he believes adversaries including China, Iran and North Korea may notice. "They may interpret the shift in US policy as a green light for increased cyber activity," he says.

Cooperation among international security agencies has been essential for taking down key figures in notorious ransomware gangs, including Conti, Lockbit and Phobos. If the US government limits its intelligence-sharing, or weakens its threat detection or international coordination, other countries will also become more vulnerable to such threats. "If you don't have active personnel working 24/7 on monitoring what adversaries are doing, then it's going to be really tough to rebuild everything from scratch," Vazdar says.

The Trump administration's handling of US cybersecurity therefore is not just a domestic matter. Any major recalibration of America's cybersecurity priorities poses risks for the rest of the world too.

ATTACKERS ARE ACTIVE IN NORTH AMERICA

Relative frequency of interactive intrusions in major geographical regions



Crowdstrike, 2025

THE RACONTEUR

50

Recognising those who lead.

The role of the modern-day CEO is evolving. It is no longer enough to focus solely on profit, revenue or share price. Leaders must balance financial performance with employee wellbeing and ESG concerns, finding ways to innovate and grow at a time of deep uncertainty and turmoil.

Across five categories, we hope that by shining a spotlight on the best business leaders, we can offer insights into what it takes to lead from the top and inspire the CEOs of the future.

Meet the 50 CEOs changing British business.

raconteur.net/raconteur50

Raconteur