Bridewell

Cyber Security. Where it Matters.

Cyber Security in Critical National Infrastructure 2025 Research Report

Contents

Foreword

As in previous years, our 2025 Cyber Security in Critical National Infrastructure (CNI) report sets out to understand how UK CNI organisations perceive the current threat landscape, assess their own levels of cyber maturity, and where they believe they must improve. Since our first report in 2021, there have been significant changes in the industry, which we've reflected with new areas of focus in our survey questions.

What's New in our 2025 Survey?

New for this year is unsurprisingly AI, which, for better or worse, has been an inescapable talking point across the industry. Several of our questions look at what AI threats respondents are concerned about, and how they are currently using AI themselves.

Additionally, with our 2024 Cyber Security in CNI report finding greater levels of concern around data privacy, we've added additional questions to understand what specific concerns CNI organisations share in this area. Other areas we've dived further into this year are supply chain risk, operational technology, and risk assessments.

Key Findings

The top challenges facing CNI organisations are consistent with last year – mainly being data privacy, cyber resilience and cloud security. Confidence in cyber security has increased slightly, as has levels of outsourcing for cyber security and managed security services.

We also continue to see that a third of breached CNI organisations have paid a ransom, which is dangerous territory to be in, as they risk conducting transactions with sanctioned entities. Once the UK government's public consultation ends in April this year (2025), such activity could be the subject of legislation, with the imposition of penalties.

The research also found incident response times continue to be far too slow, despite small improvements. When anything more than an hour can cause problems, it is not reassuring that 69% of CNI organisations are responding to ransomware incidents within six hours.

Uncovering Contradictions in CNI

It's important to remember that this report only uncovers what CNI organisations think and perceive – the findings don't always correlate to real threats, trends or capabilities. Our survey results for this year have uncovered a number of contradictions.

For example, 90% of respondents are confident their organisation's current cyber risk assessment approach accurately reflects their security posture, yet lack key capabilities to truly assess risk. Likewise, we found 84% of respondents are confident about the protection for their cloud-based infrastructure, yet 40% are also worried about cloud services being a potential avenue for attacks on their IT environments.

> "It is not reassuring that 69% of CNI organisations are responding to ransomware incidents within six hours"

Methodology

In January 2025, Bridewell commissioned international market research consultancy Censuswide to conduct research among 605 respondents who have responsibility for cyber security in the UK's critical national infrastructure organisations.

These professionals are from the following sectors:

- Central government
- Energy
- Water supply and treatment
- Telecommunications
- Civil aviation
- Financial authorities (including HM Treasury, Bank of England, Financial Conduct Authority and Prudential Regulation Authority)
- Financial services organisations including banks and payment systems
- Insurance
- Internet service providers
- Local government organisations
- Maritime
- Rail and road transport
- Broadcast media

All respondents to the 38-question survey were sourced and completed through online panels.

The Threat Landscape

The Security Challenges

What, if anything, are your biggest cyber security challenges at present? (Select up to five)

Challenge	2025	2024	2023	% increase 2024-2025
Data protection and privacy	41%	37%	18%	11%
Improving cyber resilience	36%	34%	21%	6%
Managing cloud cyber security	34%	32%	17%	6%
Ability to quickly detect incidents	32%	19%	19%	68%
Protecting our critical assets	31%	30%	18%	3%

Almost all respondents (98%) say they have security challenges in 2025, and 95% admit they have experienced a breach in the last year.

The top three challenges in 2025 remain consistent with 2024, but the overall percentage of companies battling these issues has increased. And while trust in cyber tools leapt into the top five in the 2024 report, it has dropped out this year (29% this year compared with 31% in last year's survey), replaced by the need to detect incidents quickly.

Data protection remains high on the agenda because of the intense pressure of regulations such as NIS and **DORA** on operators of essential services (OESs), along with the growing use of AI applications, especially in relation to customer data.

The UK's **NIS regulations** focus on network and information systems, and digital service providers. They derive from the EU's **NIS2 Directive**, setting out cyber protection objectives with financial penalties for non-compliance of up to £17m.

The EU's DORA regulations are designed to increase the financial sector's cyber security through stringent IT requirements, third-party risk-management and incident reporting. Infringement also carries the risk of substantial financial penalties. Both bodies of regulation impose significant reporting demands in the event of an incident.

The focus on data protection and privacy is strongest among energy businesses where it is a top-five challenge for 48% of respondents. Energy companies increasingly have significant amounts of customer data from the expansion of smart meter use in homes and businesses. This is a highly valuable resource they are using in AI applications to hone pricing strategies and increase organisational efficiency.

Loss of this data through a cyber attack could be extremely serious because of the volume of sensitive information involved. This includes the personal details of elderly and disabled people who are more susceptible to various types of fraud using their information.

To protect their data, energy companies need to start with more robust privacy-based risk assessments and reviews. With access to expert cyber security consultancy, they can establish their risk appetite and implement **data loss prevention** solutions based on policies that relate to their precise needs and usage patterns.

To counter the potential for data loss, many organisations are adopting data governance solutions such as **Microsoft Purview**. This enables the classification of data and imposition of pragmatic controls to reduce the risk of losing data outside the organisation through emails, use of USB sticks, printing or generative AI applications.

Data loss is not uniformly the most frequently cited concern, however. Among 50% of finance authorities, including the Bank of England, Financial Conduct Authority and the Prudential Regulation Authority, improving cyber resilience is a top-five challenge. This is to be expected when these regulators monitor cyber resilience across banks and financial infrastructure using CBEST thematic reports. Cyber resilience improvement is also an important element in meeting **Cyber Assessment Framework (CAF)** milestones.

The Threat Landscape

Cyber Attacks Remain Highly Varied

Approximately how many, if any, of the following have you suffered from in the past 12 months?

Type of attack	2025	2024	2023	% increase 2024-2025
Phishing	14	17	21	-18%
Malware	9	11	21	-18%
Unauthorised system access	7	17	21	-59%
Physical security breach	7	7	21	0%
Distributed denial of service (DDoS)	7	8	20	-13%
Social engineering	7	9	20	-22%
Supply chain attacks	6	8	21	-25%
Ransomware	6	8	21	-25%
Data theft or disclosure	6	8	20	-25%
Employee sabotage	5	8	21	-38%

The mean number of attacks suffered by UK CNI organisations dropped compared with 12 months ago, but organisations are still subject to a wide range of cyber attacks. The decline in attacks is likely to relate to many organisations strengthening their cyber defences.

Phishing was nevertheless among the three most common types of attack or incident that organisations experienced, along with malware and unauthorised access to systems. Although companies are more clued-up on **how to combat phishing** and have undertaken extensive staff training, human error remains an important factor. A successful phishing attack is often the precursor to a ransomware or malware attack. It therefore remains extremely important for organisations to take phishing seriously to avoid significant consequences.

To avoid complacency, it is also worth remembering that these statistics are averages. Many organisations will have experienced far greater volumes of attacks. For example, 69% of respondents said their organisation experienced anything between one and 50 phishing attacks during 2024.

Percentages of UK CNI organisations experiencing up to 50 of the following types of attack in the last 12 months	%
Malware	71%
Phishing	69%
Unauthorised system access	64%
Physical security breach	55%
Distributed Denial of Service (DDoS)	56%
Social engineering	55%
Supply chain attacks	57%
Ransomware	53%
Data theft or disclosure	56%
Employee sabotage	48%

> **“69% of respondents said their organisation experienced anything between one and 50 phishing attacks during 2024.”**

The Threat Landscape

The Risk to IT Environments

What, if anything, are the main avenues of cyber-attack in your IT environments at present? (Select up to five)

Avenue of attack	2025
Cloud services	40%
Web browsing/ internet access	37%
Business email	33%
Remote access services	33%
Weak user credentials	32%
Unauthorised/ unmanaged devices	30%
Unpatched vulnerabilities	28%
Wireless networks	28%
Internet-facing devices/ applications	27%
Removable media	25%
IoT Devices	25%
Supply chain	23%
I don't think there are any avenues of cyber attack	3%
Not sure	1%

Only 3% of respondents believe their organisation's IT environments offer no avenues of attack to cyber criminals. While this percentage is small, these CNI organisations should revise their stance and obtain support immediately, given that 95% of respondents in this report experienced some form of breach last year.

Cloud services were the most feared avenue of attack. Respondents working in central government were especially worried about cloud services as a source of attacks (47% of respondents).

Cloud services are not highest on everyone's list, however. In financial services, for instance, this research found that web browsing and internet access are of particular concern, cited by 44%. In civil aviation it is weak user credentials that feature heavily, referenced by 43%.

> "Only 3% of respondents believe their organisation's IT environments offer no avenues of attack to cyber criminals"

The Threat Landscape

Threats to IT Environments in 2025

What, if anything, do you identify as the most significant cyber threats to your IT environments in 2025? (Select up to five)

Threat	2025	2024
Malware	41%	N/A
Phishing	39%	N/A
Cloud platform attacks	36%	30%
Ransomware	32%	N/A
Supply chain attacks	27%	26%
Advanced persistent threats (APTs)	25%	19%
Remote working vulnerabilities	24%	27%
IoT device vulnerabilities	22%	24%
Social engineering	21%	20%
Zero-day exploits	19%	16%
None	2%	3%
Not sure	1%	2%

Malware and phishing are the two attack types most frequently viewed as a threat to CNI organisation's IT environments, with results largely remaining consistent with last year's survey. The outlier is APTs, which is cited by one-quarter (25%) of respondents as a significant threat to their IT environments in 2025, an increase on the 19% that referenced it last year.

The Threat Landscape

Responding to Threats

What is the average time taken to respond to a cyber event?

Type of attack	Percentage within six hours in 2025 survey	Percentage within six hours in 2024 survey
Ransomware	69%	68%
Supply chain attacks	70%	66%
Data theft or disclosure	69%	66%
Physical security breach	73%	68%
Malware	73%	76%
Phishing	73%	73%
Unauthorised access by employee	74%	67%
DDoS	73%	66%

The longer an attack persists before an organisation remediates it, the greater the potential damage. This research found average response times were similar between different types of attack but encouragingly, organisations have improved their speed overall compared to last year's survey.

This is reflected in the 22% of organisations that respond to a ransomware attack within an hour, 21% achieving the same response time for data theft or disclosure, and 20% for supply chain attacks.

Among the different sectors surveyed, the water industry stands out for its response time to incidents of data theft or disclosure. Half (50%) of respondents from this industry say they can respond to such incidents within an hour, compared with an average of 29% across all organisations surveyed. In insurance, 35% of respondents said their organisation is capable of responding to ransomware attacks within an hour, compared with just 12% in the rail industry.

Overall, this paints a mixed picture. Whilst clearly improvements are being made, most response times are far too slow for a modern enterprise, where anything beyond an hour can lead to significant problems. We would expect a **modern SOC (security operations centre)** to respond to threats within 60 minutes.

The Aggregated Annual Cost of Cyber Attacks and Data Breaches

The costs of dealing with every cyber attack or data breach constantly mount. Last year, Microsoft found the cost of cyber attacks to small and medium-sized businesses in the US and UK to be anything from $254,000 to $7 million. The 2024 IBM Ponemon Cost of a Data Breach report found the global average cost to be $4.88 million, after a 10% increase – the largest annual leap since the pandemic.

The Threat Landscape

Over the course of the last 12 months, what has been the average cumulative cost of every attack or breach suffered by your organisation

Cost	2025	2024
£0	6%	3%
£1-£10,000	11%	13%
£10,001-£50,000	12%	14%
£50,001-£100,000	11%	14%
£100,001-£200,000	11%	11%
£200,001-£300,000	10%	7%
£300,001-£400,000	10%	7%
£400,001-£500,000	6%	6%
£500,001-£600,000	6%	6%
£600,001-£700,000	4%	4%
£700,001-£800,000	3%	2%
£800,001-£900,000	1%	2%
£900,001-£1,000,000	2%	3%
Not sure	5%	7%

In this research 45% of UK CNI organisations suffered costs of up to £200,000 – down from the 52% in the 2024 report. A lucky 6% have experienced no costs from attacks or breaches in the previous 12 months. Some 16% struggled with costs between £500,000 and £1 million, similar to the 17% last year.

> “In this research 45% of UK CNI organisations suffered costs of up to £200,000”

Breaking Down the Cost of Cyber Attacks and Data Breaches

The costs for those who experienced a breach, or breaches, arose from many different sources.

> “Respondents citing downtime and disruption as the primary cause of costs shot up by 6%”

What contributed most to the cumulative cost of each attack or breach your organisation suffered over the last 12 months?

Cost	2025	2024
System recovery and repair	29%	28%
Upgrade of cyber security measures	29%	26%
Increased operational costs	29%	24%
Loss of intellectual property or sensitive data	17%	23%
Employee productivity loss	28%	21%
Downtime and operational disruption	27%	21%
Regulatory compliance and reporting costs	21%	21%
Litigation costs	15%	20%
Reputational damage	21%	20%
Incident response and investigation	25%	20%
Legal costs and fines	21%	20%
Increased insurance premiums	18%	20%
Ransom payments	18%	19%
Supply chain and partner impacts	19%	16%
Customer compensation and retention efforts	23%	15%

Although some primary consequences of attacks and breaches fell, such as litigation, loss of intellectual property or sensitive data, most increased year-on-year, including overall legal costs and fines. Respondents citing downtime and disruption as the primary cause of costs shot up from 21% in the 2024 report to more than a quarter (27%) in this report.

The Threat Landscape

Ransomware Attacks

What has been the typical cost associated with a ransomware attack on your business?

Cost	2025	2024
£0	0%	1%
£1-£10,000	5%	10%
£10,001-£50,000	13%	12%
£50,001-£100,000	13%	13%
£100,001-£200,000	10%	11%
£200,001-£300,000	13%	10%
£300,001-£400,000	12%	9%
£400,001-£500,000	8%	8%
£500,001-£600,000	10%`	8%
£600,001-£700,000	6%	5%
£700,001-£800,000	5%	2%
£800,001-£900,000	2%	3%
£900,001-£1,000,000	3%	5%
Not sure	1%	2%

Although this survey found the average number of ransomware attacks dropped compared to last year, ransomware remains a dangerous threat. A single ransomware attack can be extremely expensive. The survey found 37% of respondents' organisations bearing costs of more than £500,000, compared with 25% in the 2024 survey.

We know ransomware is increasingly professionalised into specialisms as organised crime moves into the sector. The continued development of RaaS (ransomware-as-a-service) is a symptom of these malign developments.

> "The survey found 37% of respondents' organisations bearing costs of more than £500,000"

The Threat Landscape

Events and Technologies

Rate your level of concern regarding these future events/nation state threats in 2025

Event or threat	2025	2024
Economic turbulence	75%	79%
China state-linked actors	69%	74%
Global health crisis	72%	73%
Russia state-linked actors	72%	73%
The crisis in Gaza	66%	73%
Iran state-linked actors	66%	69%
Climate-change related conflicts	67%	66%
North Korea state-linked actors	65%	63%
The US presidential election	61%	62%

Levels of concern about the wider impacts and after-effects of global events are significant but have dropped slightly over the past 12 months. Economic turbulence is still the most prominent concern, followed by the fear of another global health crisis, whilst understandable concerns about the cyber activities of Russian state-linked actors remain.

The Threat Landscape

Cyber Protection – Different Approaches

Which technologies or approaches do organisations plan on using to defend themselves – and when?

When, if ever, do you plan to implement the following?

> **“88% have board level representation for cyber or plan to implement it in the next 24 months.”**

	2025 percentage planning to implement within 24 months or already implemented	2024 percentage planning to implement within 24 months or already implemented
An effective and audited information security management system for IT	92%	90%
An effective and audited information security management system for OT	91%	89%
24/7 security monitoring on IT	91%	89%
24/7 security monitoring on OT	91%	89%
Hybrid security operations centre (SOC) services on IT	90%	87%
Hybrid security operations centre (SOC) services on OT	90%	85%
Managed detection and response on IT	91%	89%
Managed detection and response on OT	91%	87%
Threat hunting and cyber threat intelligence	92%	85%
Cyber security strategy aligned to business objectives	91%	88%
KPI and value levers for cyber security	90%	87%
Board level representation	88%	88%

The threats facing critical infrastructure organisations are constantly shifting in scale and technology, with adversaries well-resourced, highly motivated or incentivised. This year, 90% or more of all CNI organisations surveyed have either already put measures such as security operations centres in place, or will do so within the next two years. The only exception is **boardroom representation for cyber security matters**, but even here, the vast majority of organisations are represented at 88%.

As emphasised in our previous reports, conventional tools should be combined with more comprehensive approaches that include changing internal culture – such as more cyber security boardroom representation.

Confidence

Confidence in Protection Rises Again Amid Proliferating Risks

How confident are you, if at all, that the following systems within your organisation are protected from cyber threats?

System	2025	2024	2023
End user devices are secure	83%	82%	65%
Identity providers	87%	87%	68%
Cloud-based infrastructure	84%	83%	68%
SaaS applications	86%	83%	69%
IT/ OT boundaries are protected	87%	84%	67%
SCADA systems are protected	N/A	78%	66%
On-premises infrastructure and services	90%	85%	65%
OT or operational control systems	87%	84%	67%

Confidence in the cyber protection of systems and infrastructure has remained largely constant from last year, following notable increases between the 2023 and 2024. The volume of successful attacks in 2024 is evidence that this high level of confidence heading into 2025 is potentially misplaced.

Many respondents in this survey (40%), for example, are worried about cloud services being a potential avenue for attacks on their IT environments, yet 84% are confident about the protection for their cloud-based infrastructure.

Confidence in Cyber Risk Assessments is High

How confident or not confident are you that your organisation's current cyber risk assessment approach accurately reflects your cyber risk posture?

Level of Confidence	Percentage
Not confident (Net)	9%
Not confident at all	1%
Not very confident	7%
Somewhat confident	48%
Very confident	42%
Confident (Net)	90%

> "The volume of successful attacks in 2024 is evidence that this high level of confidence heading into 2025 is potentially misplaced."

Confidence

Which of the following best describes your current approach to cyber security risk assessment?

Approach	Percentage
We identify potential threat vectors to assets/data and compare the strength of threats that may traverse each vector against the effectiveness of controls along each vector.	25%
We assess against a standard set of security control measures and evaluate the risk of any control gaps or deficiencies.	22%
We assess against pre-defined risk scenarios by considering the effectiveness of controls in place to protect against each scenario.	19%
We perform vulnerability assessments and evaluate the risk of any vulnerabilities discovered.	18%
We risk assess any weaknesses as and when we discover them.	13%
We don't assess cyber security risks.	3%

Overall, the responses to these two questions are further evidence of excessive confidence about cyber security risk assessments. While 90% of respondents express confidence, in insurance the figure is 100%.

Unfortunately, current approaches to cyber risk are failing – as witnessed by the sheer volume of breaches organisations experience. Too many organisations lack real insight into the cyber risks they face.

Only 25% are conducting valid assessments by identifying threat vectors and assessing controls against each of them. Anything other than this approach is not an effective risk assessment. The 19% who employ pre-defined risk scenarios and the 18% relying on vulnerability assessments are conforming to a risk-register-centred approach which leads to concentration on single problems at the expense of the whole.

The only way to assess risk effectively is across all threat vectors and attack pathways. Fortunately, the international standards bodies have woken up to the shortcomings in approaches to cyber risk assessments and are updating their requirements.

> **“While 90% of respondents express confidence, in insurance the figure is 100%”**

Confidence

Cyber Maturity

Where do organisations feel they are in their cyber maturity and what is driving it – fear of regulatory penalties, new technology or new threats? This is something we have examined for the last three years through our CNI research.

Which of the below best describes your organisation's maturity in relation to implementing a cyber security strategy, achieving key goals and measuring performance for the following?

Level of maturity in IT	2025	2024	2023
Mature (Net)	90%	89%	89%
Very mature	44%	38%	42%
Somewhat mature	46%	50%	47%
Not very mature	9%	10%	10%
Not mature at all	2%	1%	1%

And in **OT** the assessments were:

Level of maturity in OT	2025	2024	2023
Mature (Net)	88%	86%	89%
Very mature	34%	29%	37%
Somewhat mature	53%	57%	52%
Not very mature	11%	13%	10%
Not mature at all	2%	1%	1%

The data shows organisations feel generally well-advanced in maturity. In IT and OT, the percentages assessing themselves as "very mature" have grown since last year, but still not reached the levels they were back in 2023. This confidence does not correlate with some of the other findings in this year's survey that point to lack of cyber maturity, such as the numbers of breaches.

Confidence

Where, if anywhere, is the greatest pressure to improve cyber maturity coming from? (Select up to three)

Pressure	2025	2024
Regulation - need to meet changing regulatory requirements	26%	29%
The business - desire to support new technology and digital initiatives	25%	26%
Employees - support the shift to hybrid & remote working	22%	23%
Increased connectivity - threats have greater potential to exploit critical assets	25%	23%
Threat landscape – evolving cyber threats	24%	22%
My team - greater understanding of our cyber security deficiencies	24%	22%
Finance - need to reduce security costs	24%	20%
Customers - increasing demand for improved security	21%	19%
Competitors - need to maintain competitive advantage	21%	18%
The board - need to demonstrate ROI	20%	18%
Myself - fear of losing my job if I don't drive improvements	15%	17%
There is no pressure to improve cyber maturity	4%	4%

Changing regulatory requirements remain the most common pressure to improve cyber security maturity, which is understandable given some of the updates introduced in the last 12 months.

The need to reduce security costs has seen the biggest increase as a driver of cyber maturity, rising from 20% of respondents to 24% - reflecting the current financial pressures on many CNI organisations. Tied in with this is the desire of CNI boards to see some return on their investment in cyber security – a pressure that has also increased.

Depending on the level of maturity, the process of demonstrating such ROI can begin with a **cyber security audit**, assessing an organisation's sector-specific risks and challenges, and examining **compliance of suppliers** with regulatory obligations. With assistance from external experts, IT and OT teams can consolidate their tools to extract greater value.

Another area where maturity pressures have increased compared with last year's report is around the growth in connectivity and the potential it creates for more attacks. The fear of losing their job is, however, less of a maturity driver than last year among cyber security decision-makers surveyed.

> **"The need to reduce security costs has seen the biggest increase as a driver of cyber maturity, rising from 20% of respondents to 24%"**

Confidence

Outsourcing Cyber Security

Outsourcing offers CNI organisations the opportunity to upgrade their cyber security even though internal skills and expertise are absent or deficient.

To what extent, if at all, are you outsourcing the following cyber security services for IT?

IT	2025 Outsourced fully or partially	2024 Outsourced fully or partially
Security Operations Centre	52%	50%
Threat intelligence	59%	54%
Digital forensics and incident response	56%	44%
Managed detection and response	53%	54%
Vulnerability management	54%	55%
Data privacy services	55%	55%
Cyber security training	60%	57%
Penetration testing	58%	55%
Cyber security audits	59%	57%

This year's report finds outsourcing in IT has shown signs of a resurgence compared to 2024. The use of **digital forensics and incident response** is significantly higher – by 12 percentage points. Many areas, however, remain much the same.

The findings reveal only 58% of organisations outsource penetration-testing to simulate a cyber-attack, enabling them to gain insight into the effectiveness of their defences. Very few CNI organisations are likely to have these capabilities in-house, which makes this finding surprising. The worrying truth may be that organisations not outsourcing penetration-testing are neglecting what is an important security activity.

Although only 2% of organisations in the survey admitted they are not conducting any penetration-testing, which might suggest many organisations are indeed attempting to test themselves, likely at an inadequate level. The need to cut costs is potentially having a direct impact on this decision.

Outsourcing cyber security is important when cyber skills remain at a premium and threats are steadily becoming more dangerous and demanding in the CNI world. CNI organisations may have people who can complete risk assessment services and cyber security audits, but shortages of skills in security architecture and engineering will continue to be a problem, especially as AI use expands. The active strengthening of internal capabilities or collaborating with knowledgeable partners will position organisations to adapt with greatest effect.

AI

The AI Arms Race in the Cyber-sphere

We are still in the early phases of AI-driven cyber attacks, but CNI organisations are fully aware of their potential. Conversely, organisations are already employing AI tools to improve their defences and accelerate responses.

Rate your level of concern of the following emerging AI-driven cyber threats in terms of threat to your organisation

AI-driven threat	2025 percentage registering high and slight levels of concern	2024
Polymorphic malware	73%	73%
AI-powered phishing attacks	83%	78%
AI-driven exploit development	77%	78%
Deepfake technology	74%	76%
Automated hacking	78%	78%
AI-powered botnets	78%	76%
Manipulation of machine learning models	75%	73%
Data poisoning	76%	76%
Evasion of anomaly detection systems	76%	75%
AI-driven social engineering	77%	75%

Concern about the potential of AI to cause harm to the business became even more prevalent over the course of 2024. AI-powered phishing is now out on its own as the most frequently cited threat backed by AI. The technology enables cyber criminals to write more convincing emails at scale for phishing campaigns and also complements their coding skills so they can create more sophisticated malware.

The survey highlighted once more that AI-driven threats are sources of concern for seven-in-ten or more respondents, with no threats showing any significant decline in concern. Deepfakes and AI-driven exploit development were the only AI-powered tactics of less concern now than a year ago, but the differences are small.

AI

Which, if any, AI-driven tools do you primarily use in your operations? (Select up to five)

AI-driven tools respondents primarily use:	2025	2024
Chatbots and AI assistants for cyber security operations	32%	32%
AI-powered threat intelligence platforms	28%	29%
Automated penetration testing and vulnerability management	23%	28%
AI-driven data loss prevention	30%	28%
AI-enhanced endpoint protection	28%	27%
AI-based phishing detection and prevention	27%	27%
Predictive analytics for cyber security	24%	26%
Deep learning for malware analysis	25%	25%
Network behaviour analysis	27%	24%
Secure access service edge	22%	24%
Automated incident response solutions	26%	23%
Anomaly detection systems	26%	23%
User and entity behaviour analysis	23%	21%
None	5%	4%

This year's findings reveal few dramatic increases in the use of AI-driven tools. Cyber security chatbots are still the most popular, followed by data-loss prevention tools, but no single technology has widespread implementation. Some 5% of organisations still use no AI tools. These tools have immense potential to save time and increase accuracy in many areas, including monitoring and detection.

Organisations should, however, be wary of the unrestrained use of generative AI by employees. This is often unauthorised "shadow AI" which risks the input of sensitive data into commercially available large language models. This inputted data may reappear later when other users employ the same application to draft content or answer queries, risking significant breaches of regulation or commercial confidentiality. To avoid such mistakes, organisations should ensure they and their partners are using locked down versions of large language model AI.

Bias is also a risk – especially for financial organisations using historic data in AI-powered dynamic pricing, credit approval and other transactions. If models are trained on historic data, they could repeat the mistakes of the past by discriminating on the grounds of specific demographics, such as age, gender, marital status or others.

> "Some 5% of organisations still use no AI tools"

Data Protection

In this year's findings, data protection and privacy were the most substantial cyber security challenges organisations said they face.

How Data Breaches are Usually Discovered

Typically, how are most data breaches within your organisation usually discovered - if you ever experience any? (Select up to three)

Method of discovery	2025	2024	2023
Through a proactive threat detection programme/ system	43%	43%	38%
Internal employees reporting	40%	41%	30%
Discovered by digital risk and threat intelligence capabilities	36%	37%	29%
By notification from a customer or partner	28%	22%	31%
By the media	16%	21%	31%
By notification from the attacker	25%	21%	30%
When details are posted on public forums	23%	20%	29%
When details are posted on the dark web	21%	19%	28%
We have never suffered a breach	5%	5%	0%

Nearly every organisation surveyed (95%) has experienced a data breach, but about one-in-six found out from the media. Over the last three years of our CNI research, however, we can see a gradual increase in organisations learning about breaches from their own sources as opposed to external ones, such as the media or on public forums, which is a positive development.

Nevertheless, a quarter still only realise they have been breached when the attackers contact them, by which time the damage is done. What is more encouraging is that the most common way for organisations to find out about a breach is through proactive threat detection programmes or systems (43%). This continues a trend from last year, even if the percentage is still too low.

Over the three years of research covered here, we can see a significant increase in the role of internal employees as the primary breach-discoverers and notifiers – 40% this year compared with 30% in 2023's report. It is safe to assume this is down to improved training and a more evolved security culture in many organisations.

> "Nearly every organisation surveyed (95%) has experienced a data breach"

Data Protection

Regulation

Regulation is constantly developing and constantly under review. From a data protection perspective, CNI organisations in the UK must comply with GDPR which has now been in force for seven years. Compliance requires ongoing self-assessment and continuous improvements to avoid public reprimands from the ICO and/ or penalties.

Concerns about GDPR compliance affect 90% of CNI organisations in this survey in one form or another. There are several reasons for this, including a lack of confidence in cyber security measures or a shortage of time and resources. Challenges in meeting data breach notification requirements and record-keeping are also a common reason as these obligations are resource-intensive activities that strain the internal capabilities of many CNI organisations. The requirement to map all personal data processing across an organisation is also a time-consuming task which demands that records be maintained and refreshed annually.

Which aspects of UK data protection requirements does your organisation feel least confident in complying with, if any? (Select up to three)

Aspect of Data Protection	Percentage
Cyber security measures for data protection	34%
Data breach notification requirements	33%
Record keeping, including the creation and maintenance of a record of processing activities	32%
Data processing agreements and due diligence with third parties	31%
Privacy by Design (including completion of Data Protection Impact Assessments).	27%
Data subject rights (e.g. access, deletion, portability).	26%
Cross border transfers	23%
None	10%
We have never suffered a breach	0%

The absence of data protection expertise is another problem, resulting in difficulties with breach notification (a concern to 33% in this survey). Many organisations assign responsibilities for data protection to Heads of Legal or General Counsel who are not primarily data protection officers.

In a bid to ensure notifications to the authorities are fully compliant, such organisations often engage in unnecessary or excessive reporting whenever they fear there is any incident. This splurge of data can lead to unwarranted scrutiny from the ICO.

Analysis of different sectors covered in this year's survey highlights distinctions and different areas of concern. Energy organisations, for example, are particularly lacking in confidence about cyber security measures for data protection (42%). Finance authorities such as the FCA and PRA, despite their responsibility for regulation, still struggle to be confident about compliance with data breach notification requirements (41%). This reflects either a lack of dedicated leadership in this area or greater awareness of shortcomings.

> "Concerns about GDPR compliance affect 90% of CNI organisations in this survey in one form or another"

Data Protection

The Drivers Behind Compliance Initiatives

What is the primary driver for your organisation to achieve compliance with UK data protection regulations, if any?

Driver	2025
Reducing the risk of data breaches and cyber attacks	28%
Protecting customer and stakeholder trust	25%
Meeting contractual or business partner requirements	16%
Using compliance as a competitive advantage	15%
Avoidance of fines and penalties	12%
There is no primary driver	4%
Other, please specify	0%

The findings indicate the extent to which fear of reputational damage with customers is a major stimulus in compliance. In other words, organisations see compliance as being more about protecting rather than enhancing their reputation. For many CNI organisations, the reputational damage suffered by TalkTalk (in 2015) and BA (in 2018) is still fresh in the memory.

The reputational aspect appears more potent than fear of the ICO (Information Commissioner's Office) which has levied relatively few fines, despite frequent publicity about the threat of millions of pounds in penalties for compliance failures.

Operational Technology

The Risk to OT Environments

What, if anything, are the main avenues of cyber-attack in your OT environments at present? (Select up to five)

Avenue of Cyber Attack	Percentage
Cloud services	32%
Web browsing/internet access	31%
Remote access services	28%
Wireless networks	28%
Weak user credentials	26%
Internet-facing devices/ applications	25%
Unpatched vulnerabilities	25%
Business email	24%
IT/OT border	24%
IoT Devices	24%
Unauthorised/unmanaged devices	22%
Removable media	22%
Supply chain	22%
Physical security weaknesses	19%

The results demonstrate how respondents perceive there to be many potential avenues of attack in OT environments. The prominence of cloud services, albeit by a few percentage points, is surprising, as is internet access.

The use of cloud for OT applications may still be in its early days, which generates nervousness. But internet access should be less of a concern because the NIS regulations stress the need to restrict direct internet access. CNI organisations may, however, have valid reasons for connecting OT systems to the internet and in doing so become very alive to the risks.

Most third-party experts in this field would expect **remote access** to be the main avenue of attack that most organisations fear. The fact it is not suggests OT is an area where risk-perception differs from the reality in many organisations.

In the energy sector, Ofgem has been very active about the implementation of NIS regulation requirements, which makes these results all the more surprising. In the survey, 37% of energy organisations are concerned about cloud services.

Looking at other sectors we can see web browsing and internet access are of particular concern to broadcast media organisations (cited by 45%), while for central government it is weak user credentials (highlighted by 35%).

> **“ In the survey, 37% of energy organisations are concerned about cloud services ”**

Operational Technology

Threats to OT Environments in 2025

What, if anything, do you identify as the most significant cyber threats to your OT environments in 2025? (Select up to five)

Cyber Threat	2025	2024	Percentage change
Malware	34%	32%	6%
Phishing	32%	31%	3%
Ransomware	26%	25%	4%
AI and machine-learning	26%	N/A	N/A
Cloud platform attacks	26%	N/A	N/A
DDoS attacks	24%	14%	71%
Social Engineering	24%	20%	20%
Supply chain attacks	24%	23%	4%
IoT devices	21%	N/A	N/A
IT/ Business Network	21%	N/A	N/A
Remote access	20%	N/A	N/A
Advanced persistent threats (APTs)	20%	N/A	N/A
Zero-day exploits	19%	N/A	N/A
Climate change and environmental factors	17%	N/A	N/A

Malware and phishing are again the two most significant threats in the minds of respondents, but cloud platform attacks are not far behind. Increased interconnectivity between OT and IT systems provides a potential avenue for malware access, as many organisations are already aware.

All threats to OT environments have recorded slight increases compared with last year when we asked a slightly different question relating to the biggest risks. The most significant increase was in the perception of DDoS attacks as a threat or risk – a rise of 71%. The increased concern about social engineering reflects the growth of phishing but also better cyber awareness.

> "The most significant increase was in the perception of DDoS attacks as a threat or risk – a rise of 71%"

Operational Technology

Outsourcing in OT

To what extent, if at all, are you outsourcing the following cyber security services for OT?

Service	2025 Outsourced fully or partially	2024 Outsourced fully or partially
Security Operations Centre	57%	52%
Threat intelligence	56%	56%
Digital forensics and incident response	56%	52%
Managed detection and response	57%	52%
Vulnerability management	56%	57%
Data privacy services	54%	N/A
Cyber security training	60%	60%
Penetration testing	58%	56%
Cyber security audits	62%	57%

This research found the level of outsourcing in OT and IT to be similar and to have changed little over the year. The exceptions are increases in use of outsourced security operations sectors (larger than in IT) and **managed detection and response** capabilities (which showed a one percentage point decline in IT).

Operational Technology

ICS/OT Environments

What, if any, are the main areas of concern within your ICS/ OT environments? (Select up to five)

Area of concern	Percentage
Vulnerability management	38%
Lack of security monitoring / threat detection	35%
Insecure ICS/OT protocols	32%
Out-of-support hardware / software	31%
Generic user accounts	31%
IT/OT convergence	30%
Inadequate backups	30%
Inability to respond to security threats / incidents	29%
Inadequate network segmentation	27%
Absent or incomplete asset inventory	25%
None	7%

Vulnerability management came out top of a list of concerns for CNI businesses, closely followed by a lack of security monitoring/threat detection and insecure ICS/OT protocols.

These results are not surprising. Vulnerability management is a high-profile approach with much attention in IT. It is, however, less well-suited to OT. The lack of security built into the majority of ICS components helps explain the level of concern among respondents.

Organisations are likely to come to this from an IT viewpoint, having deliberated on the CAF framework with a focus on vulnerability management. Yet, while patching programmable logic controllers is laudable (and expensive) it still leaves them exposed to instructions from any source that has gained access to the network.

To address these concerns, organisations should also consider network segmentation and securing their perimeter. The convergence of IT and OT varies between sectors, and is a long-standing concern that organisations should address.

Business Pressures and Skills

Budgets

Budget pressures never cease and elsewhere in this survey respondents have admitted there are internal imperatives in their organisation to reduce the cost of cyber security.

Approximately, what percentage of the below is spent on cyber security?

	2025	2024	2023
IT budget	88%	86%	89%
OT budget	34%	29%	37%

A struggling UK economy is likely to be one important factor influencing expenditure on cyber security throughout the last 12 months. This continues to be at substantially lower percentages than in the 2023 report. The growth in organisations considering themselves to be well-advanced on the path to cyber security maturity in IT and OT may also lead to lower spending as there may be a belief they have already done much of what is required.

Approximately what percentage of your cyber security budget, if you have one, is currently spent on the following?

Areas of expenditure	2025 report average	2024 report average	2023 report average
In-house staff for IT	27%	29%	45%
In-house staff for OT	27%	29%	46%
Risk assessments and/or risk management for IT	25%	29%	45%
Risk assessments and/or risk management for IT	26%	29%	45%
Risk assessments and/or risk management for OT	26%	28%	45%
Cyber security audits for IT	25%	28%	47%
Cyber security audits for OT	25%	28%	46%
Vulnerability management and security monitoring for IT	26%	28%	46%
Vulnerability management and security monitoring for OT	27%	29%	44%
Governance, risk and compliance for IT	26%	28%	46%
Governance, risk and compliance for OT	27%	30%	46%
Managed services for IT	25%	29%	46%
Managed services for OT	26%	29%	45%
Cyber security technology/tooling for IT	27%	28%	45%
Cyber security technology/tooling for OT	26%	28%	46%
Penetration testing for IT	25%	29%	45%
Penetration testing for OT	26%	29%	46%
Training and development for IT	26%	29%	47%
Training and development for OT	26%	29%	47%

The decline in expenditure compared with the 2023 report is just as evident as it was last year across all the areas identified in this survey.

Business Pressures and Skills

How much do you anticipate your organisation's investment in cyber security will increase or decrease by in the next 12 months for the following?

2025	Decrease net	Increase net	Stay the same
IT	19%	56%	25%
OT	23%	50%	28%
2024	**Decrease net**	**Increase net**	**Stay the same**
IT	27%	50%	23%
OT	28%	45%	26%

Analysts at Gartner predict that information security spending will increase globally by 15% in 2025, driven by heightened threats, cloud migration, AI and shortages of talent. When this survey looked at projected cyber security investment over the next 12 months in UK CNI organisations, the picture is indeed optimistic. After a very significant dip in cyber security investment in 2024, more organisations have increases in mind in both IT and OT, which is welcome news. Time will tell whether the planned investment increase will occur, or whether budgets will become constricted once more.

How Many Tools?

The complications of poorly integrated security tools are a perennial problem that many organisations are seeking to resolve. In this year's survey, 72% said their organisation currently uses or manages more than 10 security tools – slightly fewer than the 75% who said this in 2024.

Skills – Access and Confidence

How do organisations view their array of skills when cyber talent is perpetually in short supply? Overall, respondents are noticeably more confident than last year about the skill-levels they have access to in different areas of operation.

> "Analysts at Gartner predict that information security spending will increase globally by 15% in 2025"

Do you believe your organisation has the right skills in place to...?

	Yes in 2025	Yes in 2024	Yes in 2023
Secure your IT infrastructure	78%	68%	60%
Secure your OT infrastructure	74%	66%	58%
Accommodate cyber security IT transformation	75%	68%	62%
Accommodate cyber security OT transformation	74%	67%	57%
Monitor security threats in the cloud	74%	68%	59%
Secure remote working IT environment	74%	69%	61%
Secure remote working OT environment	71%	68%	57%
Run a modern SOC	72%	65%	57%
Secure business-led digital initiatives	75%	65%	55%
Effectively and quickly respond to cyber threats in IT	76%	70%	59%
Effectively and quickly respond to cyber threats in OT	76%	71%	59%

Business Pressures and Skills

What sources will you mainly be using to fill your cyber security talent pipeline over the next two-three years? (Select up to five)

Source of new cyber security talent	2025	2024	2023
Reskilling current employees	41%	43%	36%
Outsourced partners and suppliers	41%	38%	35%
Creating apprenticeship programmes	37%	38%	38%
Regional security organisations	34%	32%	38%
Networking at conferences and exhibitions	34%	32%	33%
Funding STEM programmes at universities	33%	30%	32%
Employee recommendation	32%	31%	36%
Traditional recruitment agencies	32%	35%	37%

Reskilling and outsourcing remain important, but the tactics CNI organisations use to ensure they have a pipeline of talent coming through over the next two-to-three years show few significant differences from last year's survey.

Supply Chain Attacks

Supply chain attacks are a major concern, with the infamous SolarWinds attack of 2020 still casting its long shadow. This year, the survey asked CNI organisations about their level of confidence about their ability to deal with supply chain attacks.

How would you rate your organisation's confidence to deal with supply chain attacks?

Level of confidence	2025	2024
Not confident at all	0%	2%
Not very confident	7%	13%
Somewhat confident	50%	43%
Very confident	42%	40%
Not sure	1%	2%

Confidence about the ability to deal with supply chain attacks has improved slightly year-on-year. Although the question was not specific about the definition of a supply chain attack or how organisations "deal" with such attacks, confidence is high, perhaps misplaced once more. This should be of concern, given the continuing evolution of these attack methods among well-resourced cyber crime groups.

What are the types of supply chain attacks you have witnessed the most on your business over the last year? (Select up to five)

Type of Supply Chain Attack	2025 report	2024 report
Firmware attacks	30%	26%
Data interception and tampering	29%	26%
Third-party service providers	29%	22%
Supply chain information breaches	26%	25%
Compromise of vendor emails	26%	23%
Compromise of software suppliers	25%	26%
Compromise of open-source software	24%	24%
Hardware tampering	23%	26%
Logistics and transportation compromise	22%	21%
Insider threats	22%	18%
Counterfeit products	22%	21%
None	7%	9%
Not sure	3%	3%

The results show organisations came face-to-face with many types of supply chain attack. Different sectors are likely to be targeted according to their unique characteristics. Respondents in local government are more likely to witness firmware attacks (45%), for example, while their counterparts in central government have more logistics and transport compromises (36% of respondents) than the average across all sectors (22%). In the maritime world, supply chain information breaches are much more common (34%) than in civil aviation (14%).

> **"In the maritime world, supply chain information breaches are much more common (34%) than in civil aviation (14%)."**

Supply Chain Attacks

Countering Supply Chain Attacks

What are the main practices you have incorporated to counter supply chain attacks? (Select up to five)

Practice	2025	2024
Educating and training employees	25%	20%
Regularly updating and patching systems	21%	18%
A secure software supply chain	21%	21%
Audit of shadow IT	21%	22%
Updated software asset inventory	21%	20%
Incident response and recovery plans	20%	19%
Establish security requirements in contracts	20%	16%
Continuous monitoring and auditing	20%	19%
Develop a multi-layered defence strategy	18%	18%
Monitoring third-party performance	18%	17%
Implement access controls and segmentation	18%	16%
Use of encryption and secure communication channels	18%	22%
Conducting scenario-based planning	18%	13%
Diversifying suppliers	17%	15%
Client-side protection tools	17%	15%
Implement robust vendor management programs	16%	16%
Conducting thorough vendor risk assessments	15%	16%
Collaborate and share information	13%	16%
Not sure	3%	3%
None	2%	3%
Other (please specify)	0%	0%

CNI organisations have adopted a wide range of practices to counter supply chain attacks, which may account for their high levels of confidence. Educating and training employees and regularly updating and patching systems both rose in implementation over the course of 2024.

Conclusion

The 2025 Bridewell research reveals that UK CNI organisations operate in a world where phishing, malware, ransomware, and increasingly sophisticated AI-powered methods are the focus of criminal innovation and proliferation.

While some attacks show a small decline in average frequency, any sense of relief is tempered by the high costs and lingering effects on business operations, reputations, and staff wellbeing. Confidence in existing defences is generally strong, which likely reflects prior improvements in security architectures and the growing use of threat detection capabilities.

Organisations are increasingly likely to uncover breaches themselves than via external parties, but that does not mean there is any need to relent on efforts to improve detection and response capabilities.

Budget constraints remain a critical factor, compelling security leaders to make careful choices about staffing, technology investments, and cloud migration strategies. Nonetheless, more than half of the respondents surveyed expect their organisation's investment in cyber security to increase over the next year, indicating that this remains a core priority despite fiscal pressures.

Building or acquiring strong skills is equally vital, whether through training internal teams or collaboration with specialist external providers. The emergence of AI-driven threats continues to raise new challenges, as does the evolution of supply chain attack tactics. The latter is an area where organisations often fail to fully understand the nature and scale of threats, which could be to their cost.

Looking ahead, the most successful CNI entities will refine detection, streamline their tools for greater efficiency, and coordinate closely with regulators and partners to stay aligned with emerging standards.

Pragmatic investment in people, processes, and technology will underpin a safer and more resilient future. Adherence to cyber security best practice – doing the simple things regularly and observing cyber hygiene rules – is essential. AI-powered threats are no use if they cannot penetrate systems in the first place.

If CNI organisations follow best practice and collaborate with specialist third-parties, their high levels of confidence reported in this survey may prove well-founded.

Bridewell

Cyber Security. Where it Matters.

bridewell.com ☎ +44 (0)3303 110 940 ✉ hello@bridewell.com