Bridewell

Cyber Security. Where it Matters.

Cyber Security in Critical National Infrastructure

2026 Research Report

Contents

Foreword	3
Methodology	4
Executive Summary	5
The 2025-2026 Backdrop: From Economic Uncertainty to Regulatory Momentum	7
Top Cyber Security Challenges for CNI	8
The Threat Landscape	10
When Cyber Risk Becomes Business Risk	12
Where Attacks Break Through	13
Incident Response, Resilience and Reality Gaps	15
Compliance and Frameworks: Necessary, Inconsistent, and Under-Enforced	19
What's Really Driving Cyber Maturity in 2026	22
AI in Defence: Experimentation to Operational Dependence	25
Post-Quantum Cryptography: Confidence Without Clarity	26
Asset Visibility: The Foundation Still Missing	28
People, Skills, and the New Cyber Workforce Reality	29
Conclusion: From Awareness to Advantage	30

Foreword

A Sector Under Pressure, Moving into Action

The year 2025 was a year of reckoning for UK Critical National Infrastructure. High-profile data breaches forced uncomfortable reassessments of security strategies and assumptions; yet economic uncertainty, driven by geopolitical events and fiscal caution, meant that meaningful change was often delayed.

That hesitation was understandable. Through Q2 and Q3, many organisations were trying to balance growing cyber risk against wider questions about investment, supply chains and operational resilience. What changed in Q4 was confidence. As economic conditions stabilised and the UK budget provided greater clarity, we saw previously paused security initiatives restart, audits accelerate and long-planned improvements finally move forward. Carrying momentum into 2026, it is our hope that CNI organisations can learn from these findings, maybe recognise in themselves some home truths, and prioritise accordingly for the years ahead.

What's New for 2026?

One of the most striking shifts witnessed is the growing seriousness with which regulation is now being treated. Frameworks such as the Cyber Assessment Framework (CAF) and NIS2 are shifting from being viewed as abstract compliance exercises to real tests of organisational readiness. Regulators are asking harder questions, audits are becoming more rigorous and CNI organisations are responding by moving from policy to execution.

At the same time, a new challenge is emerging at speed. Artificial Intelligence is being adopted across organisations to improve efficiency, capability and decision-making, often with impressive results. But in many ways, AI feels uncomfortably familiar. Much like the early days of cloud adoption and shadow IT, it is frequently deployed faster than the controls needed to secure it. Conversations are progressing from whether to use AI to how to do so safely: how data is protected, how access is governed as well as how organisations can prevent AI systems and agents from becoming unintended attack paths.

What this research ultimately shows is a sector under pressure but not standing still. Cyber incidents are disrupting operations, which in turn drives investment decisions and the shaping of board-level priorities. This year feels like a turning point; a year where organisations cannot afford to wait for perfect certainty before acting.

Those that succeed will be the ones that turn these lessons into action, embedding security early, treating regulation as a baseline rather than a ceiling and applying the same discipline to AI that we now expect for cloud and digital infrastructure. The challenge is significant, but so is the opportunity to build resilience that fundamentally aligns with the critical role these organisations play.

Methodology

In December 2025, Bridewell commissioned international market research consultancy Censuswide to conduct research among 600 respondents who have responsibility for cyber security in the UK's critical national infrastructure organisations.

These professionals are from the following sectors:

- Central government
- Civil aviation
- Energy
- Financial authorities
- Financial services
- Healthcare
- Insurance
- Local regional government
- Manufacturing
- Maritime
- Rail
- Road
- Water supply and treatment

All respondents to the 26-question survey were sourced and completed through online panels.

Executive Summary

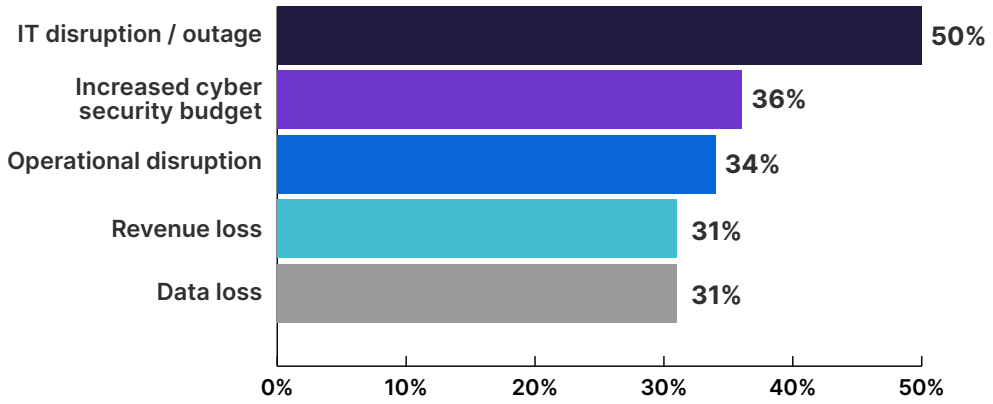
Our Cyber Security in CNI Report for 2026 shows a sector at an inflection point. While 2025 was dominated by awareness and reassessment, 2026 is shaping up to be a year of execution.

Cyber Attacks are Near Universal.

An overwhelming 93% of CNI organisations experienced a cyber attack in the past 12 months, with IT and operational disruption being among the top impacts. Given that CNI organisations depend heavily upon both IT and Operational Technology (OT) environments, this level of disruption is a clear threat to the continued delivery of critical services. More positively, 36% of respondents reported increasing cyber budgets in response to an incident, indicating that lived experience is now shaping board decisions alongside the desire to achieve or maintain regulatory compliance.

Phishing and malware remain the top ways organisations are getting attacked, and outdated software follows closely behind – signalling the importance of patching and regular updates.

Impact of Cyber Attacks



Data Protection Remains the Top Concern, Yet AI Has Arrived Fast.

Data protection and privacy continues to rank as the number one concern, reflecting both regulatory pressure and the real-world impact of breaches. However, managing AI cyber risk has entered the top five at #2 for the first time this year. Organisations are increasingly concerned not just about who can access data, but which AI systems and agents can do so as well.

Top Cyber Security Challenges 2026

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

Drivers of Security Maturity (Comparison Chart: 2025 vs 2026)

Challenge	2026	2025	2024	2023	% increase 2025 – 2026
Data protection and privacy	43%	41%	27%	18%	2%
Managing AI cyber risk	39%	N/A	N/A	N/A	N/A
Improving cyber resilience	36%	36%	34%	18%	0%
Trust in cyber security tools	28%	29%	31%	14%	-1%
Complying with regulations	27%	30%	26%	20%	-3%

Executive Summary

Regulation is Now the Primary Driver of Security Maturity.

Frameworks and regulation, including the CAF, NIS2 and the emerging Cyber Security Resilience Bill (CSRB), have become the dominant force shaping cyber security programmes. Over one-third (35%) of organisations now cite regulation as the primary driver of maturity, up sharply from last year, as audits, assurance and enforcement expectations increase.

Increased connectivity and the desire to support new technology and digital initiatives remain second and third respectively, underlining that cloud environments and increasing interconnection between IT and OT environments are still front of mind. While initiatives in these areas have been ongoing for a while, organisations are still aware that they introduce new areas of risk. Looking at the root causes of cyber incidents (p15), 32% of respondents cited the complexity of cloud environments and 22% cited poor visibility as contributing factors to cyber incidents.

> **AI is today what shadow IT was a decade ago: powerful, widespread, and dangerously easy to adopt without controls and guardrails in place to secure it.**
>
> ***Anthony Young, CEO, Bridewell***

Drivers of Cyber Security Maturity

What are your organisation's key motivators for maturing your cyber security programme? (Select up to three.)*

Motivator	2026	2025	2024
Regulation - need to meet changing regulatory requirements	35%	26%	29%
Increased connectivity - threats have greater potential to exploit critical assets	28%	25%	23%
The business - desire to support new technology and digital initiatives	26%	25%	26%
Threat landscape – evolving cyber threats	25%	24%	22%
Customers - increasing demand for improved security	24%	21%	19%
Employees - support the shift to hybrid & remote working	23%	22%	23%
My team - greater understanding of our cyber security deficiencies	22%	24%	22%
Finance - need to reduce security costs	20%	24%	20%
Competitors - need to maintain competitive advantage	20%	21%	18%
The board - need to demonstrate ROI	16%	20%	18%
Myself - fear of losing my job if I don't drive improvements	12%	15%	17%
There is no pressure to improve cyber maturity	6%	4%	4%

** In previous years, this question was phrased as "Where, if anywhere, is the greatest pressure to improve cyber maturity coming from? (Select up to three)"*

AI Is Both an Operational Accelerator and a Governance Challenge.

Defenders are increasingly using AI to automate incident response, threat hunting and adaptive security controls, but this progress is mirrored by growing concern over AI misuse, data leakage and loss of visibility. As with previous waves of shadow IT and cloud adoption, organisations are being forced to retrofit controls after innovation has already taken place.

The 2025-2026 Backdrop: From Economic Uncertainty to Regulatory Momentum

In 2026, organisational focus is narrowing around regulatory readiness. Regulation has emerged as the strongest driver of cyber security maturity, with 35% of respondents citing regulatory requirements as the primary influence on their security programmes, up from 26% the previous year. While adoption remains uneven, with 46% implemented or fully compliant with the CAF and 29% with NIS2, audit expectations and regulator scrutiny are intensifying.

Alongside this regulatory acceleration, organisations are coming to terms with the rapid expansion of artificial intelligence. AI has quickly moved from experimentation to operational use, and 39% of respondents now rank managing AI cyber risk among their top concerns, making it one of the most significant new risk areas in 2026. This mirrors earlier waves of cloud adoption and shadow IT, where deployment was often driven by speed and productivity, while attempting to apply governance and security controls retrospectively.

The result is a renewed emphasis on data protection and access governance, as organisations reassess not only who can access sensitive information, but which AI systems and agents can do so.

These dynamics illustrate a broader shift in how cyber security is positioned within CNI organisations. What was once treated primarily as a resilience or recovery function is now increasingly recognised as a core operational requirement, directly influencing investment decisions, regulatory compliance and the reliable delivery of essential services. The transition from 2025 to 2026 marks a move from reassessment to execution, as organisations seek to convert heightened awareness into sustained, measurable improvement.

> **"As AI use develops and more harmful use cases emerge, we're already seeing supplementary legislation being introduced to keep pace. Organisations should expect increasing legal and regulatory impact as AI adoption grows."**
>
> ***Chris Linnell, Associate Director - Data Privacy, Bridewell***

Top Cyber Security Challenges for CNI

The cyber security concerns facing UK CNI organisations in 2026 reflect these sectors grappling not only with persistent threats, but with the consequences of rapid technological change. While many priorities remain consistent year on year, the emergence of AI as a major concern signals a shift in how the risk associated with these tools is perceived and managed.

Challenges by Sector

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

Concern	Government	Finance/ Insurance	Utilities	Transport	Manufacturing	Healthcare
Data protection & privacy	45%	40%	45%	43%	45%	51%
Managing AI cyber risk	41%	42%	27%	55%	37%	35%
Improving cyber resilience	41%	21%	37%	34%	34%	40%
Managing cloud cyber security	28%	23%	30%	32%	36%	29%
Trust in cyber security tools	27%	36%	25%	25%	33%	26%
Complying with regulations	23%	28%	31%	30%	25%	28%

Across CNI sectors, data protection and privacy remains the dominant concern, but the intensity and underlying drivers vary. Healthcare stands out most clearly, with over half citing data protection as a top issue, reflecting the sensitivity of patient data, high public scrutiny and increasing digitisation of clinical systems. Government, utilities and manufacturing show similarly elevated concern, driven by regulatory exposure and the scale of legacy estates holding sensitive operational data.

Managing AI cyber risk reveals the sharpest divergence between sectors. Transport organisations report the highest concern, likely signifying rapid adoption of AI across operational, safety and customer-facing systems, combined with low tolerance for disruption. By contrast, utilities show markedly lower concern, suggesting more cautious AI adoption or tighter operational controls.

More and more, organisations are focused not just on who can access data, but on what can access it - particularly as AI systems, copilots and autonomous agents are given broader access across enterprise environments. As AI adoption accelerates, weaknesses in data classification, access control and privilege management are being amplified.

Top Cyber Security Challenges for CNI

Mistrust in cyber security tools is most pronounced in finance and insurance, where tool sprawl, regulatory assurance requirements and limited AI transparency heighten scepticism. Overall, the findings point to uneven AI maturity, sector-specific risk profiles and differing regulatory pressures shaping cyber security priorities across CNI.

These concerns indicate a lessening emphasis on acquiring more tools and more regard for establishing confidence in how those tools and AI systems operate, interact and make decisions.

For CNI, additional consideration needs to be taken for how AI tools interact with OT environments, if they are used at all. While AI tools may promise to enable valuable use cases such as predictive maintenance or process optimisation, such benefits shouldn't be pursued at the expense of safety. Safety-critical decisions can't be made autonomously and human oversight remains a must.

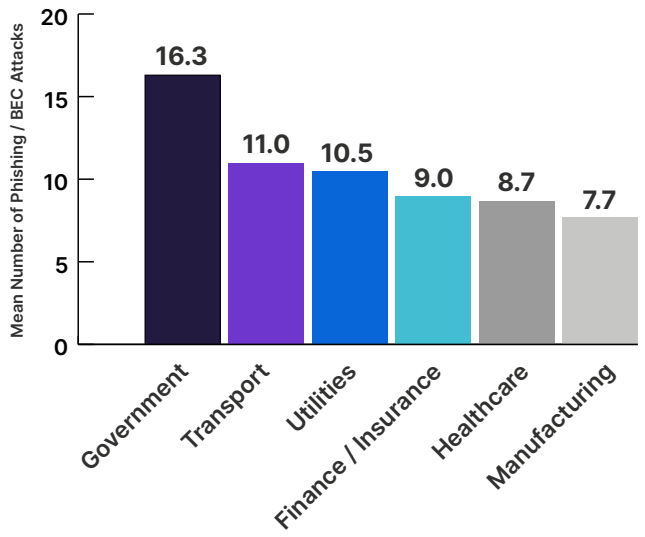
In 2026, cyber security maturity is defined by trust, governance and control across an expanding digital and AI-driven attack surface.

Cyber Attacks Are Near-Universal, Showing Common Threats Despite Uneven Exposure

Cyber attacks are now effectively universal across UK CNI, with 93% of organisations experiencing at least one successful cyber incident in the past year. Across all CNI sectors, phishing and business email compromise (BEC) remain the most prevalent forms of cyber attack, reinforcing the continued effectiveness of social engineering as the primary initial access vector. Although organisations are seeing fewer phishing attacks on average, the attacks that do get through are more sophisticated and have a far greater operational and financial impact.

Approximately how many, if any, [phishing/ BEC attacks] have you suffered from in the past 12 months?

Mean Number of Phishing / BEC Attacks by CNI Sector



The Threat Landscape

Most Prevalent Attack Types

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

Type of Attack	Mean Number of Attacks
Phishing or BEC	11
Malware	8
DDoS	7
Outdated software or unavailable patches on legacy equipment	7
Ransomware	6
Supply chain attacks	6
Data theft or leakage	6
Physical security breach	6
Unauthorised system access	6
Social engineering	6
Employee sabotage	5

The prevalence of phishing and BEC was in contrast to our findings on other types of attack. Ransomware, supply chain, data theft, physical security breaches, unauthorised system access and social engineering all averaged six attacks, almost half that of phishing/ BEC. Unsurprisingly but of concern to IT environments, malware also featured consistently across sectors, averaging 8 attacks in the last twelve months. More pressingly for organisations with OT environments, attacks resulting from outdated software or unavailable patches on legacy equipment were not far behind, averaging 7 attacks. The prevalence of these types of attacks on legacy equipment highlights ongoing challenges in asset visibility and patch management across CNI environments.

Most Prevalent Types of Threat Actor

If you had insight into the threat actors of the cyber attack, who was it? (Select all that apply.)

Type of Threat Actor	%
Cyber criminal	57%
Insider threat	25%
Hacktivist	23%
Advanced Persistent Threat (APT) group	22%
Unsure	16%
Nation-state actor	16%
Other	>1%

> **"The mainstream breaches we've seen recently were all driven by fairly advanced social engineering attacks, with personal data very much at the forefront of the impact."**
>
> ***Chris Linnell, Associate Director - Data Privacy, Bridewell***

The Threat Landscape

Looking at the threat actors behind these attacks, cyber criminals were unsurprisingly the most commonly cited at 57%. This was followed by insider threats at 25%. While there is a strong understanding across most organisations of external threats, insider threats are often unexplored as a 'known unknown'. Non-malicious insiders, for example, may accidentally cause a data breach due to a lack of controls in place around generative AI tools or through shadow IT. Nation-state actors, often the threat actors most difficult to attribute, were only cited for 16% of attacks.

While the overall pattern in attack types is broadly consistent, sector-level analysis reveals important deviations. Transport and utilities organisations show a disproportionately high exposure to attacks linked to outdated software and unpatched vulnerabilities. This reflects the asset-heavy nature of these sectors, where long system lifecycles, OT constraints and limited maintenance windows complicate timely patching and upgrades. In these environments, vulnerabilities are more likely to persist and be repeatedly exploited.

Finance and insurance organisations continue to be highly targeted with phishing and BEC attacks. This is consistent with financially motivated threat activity targeting high-value transactions, payment systems and privileged users, where relatively low technical effort can yield significant returns. The scale and frequency of attempted social engineering in this sector also reflects increased attacker use of AI-driven reconnaissance and impersonation techniques.

Healthcare organisations exhibit relatively higher exposure to malware and ransomware-related activity. Legacy clinical systems, interoperability challenges and operational pressure to restore services rapidly can all increase susceptibility and impact. When it comes to government bodies, the findings broadly mirror the cross-sector average. One deviation is that these bodies were more exposed to social engineering, which reflects the significant scale of government bodies, the diversity of their workforce and their complex supply chains.

The findings show that while attack methods are largely shared across CNI, sector-specific operational realities significantly influence exposure and risk, reinforcing the need for tailored defensive priorities rather than one-size-fits-all controls.

> **"In sectors like transport and utilities, systems are designed to run for decades. That makes patching and modernisation far more complex than in purely IT environments."**
>
> ***Martin Riley, CTO, Bridewell***

When Cyber Risk Becomes Business Risk

Half of organisations report IT disruption or outages as a direct impact of cyber incidents, while 34% experienced wider operational disruption. Financial pressure is also mounting as 36% report increased cyber security budgets, 31% experienced revenue loss, and 31% suffered data loss. Notably, one in five organisations saw cyber insurance premiums rise, further amplifying the long-term cost burden.

Top Impacts of a Cyber Incident:

What have been the main consequences of any of the previously mentioned attacks on your business? (Select up to five.)

Consequence	%
IT disruption or outage	50%
Increased cyber security budget	36%
Operational disruption	34%
Revenue loss	31%
Data loss	31%
Insurance premium increases	20%

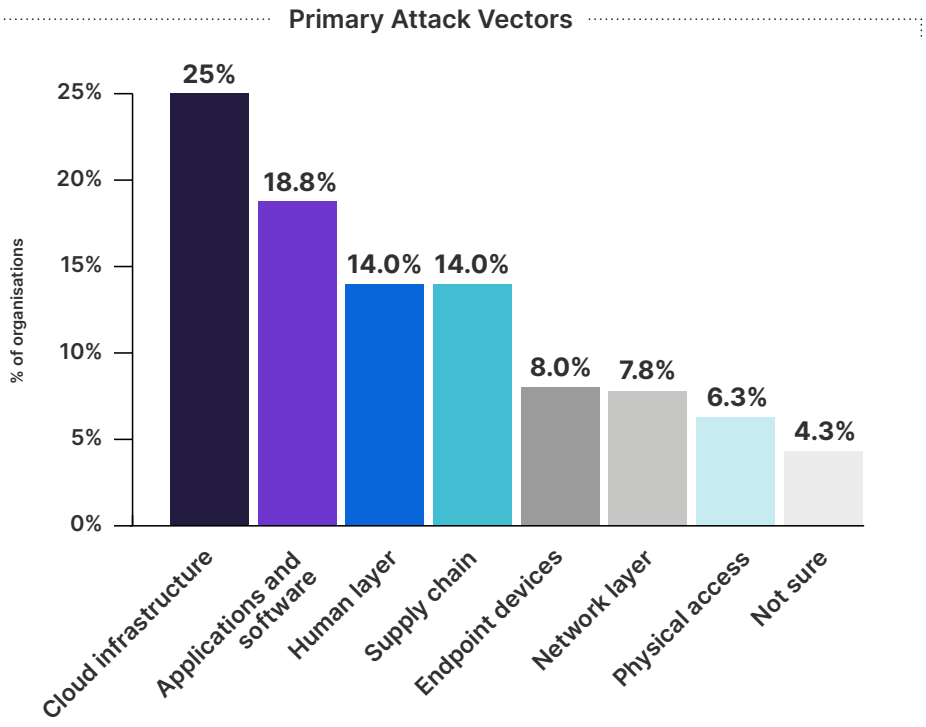
"In asset-heavy sectors, unprotected, outdated systems significantly extend recovery times. That's where costs really start to mount, because fixes aren't quick or straightforward. Once you factor in response, recovery, external support and regulatory engagement, the costs escalate very quickly, often far beyond what was initially anticipated."

Martin Riley, CTO, Bridewell

Where Attacks Break Through

Analysis of primary attack vectors shows that cloud infrastructure is now the most common route into CNI environments for a quarter of respondents, followed by applications and software (19%), with the human layer and supply chain jointly ranking as the next most significant exposure (14%). This pattern is consistent across all CNI sectors surveyed, though its implications will vary depending on operational maturity and technology mix.

What, if anything, was the primary attack vector for any cyber incidents or attacks suffered in the last 12 months?



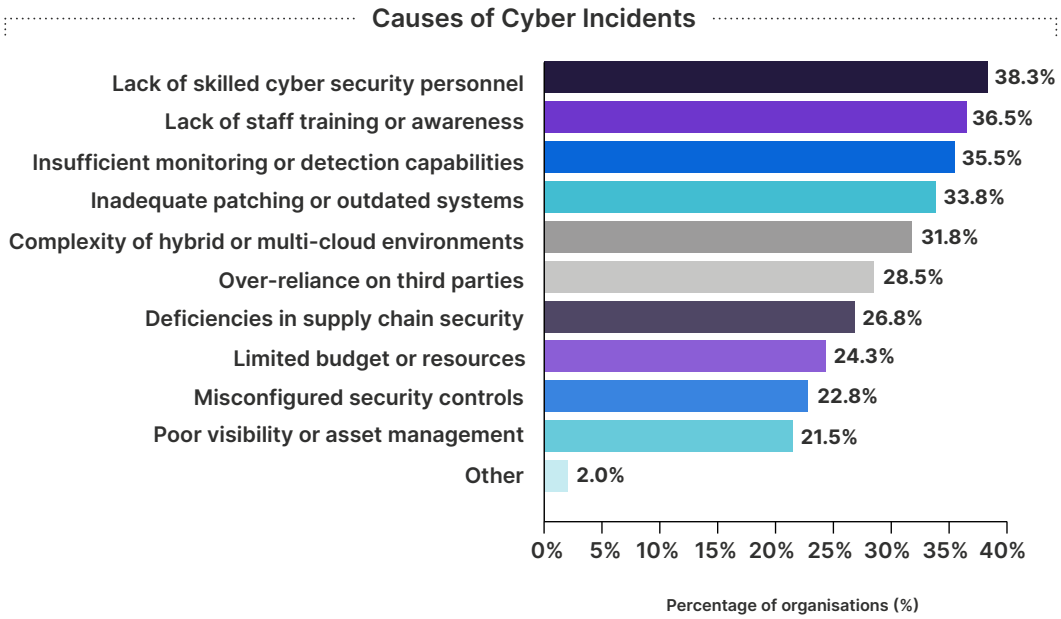
Finance, government and healthcare, in particular, show elevated exposure across both cloud and application layers, reflecting accelerated digital transformation and growing reliance on third-party platforms. Utilities and transport, while often slower to migrate core systems, still exhibit cloud exposure driven by monitoring, analytics and operational support tooling layered onto legacy environments.

Root cause analysis helps to explain why these attack paths persist. Across sectors, the most frequently cited contributors are skills shortages, insufficient training, and poor monitoring and detection, closely followed by inadequate patching and the complexity introduced by multi-cloud and hybrid environments.

> "With cloud and infrastructure, a single misconfiguration or unpatched system can expose services to the entire world. For asset-heavy environments, this poses a continual risk."
>
> *Anthony Young, CEO, Bridewell*

Where Attacks Break Through

What factor(s) specifically are contributing most to vulnerabilities remaining exposed? (Select up to three.)



The findings are indicative of a recurring failure pattern. Security is still being bolted on after cloud adoption, rather than embedded by design from the outset. This has important implications not only for today's cloud environments, but also for the emerging security curve of AI adoption. As organisations accelerate the use of AI-enabled services, existing challenges around skills, visibility and operational control are intensifying, often without the capability required to manage them securely.

Cloud services are being deployed faster than organisations can train staff, adapt monitoring and detection capabilities, or operationalise effective patching across increasingly fragmented estates. In hybrid and multi-cloud environments, this gap is further amplified, creating blind spots that attackers continue to exploit.

Addressing this challenge will require moving beyond cloud access controls alone, towards sustained investment in skills, detection maturity and security-by-design principles applied consistently across the full technology lifecycle.

> "Organisations are adopting new technologies faster than they're building the skills and controls needed to secure them properly."
>
> *Chris Linnell, Associate Director - Data Privacy, Bridewell*

Incident Response, Resilience and Reality Gaps

Our findings indicate that most CNI organisations believe they can respond to cyber incidents quickly, in 6 hours or less. However, average response times tell a more nuanced story. Data theft incidents take approximately 10 hours to respond to, ransomware nine hours, and supply chain compromises eight hours. While these times may appear reasonable in isolation, they sit in stark contrast to the reality that attackers can often exfiltrate data in minutes.

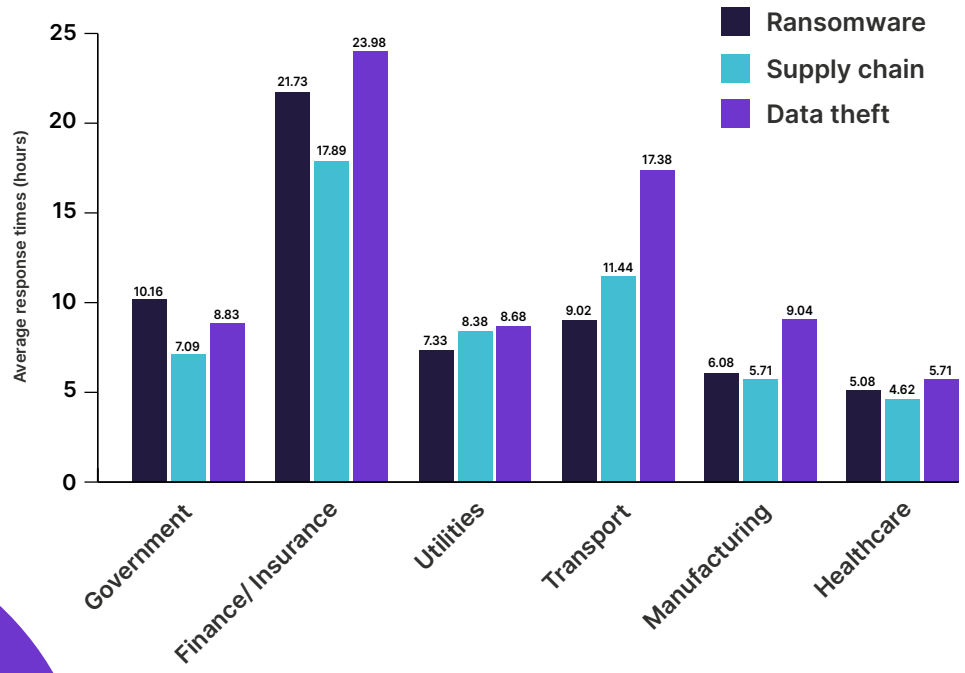
Response Times by Sector

Sector-level analysis of response times reveals significant variation in how quickly organisations are able to contain and manage incidents once detected. Finance and insurance organisations consistently report the longest response times across all three incident types, taking nearly a full day on average to respond to data theft incidents. This likely reflects the complexity of financial environments, layered governance structures and the need for extensive validation and approval before decisive action can be taken.

Transport organisations also stand out, particularly in relation to data theft, where average response times exceed 17 hours. This suggests that while ransomware and supply chain incidents may trigger clearer escalation paths, data theft is slower to identify and confirm, increasing the risk of prolonged exposure. By contrast, healthcare organisations report the fastest response times across all incident types, typically responding within five to six hours, indicating a more rehearsed operational response despite wider resilience challenges.

Utilities and manufacturing sit between these extremes, with relatively consistent response times but still well beyond the window in which attackers can achieve their objectives.

Average Incident Response Times by Sector and Incident Type



> **We're seeing threat actors go from gaining initial access to exfiltrating data within minutes. If you're not taking advantage of technology to reduce your time to respond, you are making it far easier for threat actors to achieve their objectives.**
>
> ***Martin Riley, CTO, Bridewell***

Incident Response, Resilience and Reality Gaps

Resilience and Incident Response Capabilities

Although 98% of respondents describe their organisation as cyber resilient, nearly a third rate themselves as only "moderately resilient". In practice, resilience is frequently interpreted as the ability to eventually recover services, rather than the ability to rapidly detect, contain and minimise impact. As a result, organisations may be resilient in outcome, but not in speed, a distinction that becomes more important as attacks become faster and more automated.

Levels of Cyber Resilience

Thinking about the worst cyber attack you experienced in the last 12 months, how would you describe your resiliency in recovering from it?

Level of Resilience	%
Resilient (Net)*	**98%**
Extremely resilient	24%
Highly resilient	4%
Moderately resilient	30%
Minimally resilient	2%
Not resilient at all	>1%
Minimal / Not resilient (Net)*	**2%**

** Resilient (Net) combines respondents who selected: extremely resilient, highly resilient, moderately resilient, and minimally resilient. Minimal / Not resilient (net) combines respondents who selected: minimally resilient and not resilient at all.*

Incident response capability data reinforces this picture. Most organisations now have core components in place, including training or tabletop exercises (60%), incident response policies or playbooks (58%), and log management (54%). However, fewer than half have established communications plans. This creates risk at the point where technical response must intersect with executive decision-making, external communications and regulatory reporting.

What incident response capabilities do you currently have in place? (Select all that apply.)

Incident Response Capability by Sector

Incident response capability	Government	Finance/ Insurance	Utilities	Transport	Manufacturing	Healthcare
Regular training/ tabletop exercises	58%	54%	63%	66%	57%	59%
Incident response policy/ playbooks	67%	63%	51%	64%	52%	61%
Log management/ evidence capture	59%	52%	62%	54%	50%	44%
Communication plans	55%	43%	43%	49%	47%	40%

> "Having an incident response plan is one thing, but until you've actually exercised it under realistic conditions, you don't really know how your organisation will respond."
>
> *James John, Incident Response Manager, Bridewell*

Incident Response, Resilience and Reality Gaps

Practice, Practice, Practice

Overall, the findings suggest that incident response in CNI is often better defined on paper than proven in practice. Closing this gap will require sustained investment in exercising, clearer decision-making authority and stronger integration between technical teams and organisational leadership, an approach increasingly mandated by government guidance and regulatory frameworks.

Ransomware and Government Intervention: Prepared, But Not Aligned

Ransomware preparedness across CNI organisations is increasing, but the survey findings highlight a clear gap between investment, operational readiness and alignment with government guidance. Organisations report taking tangible steps to strengthen their ability to recover from ransomware incidents, with nearly half investing more in recovery capabilities, which could include things like backup, restoration and disaster recovery. A similar proportion, 48%, have increased investment in cyber security awareness training for staff, reinforcing the continued emphasis on prevention and human risk reduction.

> **Simulating attack scenarios and response mechanisms gives you a better sense of how you'd respond in a real incident. By playing out possible incidents, you're getting a more realistic assessment of people's behaviours if the real thing occurs.**
>
> ***Sam Thornton, Chief Operating Officer, Bridewell***

Responses to Ransomware Payment Ban

Since the government announced a ban on paying the ransom to cyber criminals for public sector organisations, what effect has it had on your internal cyber security policies? (Select all that apply.)

Effect	%
We've invested more in our recovery capabilities	50%
We've invested more in cyber security awareness training for staff	48%
We've prioritised cyber insurance	46%
We've partnered with an MSP to bolster our defences	28%
We've made new hires	26%

For CNI organisations with extensive OT environments, the ransomware payment ban removes the 'easy out' for them as they will no longer be able to pay to restore services in the event of an incident. Investing in recovery capabilities will help them instead be able to reduce the operational impact of an incident by quickly restoring services. This is corroborated by the majority of respondents stating they have a dedicated fund for recovering from operational downtime (more information on p18).

However, these measures alone are not sufficient. Awareness training remains an important control, but it is not a catch-all defence against increasingly targeted and automated ransomware campaigns. As attacks continue to bypass human controls through credential compromise, software vulnerabilities and supply chain exposure, ransomware is increasingly a "when, not if" scenario. In this context, the effectiveness of an organisation's response and recovery capability becomes as critical as its ability to prevent an initial compromise.

Incident Response, Resilience and Reality Gaps

Alongside internal investment, 46% of organisations report prioritising cyber insurance, reflecting both the perceived financial impact of ransomware and uncertainty around recovery costs. However, reliance on insurance continues to present challenges, as coverage restrictions, exclusions and rising premiums reduce its effectiveness as a primary risk mitigation strategy.

Fewer organisations have turned to structural capability expansion, with 28% partnering with a managed security service provider (MSSP) and only 26% making new cyber security hires, highlighting persistent skills constraints across CNI. Despite growing preparedness, ambiguity remains around decision-making during a live ransomware incident.

Types of Ransomware Contingency Fund

Do you currently have a ransomware contingency fund for any of the following? (Select all that apply.)

Fund Type	%
Recovery from operational downtime	52%
Crypto acquisition	28%
None of the above	22%
Negotiator	20%
Paying a ransom	19%
N/A	6%

Our survey findings also uncovered that while ransomware contingency funds are relatively common among CNI organisations, their intended uses are diverse. Notably, 19% have a fund for paying a ransom. This may be because organisations haven't had time to fully understand, digest and implement the government's forthcoming ban on ransomware payments.

Overall, the findings suggest that while CNI organisations are investing in ransomware preparedness, alignment between prevention, response execution and government guidance remains uneven. Closing this gap will require clearer operational expectations, stronger integration between technical and executive response, and more frequent exercising to ensure decisions made under pressure reflect both policy intent and operational reality.

> **"Organisations often prepare for recovery, but struggle with the moment where decisions need to be made quickly and confidently during an incident. Importantly, guidance sets direction, but it doesn't always translate cleanly into operational choices under pressure."**
>
> ***James John, Incident Response Manager, Bridewell***

Compliance and Frameworks: Necessary, Inconsistent, and Under-Enforced

Compliance frameworks continue to play a central role in shaping cyber security activity across UK CNI organisations, but their effectiveness remains uneven. When asked what primarily drives compliance efforts, organisations most commonly cite reducing the likelihood of breaches (29%), followed by protecting organisational trust (21%) and meeting contractual requirements (16%). This suggests that compliance is still viewed largely as a risk-reduction and assurance mechanism, rather than a proactive driver of operational resilience.

Drivers for Data Protection Compliance

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

Driver	2026	2025
Reducing the risk of data breaches and cyber attacks	29%	28%
Protecting customer and stakeholder trust	21%	25%
Meeting contractual or business partner requirements	16%	16%
Using compliance as a competitive advantage	12%	15%
Avoidance of fines and penalties	9%	12%
There is no primary driver	3%	4%
Other	11%	0%

Despite this, confidence in meeting key regulatory requirements remains limited. The lowest levels of confidence are reported in cyber security measures for data protection, where 39% of organisations express low confidence, alongside persistent challenges in third-party due diligence and breach notification requirements. These gaps are particularly significant given the increasing reliance on suppliers and partners across CNI ecosystems, and the regulatory emphasis on timely detection, reporting and accountability.

Confidence in Data Protection Compliance

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

Aspect of UK Data Protection Requirements	2026	2025
Cyber security measures for data protection	39%	34%
Data processing agreements and due diligence with third parties	32%	31%
Data breach notification requirements	31%	33%
Privacy by Design (including completion of Data Protection Impact Assessments).	31%	27%
Record keeping, including the creation and maintenance of a Record of Processing Activities	28%	32%
Data subject rights (e.g. access, deletion, portability).	27%	26%
Cross border transfers	21%	23%
None	12%	10%

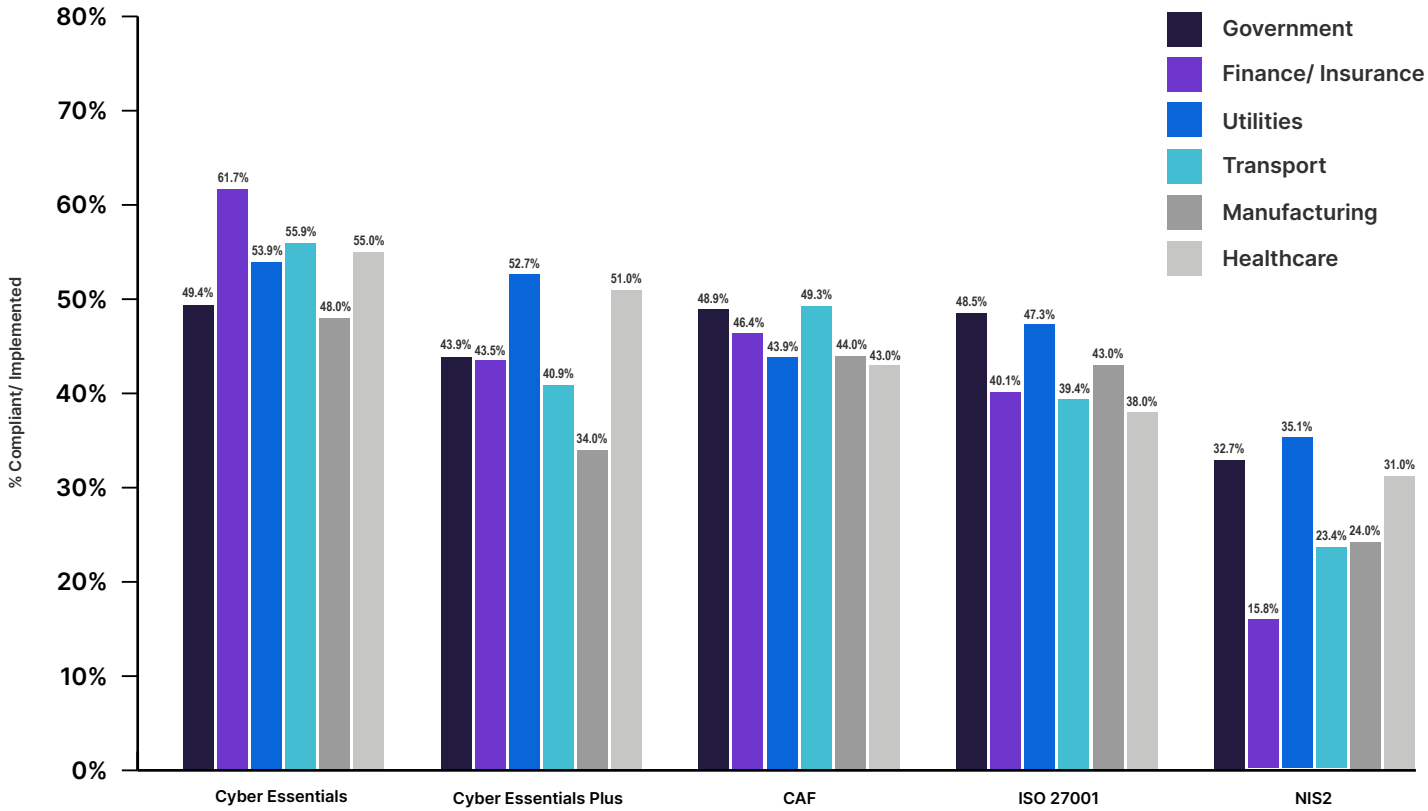
> **"The issue isn't the lack of frameworks; it's the lack of consistent enforcement and assurance that controls are actually operating as intended."**
>
> ***Anthony Young, CEO, Bridewell***

Compliance and Frameworks: Necessary, Inconsistent, and Under-Enforced

Adoption of recognised frameworks is widespread but fragmented. Cyber Essentials has the highest uptake at 54%, followed by the CAF (46%), Cyber Essentials Plus (44%), and ISO 27001 (43%). In contrast, NIS2 adoption remains comparatively low at 29%, reflecting either its relative recency or uncertainty around scope and applicability.

> **ISO 27001 is not as prevalent as it once was. Instead, we have seen a real shift as organisations pivot towards other frameworks like the CAF.**
>
> ***Sam Thornton, Chief Operating Officer, Bridewell***

Framework Compliance by Sector



Compliance and Frameworks: Necessary, Inconsistent, and Under-Enforced

Crucially, only 35% of organisations believe that current regulations are delivering "very well" in practice. This perception varies meaningfully by sector, with more heavily regulated industries often reporting higher adoption but not necessarily greater confidence.

Attitudes to Government Regulations

How well do you think government regulations in cyber security are delivering on their objectives?

Sector	% (Well*)
Finance/ Insurance	93%
Utilities	90%
Healthcare	87%
Government	86%
Transport	82%
Manufacturing	79%

** "Well" combines respondents who selected "Very well" or "fairly well".*

Perceptions of how effectively government regulations are being delivered vary markedly across CNI sectors. Finance and insurance organisations are the most positive, with over 93% rating regulations as being delivered "well" or "very well".

This likely reflects long-standing regulatory engagement, mature compliance functions and clearer supervisory expectations.

Utilities also demonstrate relatively high confidence, underpinned by familiarity with sector-specific regulatory frameworks and assurance regimes. By contrast, transport organisations report the lowest levels of confidence, suggesting that regulatory guidance is often perceived as harder to interpret or operationalise within complex, asset-heavy and safety-critical environments. Manufacturing similarly lags behind other sectors, reinforcing concerns that existing frameworks are not always well aligned to industrial and operational realities.

Overall, the findings indicate that while compliance frameworks are widely recognised as necessary, they are inconsistently adopted, unevenly enforced and often weakly operationalised. Many organisations struggle to translate regulatory guidance into embedded controls, particularly across third-party risk and incident reporting. Without stronger enforcement, clearer expectations and greater focus on operational outcomes, compliance risks becoming a tick-box exercise rather than a foundation for genuine cyber resilience.

> **"Frameworks are useful, but they're often treated as an end goal rather than a baseline. Organisations can technically meet the requirements without actually being resilient in practice."**
>
> ***Anthony Young, CEO, Bridewell***

What's Really Driving Cyber Maturity in 2026

Drivers of Cyber Security Maturity

What are your organisation's key motivators for maturing your cyber security programme? (Select up to three.)*

Motivator	2026	2025	2024
Regulation - need to meet changing regulatory requirements	35%	26%	29%
Increased connectivity - threats have greater potential to exploit critical assets	28%	25%	23%
The business - desire to support new technology and digital initiatives	26%	25%	26%
Threat landscape – evolving cyber threats	25%	24%	22%
Customers - increasing demand for improved security	24%	21%	19%
Employees - support the shift to hybrid & remote working	23%	22%	23%
My team - greater understanding of our cyber security deficiencies	22%	24%	22%
Finance - need to reduce security costs	20%	24%	20%
Competitors - need to maintain competitive advantage	20%	21%	18%
The board - need to demonstrate ROI	16%	20%	18%
Myself - fear of losing my job if I don't drive improvements	12%	15%	17%
There is no pressure to improve cyber maturity	6%	4%	4%

** In previous years, this question was phrased as "Where, if anywhere, is the greatest pressure to improve cyber maturity coming from? (Select up to three)."*

The factors driving cyber security maturity across UK CNI are changing. Regulation has now emerged as the single strongest driver, cited by 35% of organisations, up sharply from 26% the previous year. This marks a clear inflection point where compliance is no longer a background consideration, but the primary force shaping security investment, governance and executive attention.

Alongside regulation, organisations point to growing connectivity and risk exposure, particularly as environments become more distributed, cloud-enabled and interdependent. The need to enable new technology safely also features strongly, reinforcing that security maturity is tied to the ability to innovate without introducing unacceptable risk. By contrast, only 12% cite fear of job loss as a motivating factor, suggesting that individual accountability is giving way to more formal, organisational drivers.

This shift reflects a broader change in accountability. Cyber security maturity is moving away from being driven primarily by "best practice" aspirations or isolated security leadership to external expectations, regulatory scrutiny and board-level oversight.

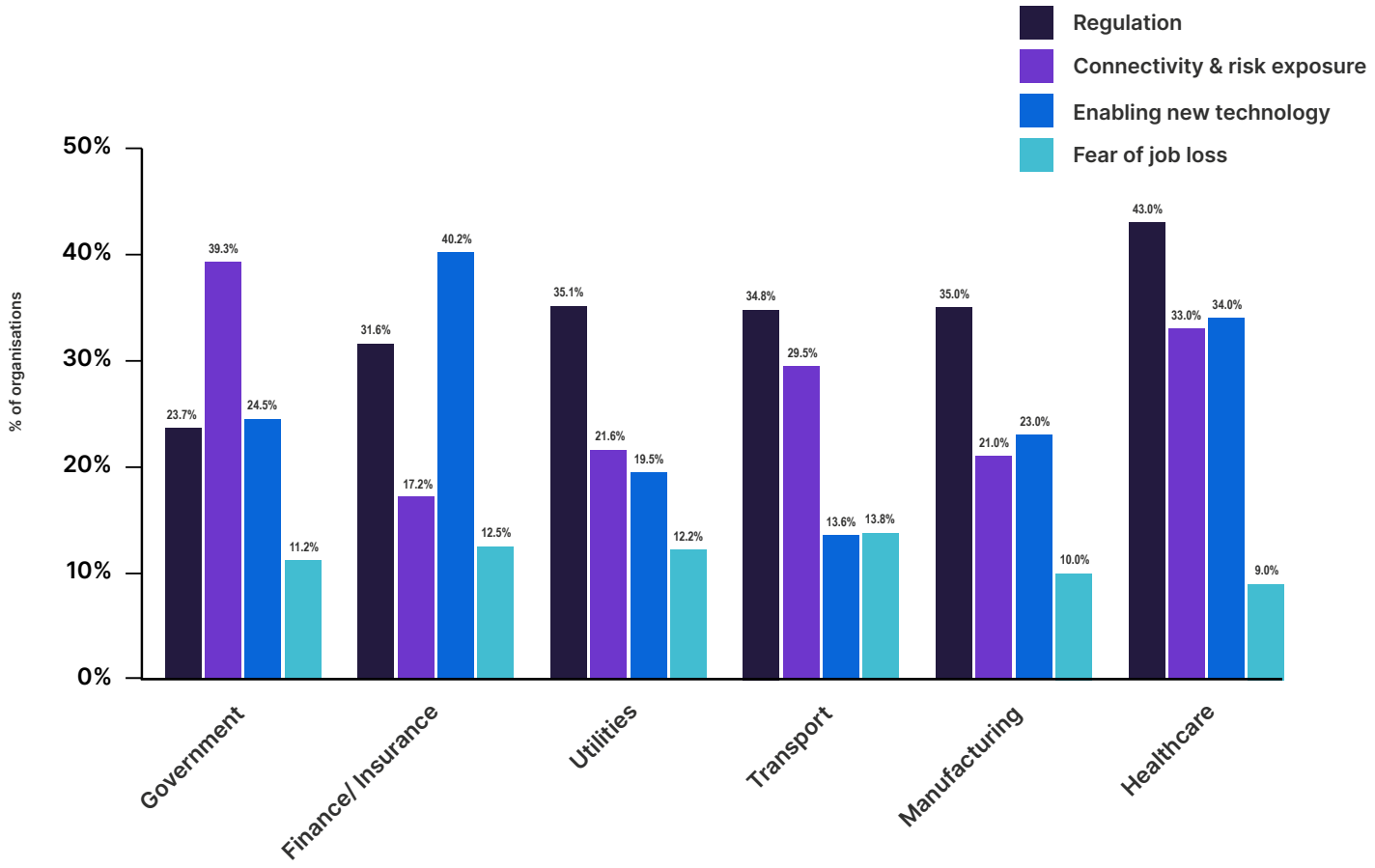
> **"We're seeing a real change in what drives action. Best practice used to be enough, but now organisations are asking what they'll be held accountable for by regulators, by boards and by the public."**
>
> ***James John, Incident Response Manager, Bridewell***

What's Really Driving Cyber Maturity in 2026

Top Motivators for Maturing Cyber Security Programmes by Sector

What are your organisation's key motivators for maturing your cyber security programme? (Select up to three.)

Drivers of Cyber Security Maturity by Sector



What's Really Driving Cyber Maturity in 2026

Sector-level analysis reinforces this trend but also reveals meaningful variation. Finance and insurance organisations are most strongly driven by regulation, reflecting long-standing supervisory pressure and mature compliance cultures. Utilities and government also show regulation as a dominant driver, aligned with critical service obligations and public accountability. By contrast, transport and manufacturing place greater emphasis on connectivity and operational risk exposure, while healthcare balances regulatory pressure with the need to safely enable digital and data-driven transformation.

The findings suggest that cyber maturity in 2026 is being shaped less by voluntary improvement and more by mandatory accountability. Regulation has overtaken best practice as the primary driver of action. The challenge now lies in ensuring that compliance translates into sustained, operationally embedded security, rather than short-term, audit-driven change.

> **"Regulation has become the baseline expectation. The organisations that struggle are those that still treat it as guidance rather than an operational requirement."**
>
> ***Anthony Young, CEO, Bridewell***

AI in Defence: Experimentation to Operational Dependence

Usage of Agentic AI

Does your organisation use agentic AI (i.e. AI systems capable of autonomous decision-making and action) in any of the following capacities? (Select all that apply.)

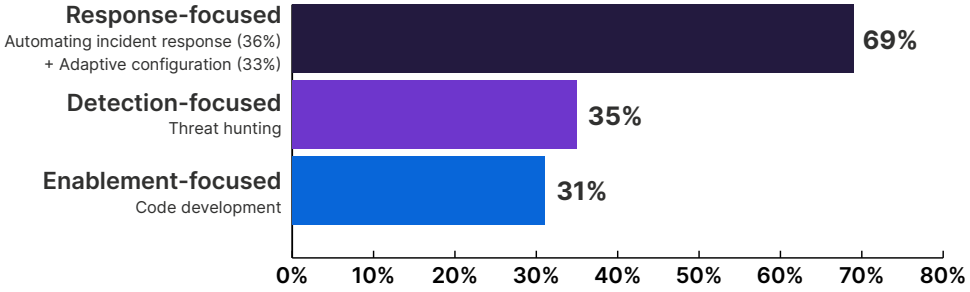
Use of AI	%
Automating incident response	36%
Threat hunting	35%
Adaptive security configuration	33%
Code development	31%
Do not currently use AI	11%
N/A	6%

The use of AI in cyber defence has moved decisively beyond experimentation. By 2026, agentic AI is playing a material role in day-to-day security operations, with organisations increasingly relying on it to accelerate detection, response and recovery. Over a third of organisations report using AI to automate incident response (36%) and support threat hunting (35%), while 33% use it to adapt security configurations in real time.

Even traditionally human-led activities such as code development are now AI-assisted in nearly a third of organisations. Notably, only 11% of respondents report not using AI at all, underlining how widespread adoption has become.

> **"If you're not using AI in your SOC, you can't say you're doing everything you can from a defensive standpoint."**
>
> ***Martin Riley, CTO, Bridewell***

AI Defensive Use by Function



Our survey results find that organisations are most likely to deploy AI in response-oriented roles, reflecting growing reliance on automation to reduce response times and manage operational scale. AI is increasingly central to reducing mean time to detect and respond (MTTR), particularly in environments where attack speed and complexity continue to outpace human capacity.

However, as adoption accelerates, the nature of risk is changing. The primary question becomes not whether AI should be used in defence, but how safely and responsibly it is governed. Agentic AI systems introduce new challenges around autonomy, access to sensitive data and decision-making authority, particularly when integrated directly into response workflows.

This creates a new dependency where organisations are beginning to rely on AI to assist analysts as well as to act on their behalf. Without clear guardrails, robust oversight and strong data governance, the same capabilities that reduce response times could also amplify risk. As environments become more automated and interconnected, the emphasis must be on governing AI with the same rigour as any other critical security control, ensuring transparency, accountability and resilience as reliance on the technology grows.

Post-Quantum Cryptography: Confidence Without Clarity

Levels of Preparedness for Post-Quantum Cryptography

How prepared is your organisation for a post-quantum cryptography world?

Level of Preparedness	%
Prepared (Net)*	90%
Extremely prepared	22%
Highly prepared	41%
Moderately prepared	28%
Minimally prepared	6%
Not prepared at all	4%
Minimal/ Not prepared (Net)*	10%

**Prepared (Net)' combines respondents who selected: extremely prepared, highly prepared, and moderately prepared. 'Minimal/ not prepared (Net)' combines respondents who selected: minimally prepared or not prepared at all.*

At first glance, CNI organisations appear confident in their preparedness for post-quantum cryptography. Almost two-thirds (63%) say they feel highly or extremely prepared for the transition. However, this confidence is not matched by depth of understanding or concrete action.

Attitudes to Government Guidance on Post-Quantum Cryptography

Which statement best describes your feelings regarding the sufficiency of the guidance from the government on readiness for post-quantum cryptography?

Statement	%
Government guidance is sufficient and my organisation is prepared	46%
I know there is government guidance, but I have yet to review it	38%
The guidance is confusing and I don't know where to start	10%
I am not aware of government guidance on post-quantum cryptography	6%
N/A	6%

More than a third of respondents (38%) have yet to review government guidance on post-quantum cryptography (PQC) at all, while around one in ten explicitly say the guidance is confusing and they do not know where to start. This disconnect points to an overly optimistic CNI sector, where perceived readiness outpaces actual progress.

Cryptography underpins almost every system in a modern CNI environment, from PKI infrastructure and network appliances to legacy on-prem and OT systems. Without a clear understanding of where cryptography is used, how easily it can be upgraded, and how long encrypted data must remain secure, claims of readiness are, at best, premature.

The findings suggest that post-quantum cryptography is widely recognised as important, yet poorly understood in practice. Closing this gap will require focused education, early scoping exercises and clearer accountability, rather than continued reliance on high-level confidence.

> **"Many organisations equate preparedness with vendor assurances or assume the challenge is limited to future cloud upgrades. In reality, post-quantum readiness requires a far broader and more complex assessment."**
>
> ***Kieran B, Head of Security Engineering, Bridewell***

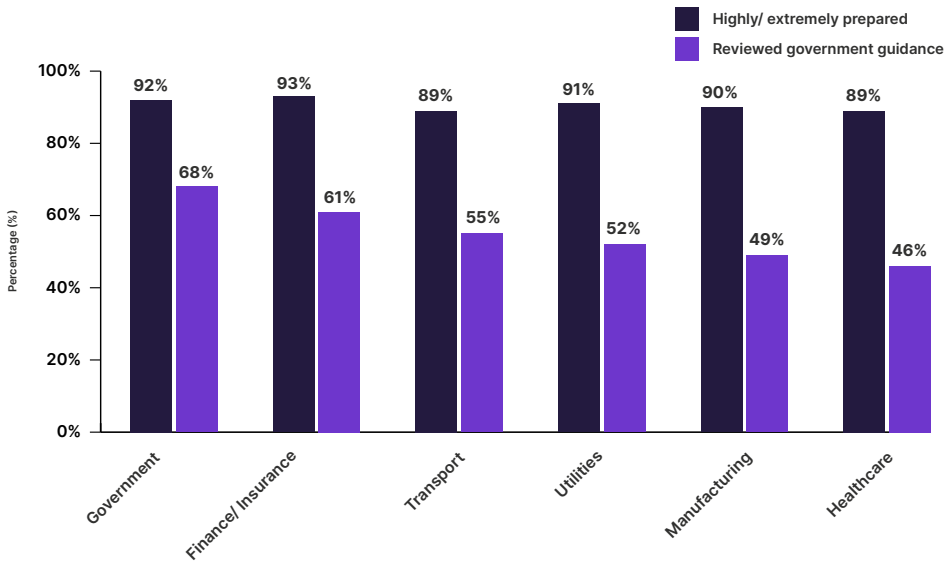
Post-Quantum Cryptography: Confidence Without Clarity

Sector Analysis

Across sectors, confidence in post-quantum cryptography preparedness is consistently high, ranging from 89% to 93%, with finance and government reporting the strongest levels of perceived readiness. However, this confidence is not matched by formal engagement with government guidance. The gap between confidence and review of government materials is most pronounced in asset-heavy sectors such as healthcare, manufacturing and utilities, where complex operational technology environments and legacy systems may make the quantum transition more challenging. The narrow variation in perceived preparedness, contrasted with the much wider variation in guidance review, suggests that optimism is high while operational planning is low.

Sectors with long-lived assets, embedded cryptography and complex supply chains are more likely to underestimate the scale of post-quantum transition, particularly where responsibility is assumed to sit with vendors or cloud providers.

Preparedness for PQC & Attitudes to Government Guidance on PQC



> **This uneven picture is not a failure of intent, but of awareness. Until organisations systematically map where cryptography is used, how valuable the data it encrypts is, and how difficult it will be to change, sector-level confidence will continue to overstate true readiness.**
>
> ***Kieran B, Head of Security Engineering, Bridewell***

Asset Visibility: The Foundation Still Missing

Despite continued investment in cyber security tools and controls, asset visibility remains a fundamental weakness across CNI organisations. Only 29% report using a centralised or dynamically managed enterprise asset management approach, while a further 27% rely on a hybrid of manual and automated tracking. Just 12% have outsourced asset management to a third party.

Approaches to Device and Asset Management

How are all the devices or assets connected to your networks primarily managed?

Approach to Device/Asset Management	%
Centrally and dynamically managed through an enterprise asset management system	29%
Managed through a combination of manual tracking and automated tools	27%
Managed by individual departments or teams	23%
We use a third-party provider to manage our assets	12%
We have limited visibility or control over connected devices	9%
N/A	6%

This fragmented picture limits organisations' ability to understand their true attack surface. Without a complete and current view of assets, particularly across hybrid IT and OT environments, security teams struggle to prioritise vulnerabilities, detect anomalous behaviour or respond effectively to incidents.

The challenge is particularly acute in asset-heavy sectors, where long-lived infrastructure, legacy systems, and non-standard devices are common. Many of these assets sit outside traditional IT monitoring and patching processes, creating blind spots that attackers can exploit.

A further concern is the immaturity of "crown jewels" identification. Many organisations still lack clarity on which systems, data and services are genuinely mission-critical, and how these map to business continuity and national resilience objectives. As a result, security efforts are often spread too evenly, rather than focused on protecting what matters most.

Asset visibility is not a hygiene task. It is the foundation on which effective risk management, incident response, and resilience are built. Until organisations can confidently answer what they have, where it is and how critical it is, claims of cyber maturity will remain fragile.

People, Skills, and the New Cyber Workforce Reality

Overcoming the Cyber Skills Gap

How are you addressing the cyber skills gap as an organisation? (Select all that apply.)

Approach to Cyber Skills Gap	%
Upskilling existing staff through training and certifications	52%
Investing in automation and AI to reduce reliance on human resources	45%
Hiring external talent with specialist skills	39%
Partnering with third-party providers or MSSPs	37%
Collaborating with academic institutions or apprenticeship schemes	32%
We are not currently addressing the cyber skills gap	5%

Skills shortages continue to shape cyber security strategy across CNI organisations, but the way those gaps are addressed is evolving. More than half of respondents now prioritise upskilling and reskilling existing staff, rising from 41% last year to 52%. This reflects growing confidence in developing internal capability, particularly where deep understanding of operational environments, legacy systems, and regulatory obligations is essential.

This shift also signals a more pragmatic response to a constrained talent market. Recruiting experienced cyber specialists remains difficult and costly, especially for highly technical roles. As a result, many organisations are investing in their existing workforce, building cyber capability on top of established institutional knowledge.

Automation and AI are increasingly used alongside upskilling efforts to reduce workload pressure and help teams focus on higher-value tasks. In security operations, this is most visible in triage, investigation, and analysis, where AI is being applied to filter noise, surface priority issues, and accelerate response. However, these tools are seen as an enabler rather than a replacement for skilled professionals, with governance and guardrails recognised as critical to prevent data leakage and unintended risk.

Despite the focus on internal development, organisations acknowledge the limits of upskilling alone. Specialist roles such as penetration testing, security architecture, and advanced OT security continue to require external expertise. This reinforces the ongoing role of new hires and third-party partners in supplementing internal teams, particularly for complex or high-risk activities.

Hiring priorities further reflect this balancing act. Professional certifications and hands-on experience are most valued, providing assurance of both technical competence and practical capability. Vendor certifications are important where environments are platform-specific, while soft skills are often deprioritised, despite their importance in incident response, communication, and decision-making under pressure.

Overall, the findings point to a more blended cyber workforce model, combining upskilled internal staff, targeted automation and specialist support. Success increasingly depends on how well organisations integrate these elements, rather than relying on any single approach to solve the skills challenge.

Conclusion: From Awareness to Advantage

The findings of this year's research show a sector moving beyond awareness and into a more decisive phase of action. Cyber security is evolving from a supporting function to an operational discipline that underpins national resilience, service continuity and public trust.

Compared with last year, the emphasis has shifted. In 2025, organisations balanced confidence in their defences against economic uncertainty and delayed decision-making. In 2026, that hesitation has given way to execution. Regulation has become the primary forcing function, driving clearer priorities, increased accountability and sustained investment across CNI environments. Frameworks such as the CAF and NIS2 are now shaping day-to-day decisions, rather than sitting alongside them.

AI has also moved from experimentation into routine defensive use. Its value is most evident in incident response, investigation and detection, where it is helping teams operate faster and with greater consistency. At the same time, the research highlights growing awareness that AI introduces new dependencies and risks.

Trust in tools, clarity over data access and governance of automated decision-making are now central concerns, rather than secondary considerations.

Across the report, another consistent pattern emerges. Organisations that maintain clear visibility of their assets, respond quickly to incidents and apply strong governance, are better placed to withstand disruption. Where any of these elements are weak, risk accumulates. Asset blind spots persist, confidence exceeds understanding in areas such as post-quantum cryptography and resilience is often measured by eventual recovery rather than timely containment.

People remain critical to this progress. The increased focus on upskilling reflects a practical response to skills shortages and the value of institutional knowledge in complex environments. However, the findings also reinforce the need for specialist expertise and carefully governed automation, particularly where the margin for error is small.

Looking ahead, 2026 is likely to distinguish organisations that can consistently operate under pressure from those that rely on point-in-time compliance. The difference will be seen in how quickly incidents are understood, how clearly responsibilities are defined and how confidently decisions are made when systems are under stress.

The challenge now is not identifying the right controls or frameworks. It is embedding them into everyday operations, so that when disruption occurs, organisations are prepared to respond, contain and recover with confidence. These are the keys to true resilience.

Bridewell

Cyber Security. Where it Matters.

bridewell.com

+44 (0)3303 110 940

hello@bridewell.com