



Bridewell

RESEARCH REPORT

Cyber Security in US Critical National Infrastructure Organizations: 2023

Contents

Foreword	3
Methodology	4
Current Threat Landscape	5
Rise of Ransomware	8
What is RaaS?	9
The Human Factor	10
Cyber Security and Economic Pressures	13
Impact on Cyber Budgets	16
Identifying and Meeting the Evolving Threat Landscape	17
How Do CNI Organizations Detect Breaches?	19
Achieving End-to-End Visibility	23
Cyber Maturity in 2023	25
Conclusion	27



Foreword

The organizations that operate US critical national infrastructure (CNI) continue to show great adaptability and tenacity in the face of evolving cyber risk. Recognizing the need for sustained collaboration across sectors, geographies, and supply chains, companies are working together to mount a more cohesive and coordinated defense posture.

However, the threat landscape is keeping pace with progress, making it more challenging than ever to secure critical systems and services from cyber attack. In 2023, significant downstream effects are taking hold, touching not only global CNI but almost every aspect of US life. With inflationary pressures contributing to price rises, particularly for food and energy, economic challenges are bringing the risk of insider cyber threats to the fore.

Whether through malicious intent or negligence, employees and other insiders can pose a substantial threat to the systems and networks that keep the country running. CNI cyber budgets are also being cut as organizations re-evaluate their budgets due to the economic downturn, leaving companies more vulnerable to attacks.

All the while, a broad spectrum of cyber threats continues to evolve in frequency, severity, and sophistication. As CNI organizations digitally transform at scale – and increased remote working drives convergence between IT, OT, and cloud – new attack surfaces are being created for criminals to exploit, as increased connectivity between systems provides more entry points for potential breaches.

In particular, the rise of targeted ransomware highlights the urgent need for better end-user awareness and proactive threat detection and response.

To help us better understand how cyber leaders in CNI organizations are faring, we commissioned research among 500 cyber security decision makers in the US transport and aviation, utilities, finance, government, and communications sectors to explore the current cyber threat landscape. This report examines the various security challenges faced across CNI sectors and OT/IT environments – and the findings will point towards steps that every organization should take to become truly cyber resilient in testing times.



Scott Nicholson
Co-CEO, Bridewell

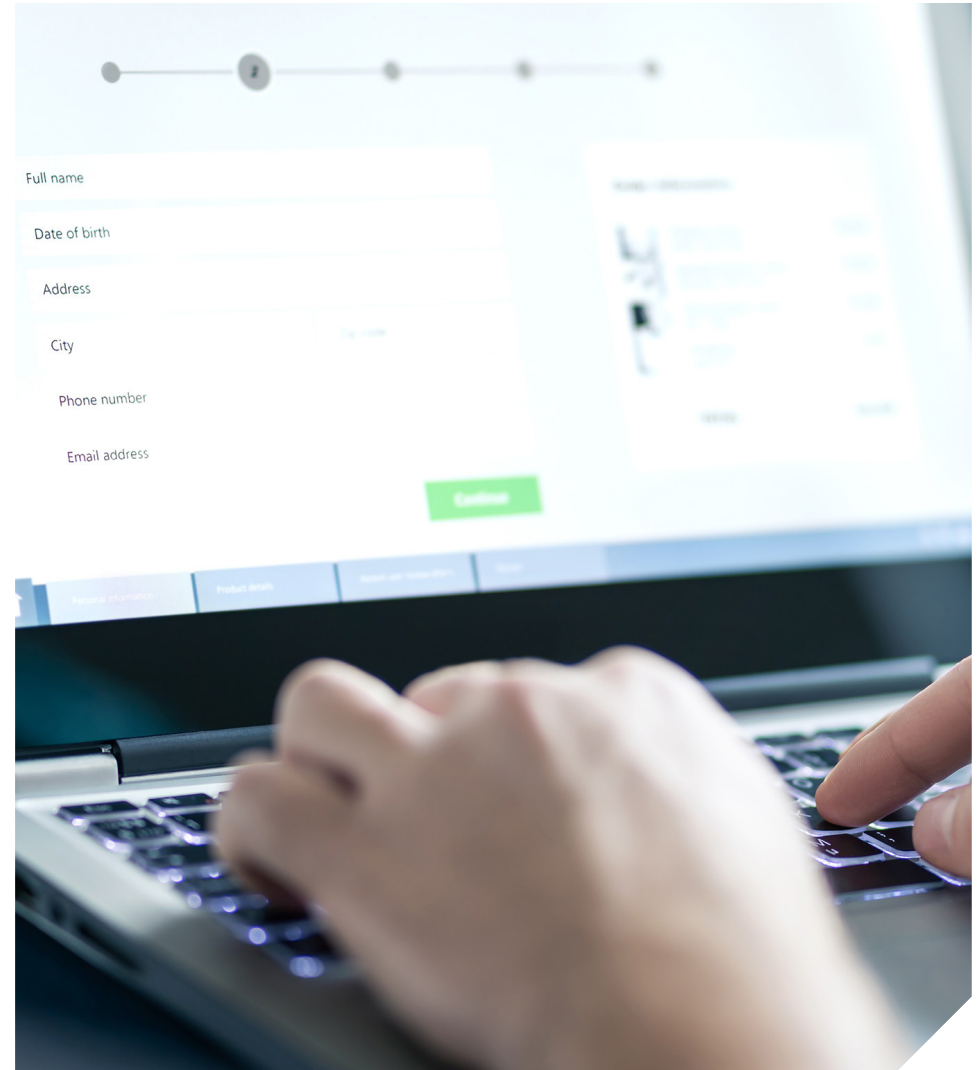
Methodology

In February 2023, Bridewell commissioned international market research consultancy, Censuswide, to conduct research among 1,025 respondents who have responsibility for cyber security from the US (525 respondents) and UK (500 respondents) in the communications, utilities, finance, government, and transport and aviation sectors. A minimum of 100 respondents were surveyed from each sector to allow for sufficient sector comparisons.

Respondents all had responsibility for cyber security and job titles included CISO, CTO, CIO, CRO, MD, IT Director, Cyber Security Director, Director of IT Security, Director of Operational Security, Head of Information Security, Head of IT, Head of IT Infrastructure, IT Manager, IT Security Manager.

All respondents were sourced via online panels and completed a 39-question online survey.

CENSUSWIDE
+
THE RESEARCH CONSULTANTS



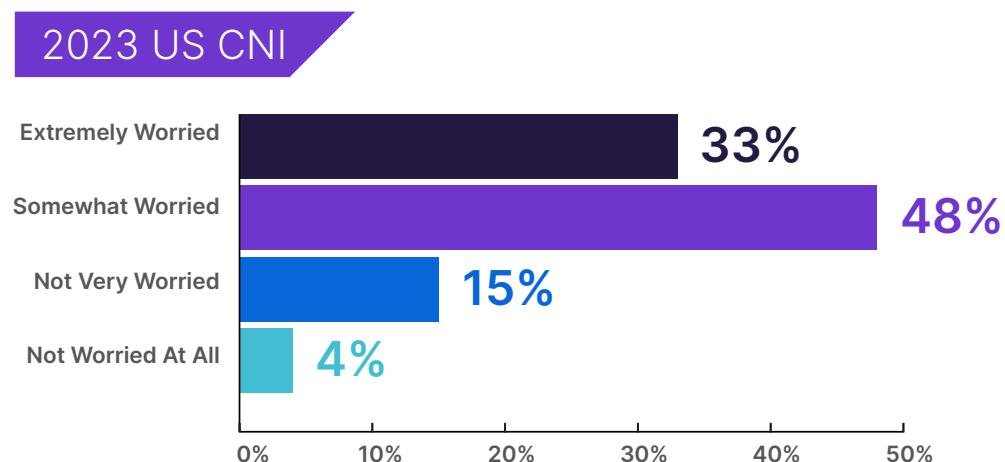
Current Threat Landscape

The events of 24th February 2022 sent shockwaves through global industries, underlining the very real threat of nation state-backed cyber attacks against CNI. With the digital world fast becoming a new theater of war for calculated, powerful, and political adversaries, operators of critical infrastructure are having to take urgent steps to understand the motivations of threat groups and develop preventative strategies.

Now, over a year after the Russian invasion of Ukraine, levels of concern about the threat of cyber warfare remain high across CNI. Over eight-in-ten (81%) of respondents are worried now about the threat of cyber warfare against US critical infrastructure – with 33% ‘extremely worried’.

“Over eight-in-ten (81%) of respondents are worried now about the threat of cyber warfare against US critical infrastructure – with 33% ‘extremely worried’.”

How worried, if at all, are you about the threat of cyber warfare against critical infrastructure now?



Current Threat Landscape

Overall levels of concern drop slightly to 75% in the next six months, 70% in the next 12 months, and 65% in the next five years. While still high, there is some cause for optimism, as figures suggest that organizations are becoming more confident as the new reality of nation-state cyber threats sinks in.

Nevertheless, the majority of respondents across IT and OT environments (64% and 59% respectively) agree that the volume of threats has increased over the last 12 months, with over a quarter strongly agreeing.

Accordingly, the volume and breadth of cyber threats faced by organizations in the past year has been substantial. CNI organizations are repeatedly coming under siege from malicious actors exploiting a variety of vulnerabilities within their IT and OT infrastructure, both externally and internally.

“ The majority of respondents across IT and OT environments (64% and 59% respectively) agree that the volume of threats has increased over the last 12 months. ”

Mean Number of Attacks Suffered in the Past 12 Months:

Attack	2023 survey
Ransomware	26
Supply chain attacks	27
Employee sabotage	27
Data theft or misuse	28
Physical security breach	27
Malware	27
Phishing	27
Unauthorized employee access	27
Social engineering	27
Nation-state attacks	27
Business email compromise	28
Terrorist threats	27
Accidental data loss/disclosure of data	25
Exploitation of unpatched vulnerabilities	27
Unauthorized devices	26
Drone threats	25
DDoS	27

Current Threat Landscape

Between 2022 and 2023, organizations suffered an average of 27 nation-state attacks. Almost a fifth (19%) reported a mean of more than 50 attacks. It appears that nation-state actors are becoming increasingly ambitious in the cyber domain, potentially as a result of nations like Iran and China joining Russia in evolving their threat tactics.

But despite this figure, organizations should avoid focusing on nation-state threats at the expense of other crimes, which are showing similar levels of frequency. From physical security breaches to social engineering, distributed denial of service (DDoS) and ransomware, a broad array of threats are placing unprecedented pressures on the systems and networks that underpin our most critical infrastructure.

Between 2022 and 2023, organizations suffered an average of 27 nation-state attacks. Almost a fifth (19%) reported a mean of more than 50 attacks.



Rise of Ransomware

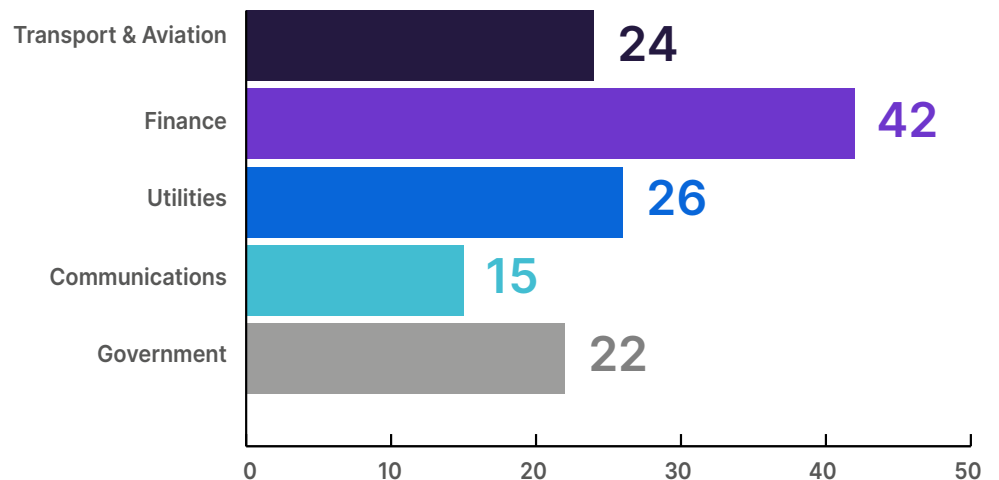
Ransomware remains a significant threat to CNI. Organizations have suffered on average a total of 26 ransomware-related security incidents in the last 12 months, with almost a fifth (17%) experiencing a mean of over 50 incidents – an average of one every week.

// Organizations have suffered on average a total of 26 ransomware-related security incidents in the last 12 months. //

In March this year, the White House unveiled its National Cybersecurity Strategy, which reclassified ransomware attacks as a tier one national security threat. This follows a continued rise in the scale and complexity of ransomware, with a series of major cyber attacks recently hitting CNI, food suppliers, hospitals, and even schools. However, the increased prevalence of ransomware is far from a US-only problem – CNI cyber decision-makers in the UK report similar figures, with organizations seeing a 50% rise in the average number of ransomware-related security incidents over the last 12 months alone.

Across US infrastructure, ransomware is a growing risk for all sectors:

Mean Number of Ransomware-Related Incidents Suffered



The finance sector was targeted by more ransomware attacks than any other CNI sector. Due to the large amounts of sensitive data institutions gather about clients, employees, and partners, financial organizations are highly attractive targets for double-extortion attacks. We saw this recently when the Russia-backed [LockBit ransomware gang](#) targeted a division of financial software firm ION Group, causing disruption and undisclosed financial losses across the US and Europe and forcing several banks to process trades manually. As regulators continue to hold the finance sector to high security standards, organizations need to take further steps to boost resilience in the face of more frequent, sophisticated, and costly ransomware threats.

What is RaaS?

Ransomware-as-a-Service (RaaS) is a lucrative business model that involves selling or renting ready-made ransomware tools to customers, or affiliates. This enables criminal groups to maximize their financial gains with the minimum of complication or risk, as even the most low-level and unsophisticated threat actors can access everything they need to carry out an attack without having to write their own ransomware. Using the dark web as a platform for selling and collaborating, operators of RaaS are also notoriously difficult to track down or prosecute.

RaaS and other 'as-a-service' offerings pose a growing threat to all CNI organizations. Since 2021, when [Colonial Pipeline](#) was hit by a crippling ransomware attack at the hands of the Darkside RaaS group, tactics have continued to diversify and intensify. Criminals are exploiting this efficient operating model to keep costs low and become even more targeted in their attacks.

To mount a more proactive defense against RaaS, organizations need to look beyond prevention alone. Instead, they must consider how they can limit the damage of these attacks through effective detection and response. There are multiple opportunities within the kill chain to detect malicious activity and take action. If the organization can identify an attack at the earliest opportunity, they can adapt controls to defend against the threat and quickly restore systems to their previously healthy state once the immediate threat has been neutralized.

However, despite the increasing number of ransomware attacks suffered across CNI, only 23% of respondents identify ransomware as a top risk to their organization's IT and OT environments.

It is possible that a disconnect exists around the prioritization of security and the number of attacks being suffered. In any case, CNI leaders have a wide variety of other security challenges and concerns – encompassing both the technical and human elements of cyber security – which is perhaps leaving some struggling to focus their security efforts.



The Human Factor

Cyber security is not just underpinned by technological architecture – it is fundamentally shaped by human behavior and decision-making. As such, sectors across CNI are realizing the need to consider and mitigate internal, end-user-driven cyber threats as much as threats from outside the organization.

Over three-quarters (77%) of respondents have seen an increased cyber security risk from insiders (whether malicious or negligent) over the last three years. As remote/hybrid working patterns continue their upward trajectory and workforces become ever-more distributed, the growing dependence on interconnected digital technologies has widened the attack surface and left organizations more exposed to cyber risks. Rising insider risks could also align with the mounting geopolitical and economic challenges of recent months, with threat actors looking to exploit human vulnerabilities and fears.

“Over three-quarters (77%) of respondents have seen an increased cyber security risk from insiders (whether malicious or negligent) over the last three years.”

Across IT environments, the ‘people risk’ is heavy on the mind of CNI decision-makers:

Top 3 Risks Facing IT Environments:

- 1 Data theft or misuse (28%)**
- 2 Distributed Denial of Service (DDoS) (28%) (joint 1st)**
- 3 Accidental loss or disclosure of data (26%)**

Data theft and accidental loss or disclosure of data are now among the top perceived risks to organizations’ IT environments. This highlights the extent to which human error can lead to cyber breaches, particularly in finance, where over a third (34%) of respondents named accidental loss/disclosure of data as their biggest IT risk. While most financial services firms have robust technical measures in place to protect their sensitive data from outsiders, opportunities for employees to make honest mistakes have risen in remote and hybrid settings, with staff now able to consult and share privileged information from anywhere across multiple devices.

The Human Factor

In an increasingly interconnected and complex global financial ecosystem, traditional 'ring of fire' perimeter defenses can be easily bypassed – meaning that employees in the financial sector must perform a dual role as business partners and key cyber security assets. The sector has shown a high level of maturity in vetting and monitoring staff to avoid intentional or negligent security lapses, but organizations remain acutely aware of the internal risks that come with today's era of mobile computing, cloud-based services, and dispersed workforces.

To avoid the heavy financial, reputational, and legal consequences of an accidental breach, firms must implement clear written policies and procedures related to data security standards, whilst consistently educating employees on cyber security best practice.

“Almost a quarter (23%) of CNI organizations now regard social engineering and phishing as two of their biggest OT risks.”

Top 3 Risks Facing OT Environments:

- 1 Social engineering (25%)**
- 2 Phishing (24%)**
- 3 Supply chain attacks (23%)**

Breaches targeting the human element are also posing significant risks to OT environments. Almost a quarter (23%) of CNI organizations now regard social engineering and phishing as two of their biggest OT risks. Within the US energy (oil and gas) sector, this figure rises to 26%, reflecting an [increase in spear phishing campaigns](#) against global energy firms. A more elaborate and sophisticated version of phishing, spear phishing uses advanced social engineering techniques to target specific organizations and individuals, often impersonating family members or colleagues via spoofed emails to manipulate employees into committing unauthorized actions.

The Human Factor

Phishing is a foundational technique for getting credentials and allowing access to a victim's system which is often used as a springboard for multiple attacks ranging from data theft to equipment damage. Phishing can be countered by developing a culture of awareness around phishing that educates employees on what to look out for and implements appropriate information security policies and controls to mitigate risk.

It's significant that social engineering and phishing are now considered major cyber risks facing OT. As the boundary between IT and OT continues to blur, and traditionally isolated systems become more interconnected and interdependent, the OT attack surface inevitably expands. This can result in vulnerabilities in OT systems being exploited by attackers who have already gained access to the IT network – and if organizations do not have cyber security experts with high levels of familiarity with OT, they may struggle to recognize and respond to this new breed of targeted social engineering.

Accordingly, CNI decision-makers across the IT/OT boundary identify improving cyber security awareness and education as one of their biggest security challenges (18%). Establishing organization-wide awareness of new and emerging security threats, including social engineering tactics, is crucial in ensuring that employees understand the important role they play in protecting both their organization and society at large.

It is essential that organizations across CNI support and educate all their people on cyber security best practices. This need is nothing new – but with over a third (37%) of OT respondents stating that the prevalence of social engineering and phishing attacks is likely to grow further due to the economic downturn, it's likely to be an area of increased focus in the months ahead.



Cyber Security and Economic Pressures

With economic challenges and the threat of recession set to continue through 2023, pressures are mounting on employees. Many are already feeling the squeeze of higher gas and food prices – and as the focus of both companies and employees increasingly turns to financial stability, security issues could be sliding down the priority list.

This can create opportunities for insider threats to go unnoticed. Over in the UK, which is facing an ongoing 'cost-of-living crisis', it was recently reported by Zurich that [theft at work](#) has jumped by a fifth, with crimes ranging from petty pilfering of office supplies to the theft of data and embezzlement of company funds. Rising costs could be triggering a spike in employee crime, as workers increasingly steal from their employers to make ends meet.

Financial pressures also present a significant risk to CNI organizations – already highly valued targets of cyber crime. Organized criminal groups are primed to exploit people's vulnerabilities by reaching out to individual employees within an organization, often offering them a lucrative payoff in return for access to sensitive data or protected systems.

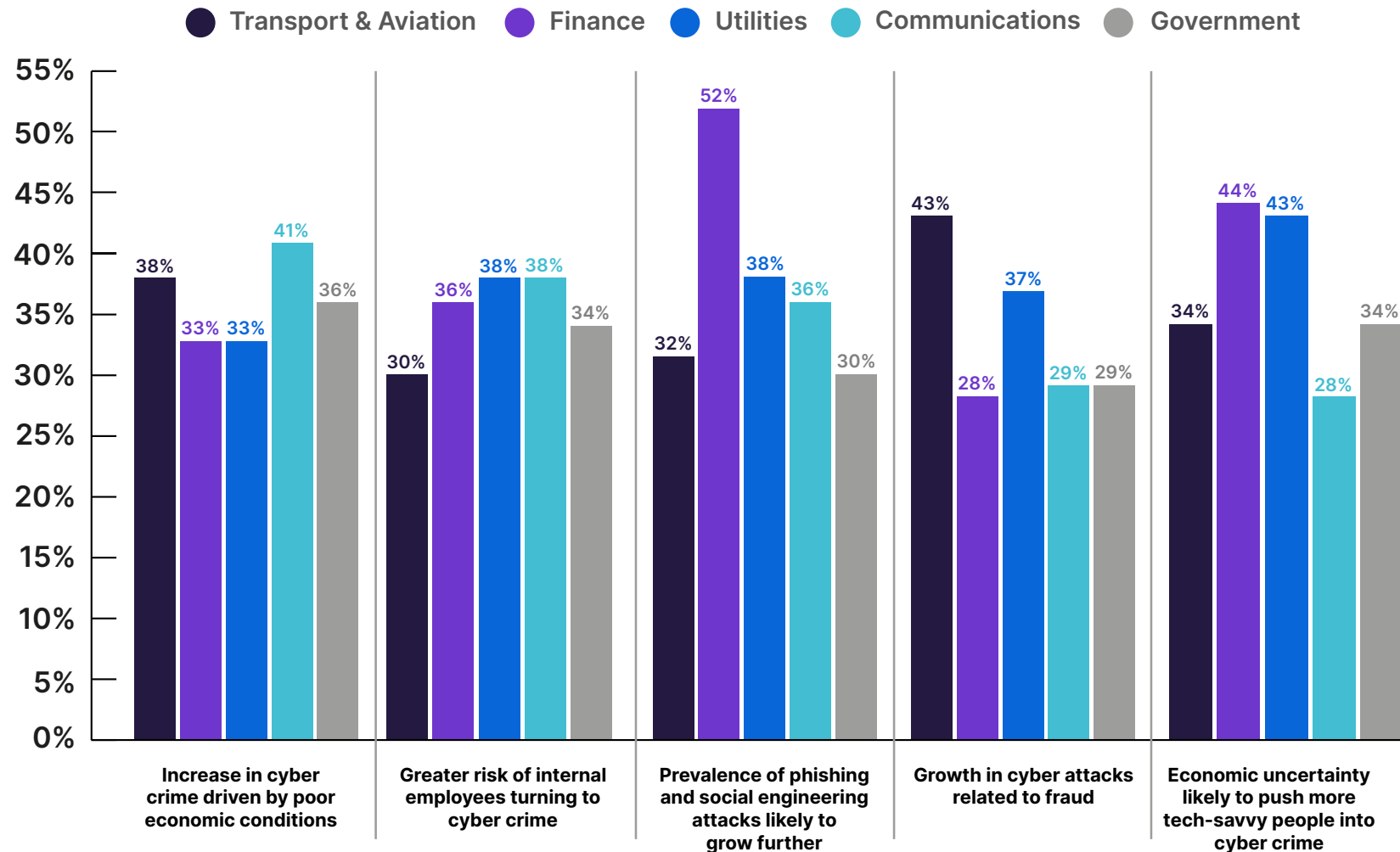
Accordingly, over a third (35%) of CNI decision-makers believe that the economic downturn is causing more internal employees to turn to cyber crime.

“Over a third (35%) of CNI decision-makers believe that the economic downturn is causing more internal employees to turn to cyber crime.”



Cyber Security and Economic Pressures

What are/will be the main impacts of the coming downturn on the cyber-risk posed by people?



Cyber Security and Economic Pressures

Employees struggling with economic insecurity could have their judgement clouded when they are offered the motivation or means to commit cyber crime. According to [Ponemon's 2022 Cost of Insider Threats](#), these types of attack have risen 44% over the past two years, with costs per incident exceeding \$15 million.

Within US CNI, the insider threat seems particularly prevalent in the finance sector. Financial services organizations suffered on average 41 security incidents caused by employee sabotage over the past 12 months, along with 40 instances of data theft or misuse – by far the highest average amongst all sectors. Finance also experienced significantly more social engineering attacks than other sectors, with a mean of 44 in the past year alone.

// **Financial services organizations suffered on average 41 security incidents caused by employee sabotage over the past 12 months, along with 40 instances of data theft or misuse – the highest average amongst all sectors.** //

To mitigate rising internal security risks – whether driven by employee negligence or criminal intent – organizations should invest in strengthening their cyber defenses from the inside out, carrying out continuous vulnerability assessments to provide a detailed picture of their attack surface. Sophisticated penetration testing methods, such as Red Teaming, can also simulate a range of internal attacks.

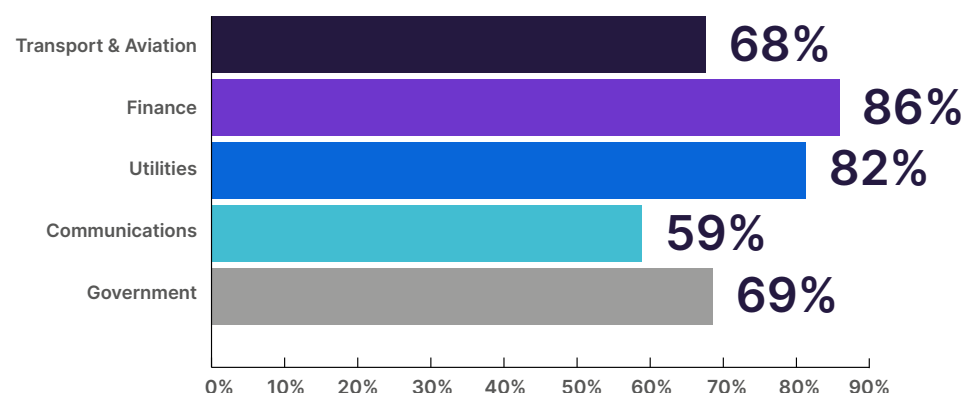
Top Tips for Reducing Insider Risks

- **Background checks:** The hiring process is the first stage where an organisation can reduce the risk of insider threats. Employers should perform thorough financial checks and referencing on individuals who will have access to confidential information and systems.
- **Appropriate access and controls:** Employees should have access to what they need and nothing more. Determine appropriate standards for access and controls around sensitive data – and ensure individuals understand the specific risks posed by the level of access they have.
- **Robust monitoring:** Proactively monitor for any anomalous activity on confidential systems. For example, are employees exporting large numbers of files at unusual times of the day?
- **Training and awareness:** Help employees understand what insider threats look like and how to identify suspicious activity. Training should be continuous and regularly updated to reflect the changing threat landscape.

Impact on Cyber Budgets

However, against a backdrop of evolving security threats, the economic pressures facing CNI are causing some organizations to re-evaluate their cyber spend. This is in sharp contrast to 2022, when cyber security budgets rose across all sectors.

“We’ve already seen a reduction in cyber security budgets due to the economic downturn”:



Almost three-quarters (73%) of respondents across US CNI have seen some reduction or a significant reduction in their organization’s cyber security budget.

The communications sector has been impacted the least by cyber budget cuts, with 41% seeing no change in cyber security budgets. This could align with the implementation last year of [tough new security rules](#) to protect UK telecoms networks against cyber attacks. Under much greater regulatory scrutiny, organizations may be more incentivized to embed robust cyber security practices within their long-term investment decisions.

However, the finance and utilities sectors (including energy, oil, and gas) have experienced the greatest fall in cyber budgets, with 84% of collective respondents seeing some reduction or a significant reduction. For energy, oil, and gas, this is perhaps unsurprising given the extraordinary pressures the sector is under – but it does leave energy providers particularly vulnerable to large-scale attacks from hostile nation-states and organized criminal groups.

As economic instability continues to squeeze budgets across all industries and business sizes, CNI operators should avoid losing sight of the progress made in previous years. Strategic cyber security spend has helped many organizations to close the security gaps and weaknesses that traditionally made them easy targets.

Therefore, instead of reducing their cyber security investment, CNI organizations need to allocate their budget more smartly, investing in tools and technology that support cyber resilience. This can be done even with a stretched budget – the consolidation of security tools and the utilization of managed detection and response (MDR) services supports companies in managing costs whilst shifting from a reactive to proactive security posture.

Identifying and Meeting the Evolving Threat Landscape

Top 3 cyber security challenges facing IT:

- 1 **Data protection and privacy (22%)**
- 2 **Lack of cyber security talent/expertise (21%) / Improving awareness and education of cyber security (21%) (joint)**
- 3 **Supporting remote and hybrid working (20%)**

The top-ranked cyber security challenges facing CNI in 2023 are emblematic of how the world has fundamentally and irreversibly changed in recent years. As hybrid and remote arrangements shape the 'new normal' of work, additional layers of complexity and risk have been introduced to data protection and privacy – the highest rated security challenge facing IT environments (22%).

With millions of employees rotating between home, the office, and anywhere in between, securing devices and networks against potential data breaches has become significantly more complex. Organizations are now prioritizing cyber security education and awareness (21%) as a means of mitigating the risks of data exposure, at a time when human error is responsible for up to 82% of breaches.

Top 3 cyber security challenges facing OT:

- 1 **Disaster recovery and business continuity (25%)**
- 2 **Managing cloud cyber security (24%)**
- 3 **Managing supply chain risks (22%)**



Identifying and Meeting the Evolving Threat Landscape

As more organisations move towards remote working to support flexibility and increased autonomy, there is a fine balance to ensure cyber security best practice (once centralised in offices and on company-secured Wi-Fi networks) is still adhered to. Some key considerations when providing employees with remote working are:

1 Implementing Multifactor Authentication (MFA)

This adds an extra layer of security by requiring the user to confirm their identity through multiple, alternative methods, thus reducing the risk of inappropriate access through compromised passwords.

2 Zero Trust Policy

This is a user-centric approach that verifies the identity of users, rather than relying on network-based trust. This approach is particularly relevant for remote work, where users may access resources from external networks, to ensure that only authorized users are granted access.

3 Incident Response Testing

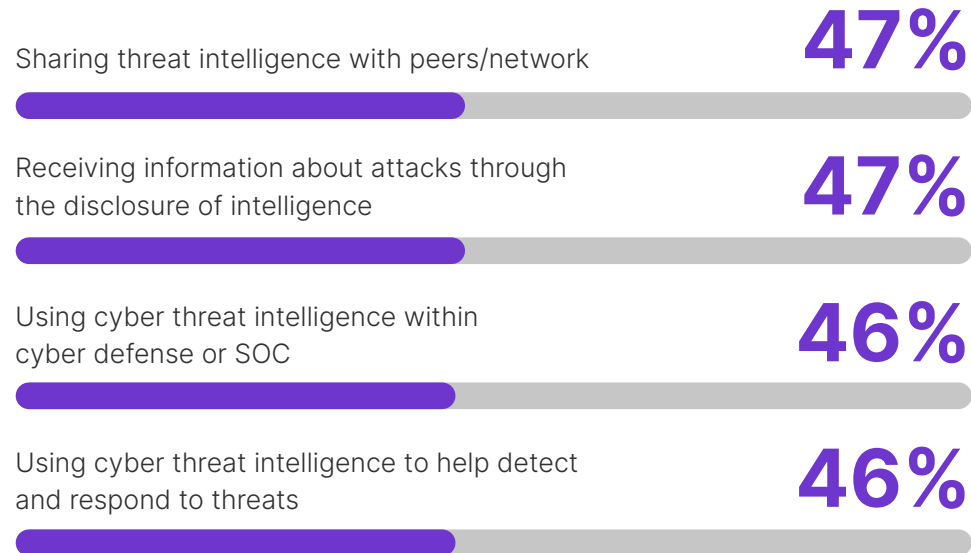
The prospect of an incident may be overwhelming when your workforce is spread across networks and locations, amplifying the need to ensure users know their roles and responsibilities in the event of an incident. Ensuring that your incident response plan is appropriate and tested for remote workers is essential in protecting your business against increased exposure during a cyber incident.

Meanwhile, supply chain and cloud concerns are front of mind for today's OT security leaders. This, too, reflects the changing landscape organizations are operating in. Industrial systems are increasingly being integrated with cloud services and supply chain networks, which has led many organizations to work with multiple third parties to enhance productivity. This has inevitably created new risks.

With change becoming the only constant in the cyber security landscape, CNI organizations must be agile enough to prevent, withstand, and recover from a wide range of evolving threats. To achieve this cyber resilience during these turbulent times, CNI operators should focus on three of its critical components: threat intelligence, visibility, and cyber maturity.

How Do CNI Organizations Detect Breaches?

Fewer than half of organizations are undertaking critical threat intelligence practices:



Furthermore, almost a quarter of respondents don't agree that they act on information received about attacks through the disclosure of intelligence or receive threat information in a timely fashion from the supply chain (both 22%). This figure is higher for OT than for IT, suggesting that OT operators should take further steps to proactively identify and analyze potential cyber threats.

To meet the requirements of relevant regulatory frameworks - such as the NIST Cybersecurity Framework (CSF) - CNI organizations must commit to strengthening these practices and ensuring all cyber resilience principles are tightly aligned with their wider business objectives. In particular, organizations should build a culture of timely information-sharing among peers and supply chains - and improving the number of threats detected internally is a crucial first step.



How Do CNI Organizations Detect Breaches?

Encouragingly, organizations across all sectors are more likely to discover a data breach through a proactive threat detection program or system (36%), or other threat intelligence capabilities, than through more reactive means:

Top Ways of Discovering Data Breaches per Sector:

Transport and Aviation

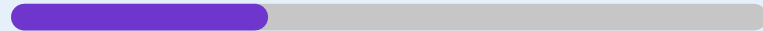
Through a proactive threat detection program/system **36%**



Internal employees reporting **34%**



By notification from a customer or partner **34%**



When details are posted on the dark web **34%**



Discovered by digital risk and threat intelligence capabilities **30%**



Finance

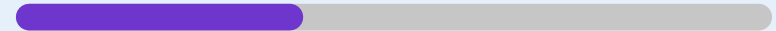
Discovered by digital risk and threat intelligence capabilities **46%**



When details are posted on the dark web **39%**



Internal employees reporting **38%**



By the media **37%**



By notification from a customer or partner **34%**

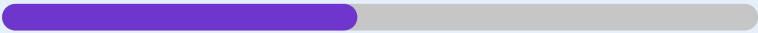


How Do CNI Organizations Detect Breaches?

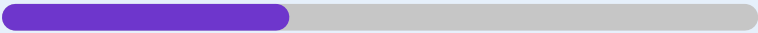
Top Ways of Discovering Data Breaches per Sector:

Utilities


Through a proactive threat detection program/system **47%**



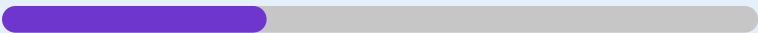
Discovered by digital risk and threat intelligence capabilities **38%**




When details are posted on the dark web **38%**



By notification from a customer or partner **35%**

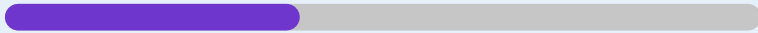


When details are published on public forums **33%**

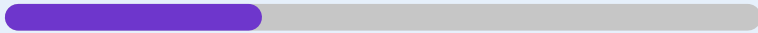


Communications


Discovered by digital risk and threat intelligence capabilities **39%**



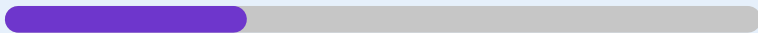
Internal employees reporting **34%**




Through a proactive threat detection program/system **32%**



When details are posted on the dark web **32%**

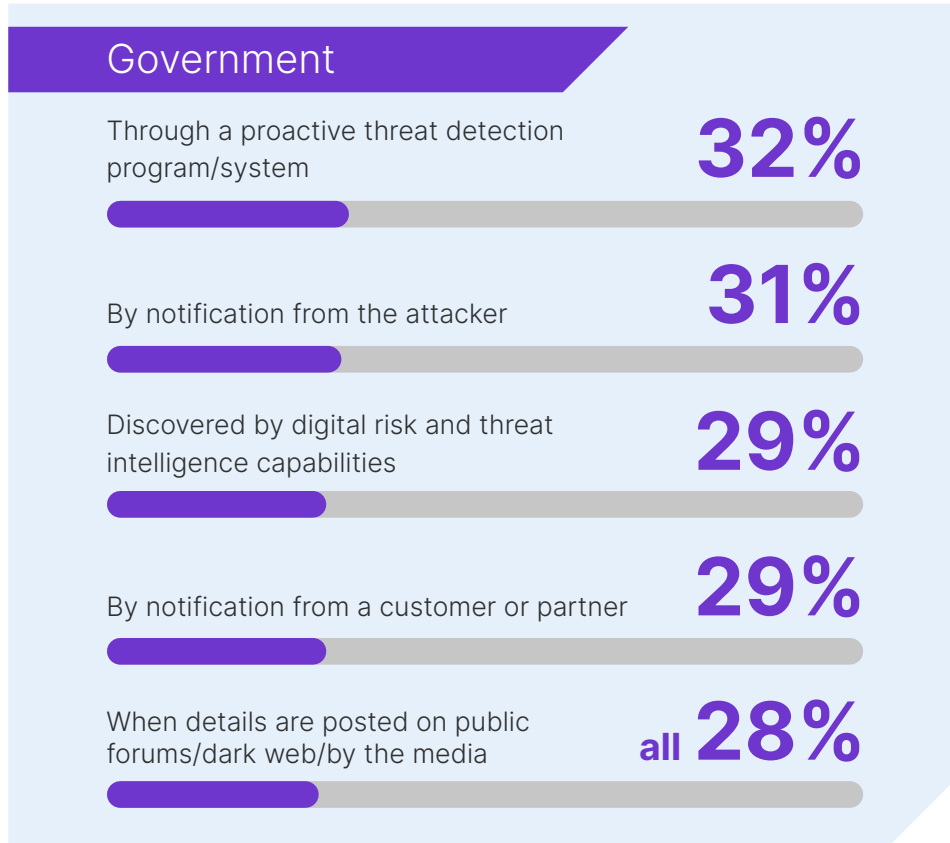


When details are posted on public forums **31%**



How Do CNI Organizations Detect Breaches?

Top Ways of Discovering Data Breaches per Sector:



However, failing to utilize threat intelligence can lead to breaches only being discovered when details are exposed by the media (28%), posted on public forums (31%), or even the dark web (34%) – a current reality for a significant proportion of overall respondents.

Threat intelligence is integral to cyber resilience, as it enables organizations to develop better incident response plans that are tailored to the specific threats they are likely to face. It also allows organizations across CNI to share intelligence and collaboratively identify and respond to evolving cyber threats, strengthening the sector's overall security posture.

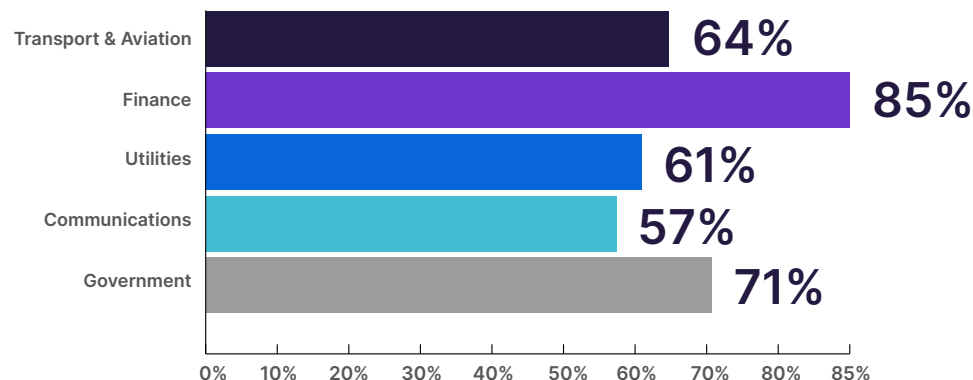


Achieving End-to-End Visibility

For security teams to detect and respond to cyber threats quickly and effectively, they need full visibility across their assets. This is proving a challenge for CNI, particularly as IT/OT convergence continues to blend previously separate technologies, teams, and processes.

“We don’t have sufficient visibility over all our end user devices, networks and systems”:

Agree:



Almost two-thirds of respondents (65%) overall say their IT environment lacks sufficient visibility over all end user devices, networks, and systems, with a similar number (63%) saying they don’t have sufficient visibility over the IT network boundary.

“Almost two-thirds of respondents (65%) overall say their IT environment lacks sufficient visibility over all end user devices, networks, and systems, with a similar number (63%) saying they don’t have sufficient visibility over the IT network boundary.”

OT tells a similar story, with two-thirds (63%) lacking sufficient visibility over all end user devices, networks, and systems. Many OT systems have traditionally been designed with a decades-long lifespan in mind. As these systems increasingly converge with fast-moving IT networks and IoT devices, maintaining centralized visibility and control can be challenging. Accordingly, 64% of respondents across operational technology agree that they lack sufficient visibility across the OT network boundary.

Achieving End-to-End Visibility

“ Although financial services companies have concerns about security in the cloud, they are using cloud infrastructure for highly sensitive and restricted workloads. Nearly a fifth of such workloads operate in the cloud, the CSA found. This allows for greater agility in day-to-day operations but does introduce a new dimension of risk compared to traditional IT infrastructure. For financial service organisations, visibility in the cloud remains an issue. This could be due to their reliance on multiple cloud service providers, which can make it difficult to achieve a unified view across all cloud endpoints. This is especially the case for organizations that lack the right tools to integrate and correlate data from across multiple sources. ”

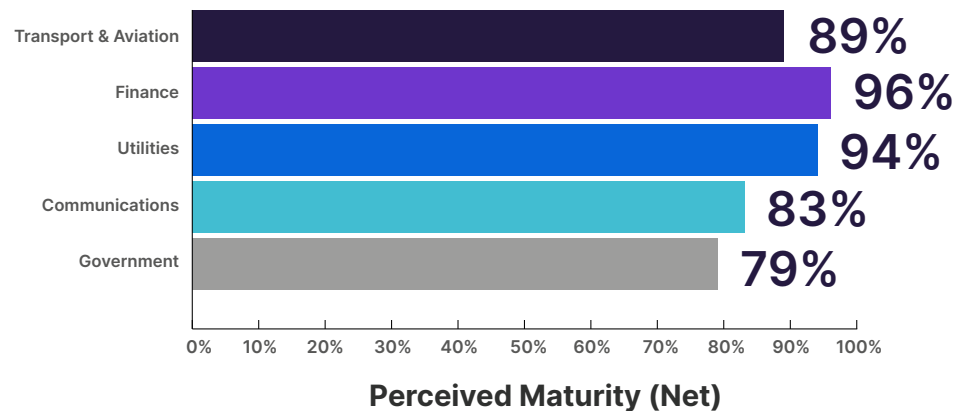
- Jack Willis, Principal Cyber Security Consultant

Organizations now need to integrate their myriad technologies and tools to build a rich view of all their assets, enabling them to gain a thorough, comprehensive understanding of their security posture. They can do this by engaging with MDR and Extended Detection and Response (XDR) services, which are designed to detect, mitigate, contain, and remediate threats across a company's entire technology stack.



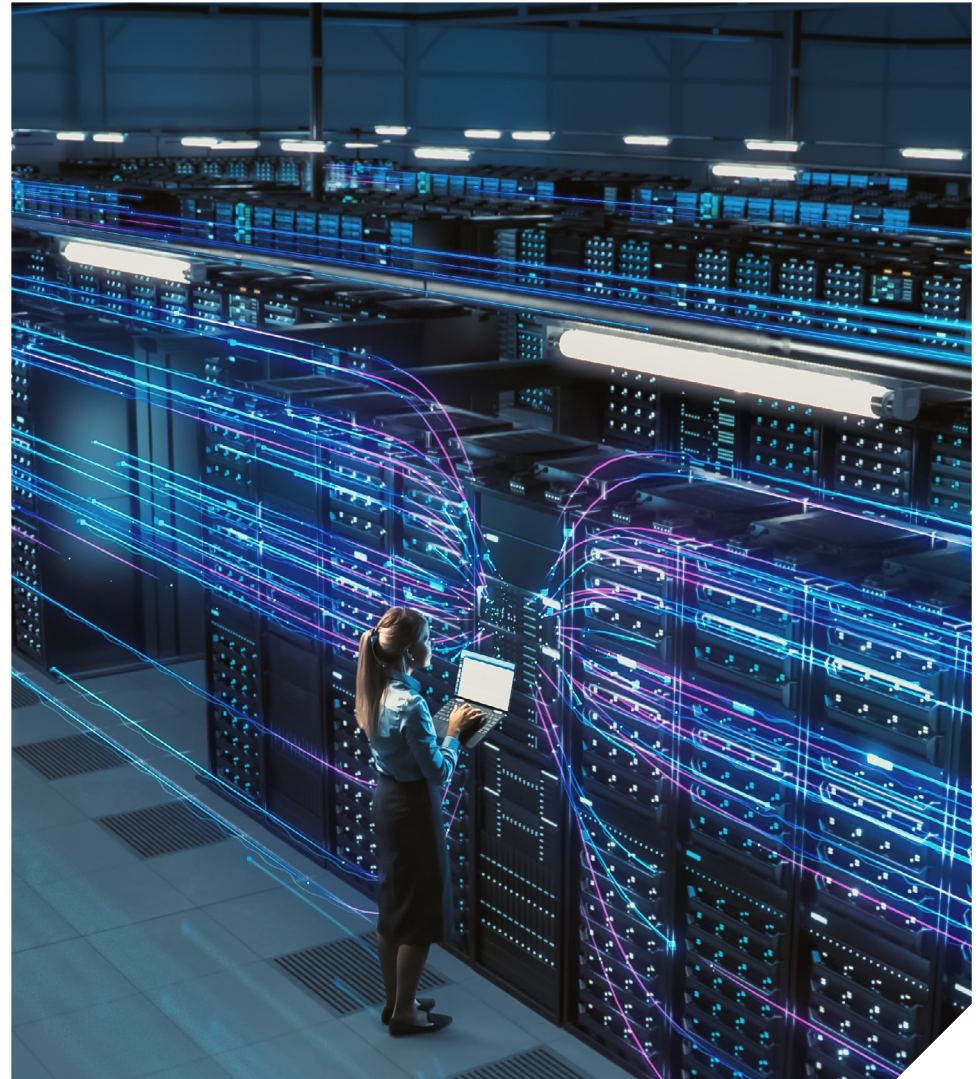
Cyber Maturity in 2023

Organizations show a high level of confidence in their cyber maturity:



Across IT and OT, 89% of respondents say their organization demonstrates maturity in relation to implementing a cyber security strategy, achieving key goals, and measuring performance.

However, gaps start to emerge when the specific tenets of cyber maturity are examined, suggesting that this confidence could be misplaced. For example, almost three-quarters (73%) of respondents admit that their organization takes a reactive approach to cyber security transformation in its OT environments, whereby security is only considered afterwards. In IT environments, seven-in-ten (70%) decision-makers admit that their company struggles to understand how and why a breach has taken place.



Cyber Maturity in 2023

As organizations progress on their security transformation journeys, they must develop their cyber maturity by continuously assessing risks, identifying vulnerabilities, and proactively implementing measures to mitigate these risks and vulnerabilities – rather than waiting until a breach has occurred.

Only a minority of CNI organizations have already implemented the policies, procedures, processes, and systems necessary to continuously manage information security risks:

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

	Already Implemented
An effective and audited information security management system (ISMS) for IT	20%
An effective and audited information security management system (ISMS) for OT	25%
24/7 security monitoring on IT	25%
24/7 security monitoring on OT	26%
Hybrid security operations centre (SOC) services on IT	24%
Hybrid security operations centre (SOC) services on OT	24%
Managed detection and response on IT	20%
Managed detection and response on OT	24%
Threat hunting and cyber threat intelligence	25%
Cyber security strategy aligned to business objectives	23%
KPI and value levers for cyber security	21%
Board level representation	22%

Reassuringly, however, the majority of respondents have plans to implement these crucial services and strategies within the next 12 months, recognizing the vital role they play in strengthening cyber maturity through the round-the-clock monitoring and safeguarding of critical systems and data.



Conclusion


As geopolitical and economic disruptions continue to make their mark on the cyber threat landscape, operators across CNI need to build a strong understanding of the specific risks they face in the immediate term – both from outside and within the company. At the same time, they must take a longer-term strategic view of their organization and its place in an increasingly connected, complex, and unstable world. While short-term measures such as reducing cyber budgets or delaying key security projects may be tempting at times of financial hardship, it's more important than ever for organizations to allocate their resources wisely, enabling them to make further progress towards their security transformation goals.

This survey set out to evaluate the shape and scale of today's cyber threat landscape, along with how CNI organizations are faring in this ever-more fraught environment. Our findings suggest that many organizations are rising to the challenge, particularly when it comes to collaborating across industries and across OT/IT boundaries. However, there is always room for improvement – and companies now need to take more proactive steps towards strengthening and maturing their cyber security posture. Leveraging rich, threat-led intelligence and maintaining end-to-end visibility across their diverse environments will help organizations to achieve this maturity and resilience, even as they come under ever-greater security demands.





Bridewell

 +1 713 300 4009

 hello@bridewell.com

 bridewell.com