Bridewell
CONSULTING
Above. Beyond. Always

CNI Cyber Report:
Risk & Resilience

Introduction

Daily life in the UK depends on our Critical National Infrastructure (CNI). As we continually seek increased connectivity, the need for more remote working practices, improved operational management and legacy infrastructure upgrades, coupled with growing challenges posed by increasing cyber threats and new legislative requirements, is putting significant demand on our CNI.

Traditionally many organisations within CNI sectors have managed Industrial Control Systems (ICS) and critical applications on their own closed private networks and often the availability of those systems is king. However, the rise of the Internet of Things has brought the benefits of connectivity to the fore and there is a growing need to drive convergence between critical operational technology, IT networks and the internet for remote management. This introduces a completely new attack surface and a wider range of threats.

All these factors lead to some very important questions: how true are the perceived threats and risks to CNI? What are the biggest risks and challenges? Has regulation helped? And what does the future look like for the sector?

To answer these questions we commissioned independent research organisation, Censuswide, to conduct research among 250 UK IT and security decision-makers across five key CNI sectors: aviation, chemicals, energy, transport and water.

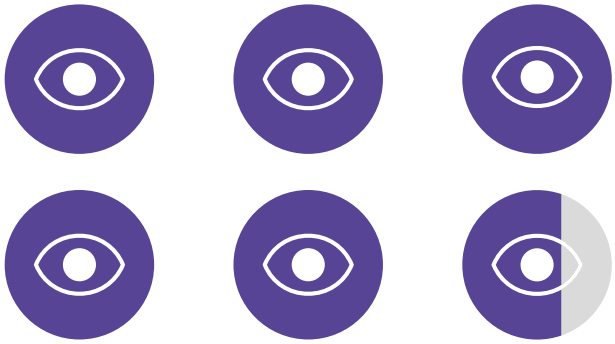
This report seeks to understand the current state of cyber security in the CNI, exploring the trends, attitudes and challenges organisations are facing. It will take a deep dive into a range of subject areas including confidence in cyber security, attack volumes, cloud adoption, skills and regulation.

Contents

Snapshot of key findings

Confidence in CNI cyber security is high...

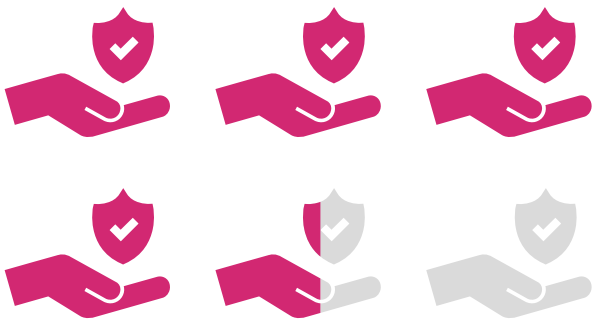
- 78% of organisations are confident that their OT systems are protected from cyber threats
- But less than a third (28%) are 'very confident' their OT systems are protected
- 73% of organisations believe they have the right skills in place to maintain and secure their OT environment



93% have experienced a successful attack in the last 12 months

Ageing infrastructure and increased connectivity is introducing new risks

- The majority of organisations are using ageing infrastructure:
  - » Over three quarters (79%) of organisations' main OT systems are over five years old
  - » Over a third (34%) are over 10 years old
- Systems are becoming more accessible:
  - » The majority (84%) of OT/ICS environments are accessible from corporate networks
  - » Only 42% say their OT/ICS environments are not accessible from the internet and 22% of these have plans to make them accessible

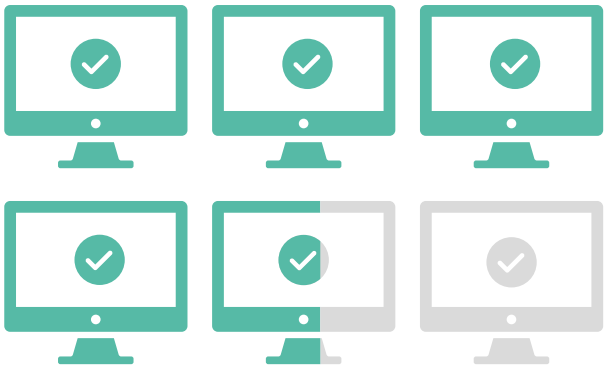


73% of organisations believe they have the right skills in place to maintain and secure their OT environment

...Yet, CNI is facing a cyber siege

86% of organisations have detected cyber attacks on their OT/ICS environments in the last 12 months

- Of these, 93% experienced at least one successful attack on their OT/ICS environments in the last 12 months
- Nearly a quarter (24%) have experienced more than 5 successful attacks
- Over two-thirds (69%) have experienced between 1-5 successful attacks
- Water and transport experienced the most successful attacks



79% of organisations' main OT systems are over 5 years old

Organisations are facing a plethora of different threats

- The top three threats are cyber attacks (39%), malware (34%) and physical security risks (28%)
- Only 18% see third party suppliers / partners as the biggest risk to their organisation

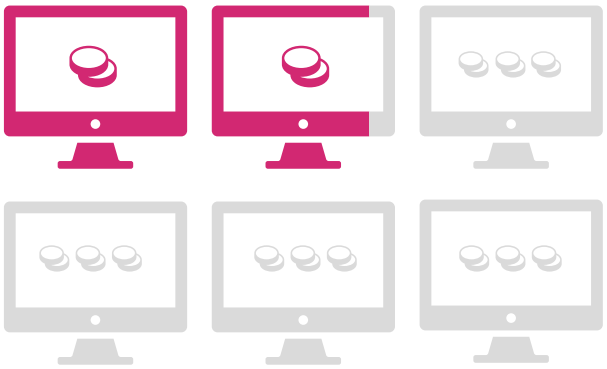
Responsibility for cyber security of OT/ICS systems is spread across teams

- 32% of organisations say the responsibility belongs to a combination of the IT team, security team and OT/engineering team
- 25% say the responsibility belongs to the IT team
- 24% say the responsibility belongs to the security team
- 18% say the responsibility belongs to the OT/engineering team

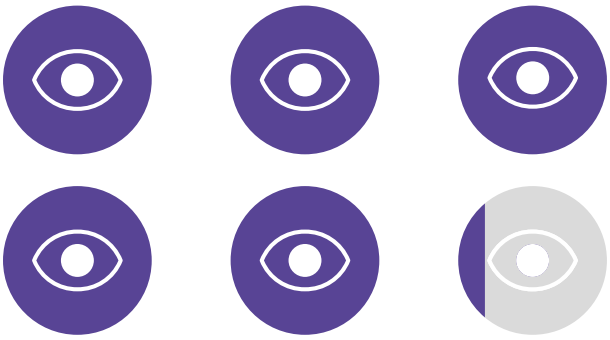
Cloud migration for OT is being widely adopted...

- 98% of organisations either have or plan to migrate elements of OT environments to the cloud
- 93% say it's either as secure or more secure in the cloud
- 84% say it's either as resilient or more resilient in the cloud

98% of organisations have or plan to migrate elements of OT environments to the cloud



32% have reduced cyber budget due to Covid-19



85% agree that they have felt increasing pressure to improve cyber security controls

...But a skills shortage is highly anticipated

- 84% of organisations agree the UK's CNI industry will be impacted by a critical cyber security skills shortage in the next 3 to 5 years

Covid-19 has reduced cyber budgets and raised risks

- 32% have reduced cyber budget due to Covid-19
- 50% have experienced increased attacks during the pandemic

Pressure is building to improve OT/ICS security controls

- 85% agree they have felt an increasing pressure to improve cyber security controls for the OT/ICS environment in the last 12 months (aside from supporting remote working in the current circumstances)

Confidence in CNI Security

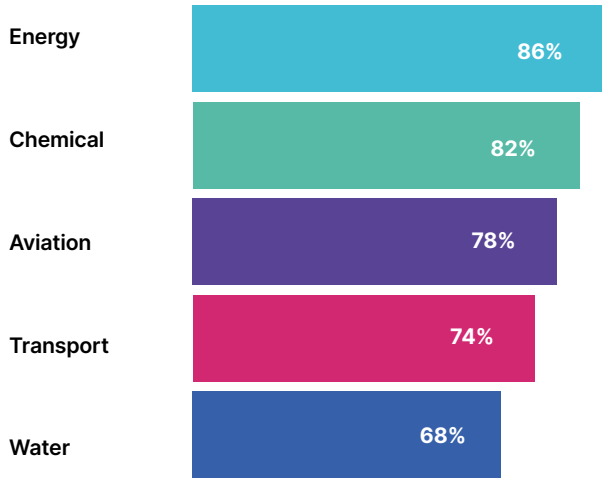
The importance of CNI and the danger that security risks could pose to human lives means that confidence in security is critical and all weaknesses need to be understood and appropriately managed.

> ***Over three-quarters of organisations (78%) are confident that their OT systems are protected from cyber threats***

Operational technology (OT) systems are at the core of CNI organisations. They monitor and control the equipment and processes that deliver vital CNI services to the nation, therefore they must be continually monitored and protected from cyber threats.

Worryingly, the survey found confidence in OT system security could be higher. Over three-quarters of organisations (78%) are confident that their OT systems are protected from cyber threats, yet less than a third (28%) of organisations are 'very confident' their OT systems are protected.

While these findings seem encouraging, a fifth of respondents said they are not confident in OT system security (16% 'not very confident', 4% 'not confident at all'). Energy, chemical and aviation are the most confident sectors.



Is this confidence misplaced?

Despite a high degree of confidence, a number of factors are putting the sector at risk. The majority of organisations rely on ageing operational technology (OT) systems. Over three-quarters (79%) of organisations' main OT systems are over five years old and a third (34%) are over 10 years old. What's more, only a fifth of organisations (20%) have implemented a new system in the last 2-5 years. The challenge with older systems is that often they don't have sufficient security support anymore, so organisations need to ensure the right security controls are introduced to ensure protection.

> ***Over three-quarters (79%) of organisations' main OT systems are over five years old***

Average age of OT systems per sector (years):

Energy	8
Chemical	8
Aviation	10
Transport	9
Water	9

Another risk is increasing accessibility and connectivity. The vast majority (84%) of OT/ICS environments are accessible from corporate networks. Of those organisations that have not made OT/ICS environments accessible from corporate networks, 80% do plan to make them accessible.

Similarly, more OT and ICS systems are becoming connected to the internet. Only 42% say their OT/ICS environments are not accessible from the internet and over half of these have plans to make them accessible.

Nearly a third (31%) of organisations use standard secure remote access mechanisms to access the internet while 26% say internet access methods to OT/ICS vary from system to system.

Traditionally CNI sectors have managed control systems and critical applications on their own closed private networks. But, a move towards open networks and an increase in connections between ICS, office networks and the internet will make these sectors more vulnerable to cyber attacks. A lot of those systems weren't designed to be put on the internet or connected up in the first place, so need to be segregated from the wider IT environment. Having clearly defined layers of network segregation provides a solid foundation to reduce the attack surface and limit an attacker's ability to move laterally within their network.

> ***Only 42% say their OT/ICS environments are not accessible from the internet***

The evolving threat landscape

Aside from the increasing risks posed by ageing and increasingly connected infrastructure, the CNI sector is facing a plethora of other threats. The majority (96%) of decision-makers think there are risks facing their organisation, with the top five threats perceived to be cyber attacks (39%), malware (34%) physical security risks (28%) social engineering (26%) and terrorism (24%).

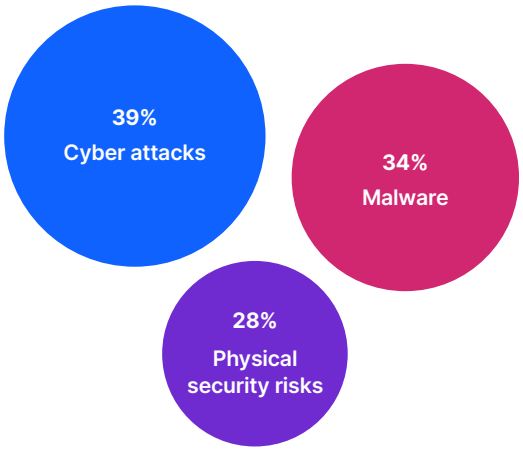
Interestingly, only 20% selected attacks from nation-states as a top risk, while threats from third party suppliers was considered the lowest threat (selected by 18% of decision-makers), which could signify a degree of complacency in supply chain risks – an area which has been highlighted by the National Cyber Security Centre as a key source of vulnerabilities.

The supply chain is an attractive target for cyber criminals as it means they no longer need to target organisations directly; they can attack vendors,

harvest information and use that to gain a foothold in the organisations they are actually after.

Organisations need to know who has access to which systems and make sure supply chain vendors have the right practices and procedures in place to deal with cyber threats. This means qualifying and quantifying all supply chain risks before flexible and adaptive risk management processes and procedures can be put in place.

Top three threats decision-makers think are facing their organisation:



The combination of older OT systems, increasing connectivity to OT/ICS environments and the plethora of threat vectors is opening the door to more risks. CNI organisations must consider updating their OT systems and isolating and segregating OT/ICS environments. The lack of understanding around supply chain risks shows a worrying lack of education around where the greatest risks lay, posing the question: do organisations need to invest more in educating teams around the different risks?

Cyber attacks are widespread

The CNI sector has been subject to a significant number of cyber attacks with the majority of organisations reporting high attack volumes on their OT/ICS systems in the last 12 months.

The majority (86%) of organisations have detected cyber attacks on their OT/ICS environments in the last 12 months with an average of nine attacks detected per organisation, with the most-targeted sectors being aviation and transport.

Average number of detected attacks in last 12 months per sector:

Energy	8
Chemical	8
Aviation	11
Transport	11
Water	8

It's no surprise that aviation remains a high target. Air transportation's importance in the economy, combined with its interconnectivity and complexity, makes it an attractive target for cyber criminals. A cyber attack has the potential to wreak major-scale havoc on major transport hubs worldwide and lead to huge numbers of delays, flight cancellations and heightened security alerts.

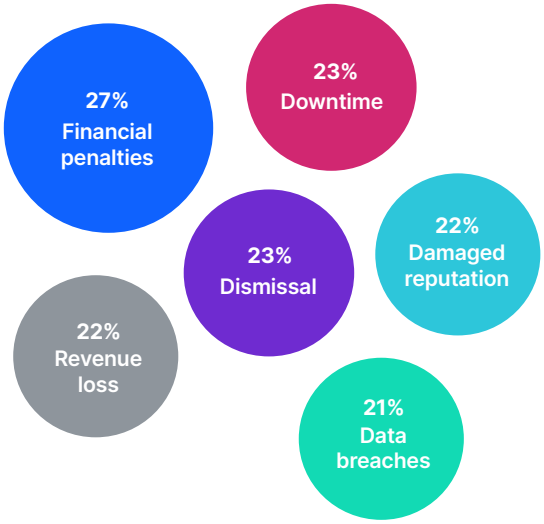
> ***The majority of organisations (93%) admit to experiencing a successful attack in the last 12 months***

The majority of those organisations that have detected attacks (93%) admit to experiencing at least one successful attack in the last 12 months. And nearly a quarter of these organisations (24%) have experienced more than five successful attacks in the same period with an average of 4.4 successful attacks per sector.

Understanding the consequences

The biggest consequences of successful cyber attacks were financial penalties (27%), downtime (23%) and dismissal of employee/employees (23%). These were closely followed by reputational damage (22%), loss of revenue (22%) and data breaches (21%). In some cases, organisations even reported increased risk to national security (19%), loss of life (16%) and environmental damage (15%).

Biggest consequences of successful cyber attacks:



To help improve cyber security, it is recognised that cyber security budgets could be increased. Only a quarter (27%) of respondents say their cyber security budget is very sufficient, nearly half (49%) say it's somewhat sufficient and almost a quarter (24%) say it's either not very sufficient or not sufficient at all.

On average, organisations spend 25% of their IT budget on cyber security and 75% say investment will increase in the next 12 months (37% significantly'; 38% 'moderately'). The transport and water sectors are set to lead in investing in the next 12 months, closely followed by aviation and energy. The chemical sector is set to see the lowest increase in investment.

Volume of organisations that will increase cyber security budgets 'significantly' or 'moderately' in the next 12 months per sector:

Energy	74%
Chemical	66%
Aviation	74%
Transport	84%
Water	78%

Impact of Covid-19

The pandemic has forced many organisations to rapidly deliver digital transformation. Many now face a completely different set of security risks than before, with cyber criminals posed to take advantage of any weakened defences.

> ***Half of IT decision-makers have experienced increased attacks since the beginning of the pandemic***

Half of IT decision-makers (50%) say they have experienced increased attacks since the beginning of the pandemic, with the biggest increases experienced in the water, transport and chemical sectors.

Changes to the volume of cyber attacks per sector since the beginning of the pandemic:

	Increase	No Diff'	Decrease	Not sure
Energy	44%	40%	12%	4%
Chemical	53%	29%	10%	8%
Aviation	45%	41%	14%	0%
Transport	53%	18%	22%	6%
Water	56%	32%	6%	6%

Covid-19 has also had a clear impact on approaches to cyber security with organisations responding by implementing new remote access technology (37%), increasing employee education (36%), introducing more security controls (34%) and increasing patching and system updates (29%). However, while 24% of organisations have increased the cyber security budget, worryingly almost a third (32%) have reduced it, despite an increase in attacks.

Cyber security strategy and controls

Encouragingly, the C-suite/senior management generally has visibility of cyber security controls according to 90% of respondents. More than half (52%) of C-Suite/senior management teams have full visibility while 38% have some visibility.

Buy-in from the C-Suite/senior management team should be the standard across every organisation. Influence from the top levels of the business help to ensure organisations are properly prepared for successful cyber attacks through implementing the right policies and procedures and having a robust response plan in place.

Vulnerability identification

When it comes to the measures implemented to help identify vulnerabilities, an overwhelming majority of organisations carry out security assurance activities with 99% of organisations saying they do so. The activities organisations use are varied with the top three assurance activities being penetration testing (42%), risk assessments (39%) and red/blue/purple team assessments (37%). However, worryingly less than half of organisations say they are currently carrying out these forms of testing.

Penetration testing and red team activities are important to the identification of vulnerabilities and it would be encouraging to see more organisations carrying out these assurance activities. Penetration testing tests the vulnerabilities in one area of the IT environment with pre-defined rules of engagement while red teaming assesses the organisation against a real-world scenario. Carrying out both penetration testing and red teaming regularly is a good all-round approach to ensuring security are as robust as they should be.

Percentage of companies who carry out security assurance activities and which types:

Top assurance activities currently carried out by sector

Aviation

- Penetration testing: 44%
- Audits using internal resource: 44%
- Risk assessments: 38%
- Audits using third-party resources: 38%

Chemicals

- Risk assessments: 54%
- Penetration testing: 36%
- Audits using internal resource: 34%
- Audits using third-party resources: 34%

Energy

- Penetration testing: 48%
- Security incident response testing: 42%
- Risk assessments: 40%

Transport

- Penetration testing: 42%
- Red team/blue team/purple team assessments: 40%
- Audits using third party resources: 38%

Water

- Audits using third party resources: 46%
- Red team/blue team/purple team assessments: 42%
- Penetration testing: 38%

Aligning physical and cyber security

It's also encouraging that physical security strategies are aligned with cyber strategies. The majority (91%) of respondents say their physical security strategy is aligned with their cyber security strategy and nearly half (49%) say they have regular joint working groups to ensure alignment.

When asked how physical and cyber security controls compare, nearly a third (32%) say physical security controls are stronger than cyber security controls, but 46% say cyber security controls are stronger than physical security controls. Just under a fifth (19%) say both physical security and cyber controls are the same.

Breaking down siloes between physical and cyber security teams is essential to improving cyber security controls. This why regular red team testing is so important. It combines physical and cyber security testing in a cohesive, robust approach. Organisations that don't ensure alignment can leave themselves open and vulnerable to escalating cyber threats.

> ***Nearly a third (32%) say physical security controls are stronger than cyber security controls***

Cloud migration

An increasing number of organisations are moving their IT systems off their premises and into the cloud. Cloud migration can offer many benefits such as cheaper operation, ease of deployment, greater scalability, potentially improved physical resilience and no infrastructure to manage. However, at the same time cloud is also one of the largest successful attack vectors if misconfigured so having the right skills to support will be key.

The majority (98%) of organisations have either migrated elements of their OT environments into the cloud or plan to do so.

Almost a quarter (23%) have already migrated all of their OT environment to the cloud while 52% say they have migrated most of it. Nearly a fifth (19%) have already migrated some of it.

Of the respondents who have migrated elements of their OT environment to the cloud, 83% have migrated all supervisory control and monitoring systems, as well as OT management services such as IDAM, malware protection servers or security patching servers. Nearly a fifth (17%) have migrated just OT management services.

Of the respondents who have migrated most or some elements of their OT environment to the cloud, 47% say it's more secure than their on-premise environment while 46% say it's as secure. That means, combined, 93% say their OT environment is either as secure or more secure in the cloud.

Skills, ownership and staff wellbeing

It's long been acknowledged that Europe is suffering a cyber security skills shortage. However, in the CNI sector most organisations feel they currently have the right skills in place. Nearly three quarters (73%) of organisations believe they have the right skills to maintain and secure their OT environment. Yet, lack of knowledge and skills was listed as the top challenge currently facing cyber security teams, with nearly a quarter of decision-makers (23%) selecting this.

> ***84% believe the UK's CNI industry will be impacted by a critical cyber security skills shortage in the next 3 to 5 years***

Looking further ahead to 2025, understanding new technology is anticipated to be the biggest challenge facing teams, again emphasising a need for the right skills and knowledge. More worryingly, 84% believe the UK's CNI industry will be impacted by a critical cyber security skills shortage in the next 3 to 5 years. Aviation is the most optimistic sector when it comes to skills and transport the least.

Does your organisation have the right skills in place to maintain and secure your OT environment?

	Yes	No	Not sure
Energy	80%	10%	10%
Chemical	72%	14%	14%
Aviation	86%	12%	2%
Transport	62%	30%	8%
Water	66%	26%	8%

Of those who believe they have the right skills in place to maintain and secure their OT environment, 69% believe it could be improved or strengthened.

Nearly half (48%) say they have separate specialists in IT and OT who work closely together, while 46% say their team fully understands both the IT and OT environment.

It's widely accepted that OT is a particular challenge when it comes to cyber security skills. The acknowledged skills gap in cyber security is made even broader around OT and SCADA as cyber security experts don't necessarily have the skills to apply this knowledge to SCADA-based infrastructures and vice versa. Therefore, it's positive to see good collaboration between both sides.

Ownership of OT/ICS cyber security

It's vital that IT and OT teams work closely on cyber security. Collaboration is vital to an organisation's health and cyber security isn't an IT or OT issue; it's a business issue and therefore must be tackled as such. Utilising third-party cyber experts in both security and engineering can also alleviate the problem.

Different organisations have different needs which drives their ownership model. Nearly a third (32%) of organisations say the responsibility belongs to a combination of the IT team, security team and OT/engineering team. A quarter (25%) say it is the responsibility of the IT team, 24% say the security team and 18% say the OT or engineering team.

Main responsibility for cyber security of OT/ICS within each sector

Aviation

- Combination of all: 34%
- OT/Engineering team: 30%
- Security team: 20%

Chemicals

- Combination of all: 36%
- IT team: 32%
- Security team: 20%

Energy

- Combination of all: 40%
- IT team: 28%
- Security team: 16%
- OT/Engineering team: 16%

Transport

- Combination of all: 34%
- Security team: 26%
- OT/Engineering team: 22%

Water

- Security team: 46%
- IT team: 24%
- Combination of all: 18%

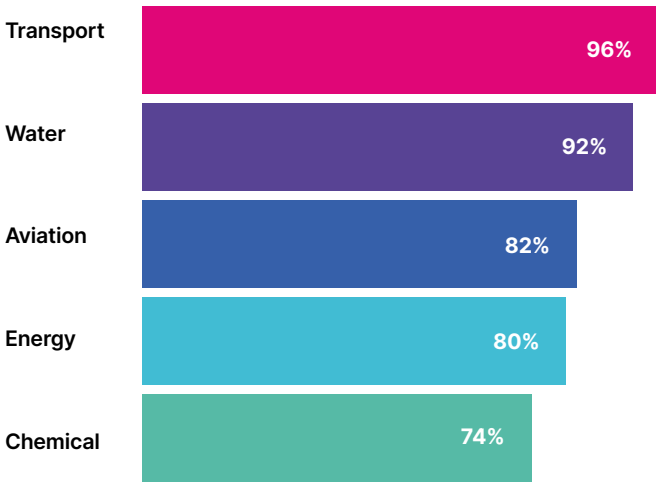
Security teams are burning out

With a high volume of cyber attacks, an increase in cyber security compliance, greater interconnectivity of systems, new emerging technology and the need to support more cyber assurance activities, security teams are being pulled in multiple directions. This is reflected in the fact that an increase in duties and responsibilities was listed as the second biggest challenge facing cyber security teams (23%).

Not surprisingly, 85% of decision-makers agree that they have felt an increasing pressure to improve cyber security controls for the OT/ICS environment in the last 12 months (aside from supporting remote working in the current circumstances), with transport and water feeling the pressure the most.

This is also reflected in the fact that burnout of employees was listed as a top-three challenge facing organisations today, stated by nearly one fifth (19%) or organisations.

Percentage of respondents that agree with the following statement: In the last 12 months, I have felt an increasing pressure to improve cyber security controls for the OT/ICS environment (aside from supporting remote working in the current circumstances)



These pressures are impacting cyber security teams in a number of concerning ways. Of those that said they were under increasing pressure:

- Nearly half (47%) say they are suffering from increased stress which is unsustainable and will result in burnout (again) if not addressed
- 41% have experienced burnout which has resulted with absence from the business
- Over a third (38%) have experienced or are experiencing anxiety
- Nearly a third (32%) have started looking for another job
- Over a quarter (28%) have resigned

The figures paint a very worrying picture. With a skills shortage expected and existing teams impacted significantly by stress, burnout, anxiety, absence and attrition, action clearly needs to be taken.

> ***Not only does more need to be done to attract skilled workers to the industry, more needs to be done to support existing workers and new workers joining the industry***

Clearly more needs to be done to alleviate the pressure on CISOs and their teams. If more investment and resources aren't put into cyber security, organisations' security and the security of the CNI could suffer significantly. Not only does more need to be done to attract skilled workers to the industry, more needs to be done to support existing workers and new workers joining the industry.

Understanding the NIS Directive

The directive on security of network and information systems (NIS Directive) is legislation passed by European Union. The NIS sets a range of network and information security requirements which apply to operators of essential services and digital service providers (DSPs).

The NIS Directive is certainly a step in the right direction and has done a lot to improve cyber security in the sector, however there is still clearly a long way to go. The survey reveals there is uncertainty around NIS alignment within the UK CNI sector.

While it's encouraging that 74% of organisations say they fully understand the requirements of the NIS directive, nearly a fifth (17%) say they don't and 9% are unsure.

Level of understanding of the NIS Directive by sector

	Fully understand	Don't fully understand	Unsure
Energy	78.00%	14.00%	8.00%
Chemical	70.00%	24.00%	6.00%
Aviation	78.00%	14.00%	8.00%
Transport	68.00%	16.00%	16.00%
Water	74.00%	16.00%	10.00%

While following the requirements set out by the NIS Directive is a positive move for any organisation, it can be easy to be caught off guard by expecting to sail through the requirements to pass the regulation. It's encouraging that 70% of organisations say they were 'very prepared' or 'prepared' for the NIS assessments, however, more than a fifth (21%) were neutral and 6% were unprepared.

The extent to which each sector was prepared for the NIS Regulation:

	Aviation	Chemicals	Energy	Transport	Water
Very prepared	40%	22%	26%	32%	30%
Prepared	34%	40%	42%	38%	48%
Neutral	18%	20%	26%	26%	16%
Unprepared	8%	10%	4%	4%	4%
Very unprepared	0%	2%	0%	0%	2%
My organisation didn't have an NIS assessment	0%	4%	2%	0%	0%
Not sure	0%	2%	0%	0%	0%

Meeting NIS Indicators of Good Practice

Of the respondents who said their organisation had been through an NIS assessment, only 22% said they met all the Indicators of Good Practice (IGPs) they aimed to meet. A quarter (25%) said their organisation didn't aim to meet an IGP but will work towards meeting the IGPs that are sensible for their environment and will look for alternatives ways to meet those that would be unsuitable.

Encouragingly, 23% are working towards meeting all the 'Achieved' IGPs. Meanwhile, 21% didn't aim to meet an IGP as they feel they don't work for their environment and have their own criteria meeting the CAF outcomes.

Success by sector in meeting all target IGPs

	My organisation aimed to meet Achieved indicator of good Practice (IGP) in the NIS Cyber Assessment Framework and we have met every 'Achieved' IGP
Energy	18.37%
Chemical	20.83%
Aviation	16.00%
Transport	30.00%
Water	26.00%

It's clear that CNI organisations generally understand the NIS Regulation but there is a lack of understanding and failure to prepare is also evident. It's crucial that organisations put the time and resource in to understand the Directive and ensure they're thoroughly prepared but this can be difficult.

Working with a third-party that can provide expertise and guidance is one way organisations can be better prepared for the assessment and meet all of their IGPs.

Looking ahead

When asked about the next 12 months, the biggest areas of focus respondents identified were: introducing new methods of security testing (28%), investing in cyber security technology (28%) and more regular patching and updates (27%). While it's good that more organisations will be engaging in these activities, these are activities that every organisation should already be doing on a regular basis.

The top three focus areas per sector for the next 12 months

Aviation

- Introducing new methods of security testing: 38%
- Increasing frequency of security testing: 38%
- Implementation of greater physical security controls: 32%

Chemicals

- More regular patching and updates: 38%
- Updating ageing infrastructure: 32%
- Increasing frequency of security testing: 30%

Energy

- Introducing new methods of security testing: 34%
- Increased threat analysis: 32%
- Improved employee education 32%

Transport

- Updating ageing infrastructure: 38%
- Investing in cyber security technology: 34%
- More regular patching and updates: 28%

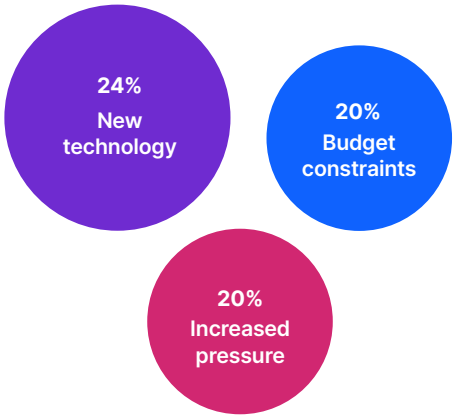
Water

- Improving identity and access management: 34%
- Increased threat analysis: 32%
- Improved security monitoring and detection: 30%

The biggest challenges facing cyber security teams by 2025

As anyone in business knows, 12-months can go by in the blink of any eye. Therefore, it's important to look ever further ahead and understand the challenges cyber security teams expect to come up against in the next five years. The biggest challenges cyber security teams expect to face by 2025 are understanding new technology (24%), budget constraints (20%) and increased pressure to prevent against cyber attacks (20%). The perceived challenges by 2025 vary by organisations in each sector.

Top three threats that cyber security teams expect to face by 2025



The top three challenges facing cyber security teams by 2025

Aviation

- Understanding new technology: 28%
- Increase in connected devices: 24%
- Lack of knowledge/ skills: 24%

Chemicals

- Understanding new technology: 26%
- Budget constraints: 24%
- Increased pressure to prevent cyber attacks: 24%

Energy

- Understanding regulation: 26%
- Lack of support from C-level/senior management: 26%
- Budget constraints: 24%

Transport

- Burnout of employees: 32%
- Keeping up-to-date with changes in the cyber security industry: 28%
- Increased pressure to prevent against cyber attacks: 26%

Water

- Budget constraints: 26%
- Increase in duties and responsibilities: 24%
- Increased pressure to prevent against cyber attacks: 22%

Conclusion

At the start of this report we posed a few important questions: how true are the perceived threats and risks to CNI? What are the biggest risks and challenges? Has regulation helped? And what does the future look like for the sector?

It's clear that decision-makers within CNI organisations believe there are indeed existing threats and risks that will grow in the coming years. There is are a broad range of challenges, from ageing OT systems and OT/ICS environments becoming increasingly accessible from external environments to the rise in cyber threats that has been spurred on by the pandemic. It's a worrying discovery that a number of organisations have reduced their cyber security spend in response to the pandemic when the increase in cyber risks is widely acknowledged.

The findings also suggest a lack of education around where the greatest cyber risks lie, made clear by the fact the supply chain is seen as the lowest area of risk, despite the NCSC naming this one of the biggest threats.

Perhaps most worrying is the evident lack of cyber security skills that decision-makers openly admit will become a growing problem in the next five years despite many also stating they have the right skills in place. With lack of knowledge/skills, increase in responsibilities and burnout identified as the top challenges facing security teams today, organisations will need to invest in improving cyber skills and resources.

A number of organisations have clearly had success with the NIS Regulation but many have not. Some organisations have struggled to understand the Directive's requirements while others have found themselves unable to prepare for it properly. Some organisations simply don't see the value. In all cases it appears the UK CNI sector could benefit from more education and guidance around the NIS, its benefits and how to prepare to successfully meet IGPs.

The key takeaway from these findings is that UK CNI organisations need more support, guidance, skills and expertise. So what steps should the industry take in response? Certainly, additional work needs to be done on cyber security development in the sector which should involve a closer focus on apprenticeships. Improving education will also be important, with additional CNI focused cyber security modules in degrees, along with more OT focused cyber security courses. Furthermore, where organisations are facing these struggles internally, external assistance could be the answer.

A partner versed in cyber security best practice will be able to identify threats and vulnerabilities, provide independent advice and recommend remediation plans tailored to the organisation and its unique requirements. The right partner will also be able to provide specialist cyber security skills to plug resource and knowledge gaps that are set to become a growing problem. One thing that is clear: the safety and longevity of CNI organisations will be at risk without urgent and vital improvements to their cyber resilience.

Bridewell
CONSULTING
Above. Beyond. Always

ABOUT BRIDEWELL CONSULTING

Bridewell Consulting is a cyber security services company providing global, 24×7 managed detection and response services and cyber security consultancy.

With extensive experience in delivering large-scale transformational projects in highly regulated environments, we enable organisations to drive strategic change securely, providing a full breadth of end-to-end cyber security services.

www.bridewellconsulting.com