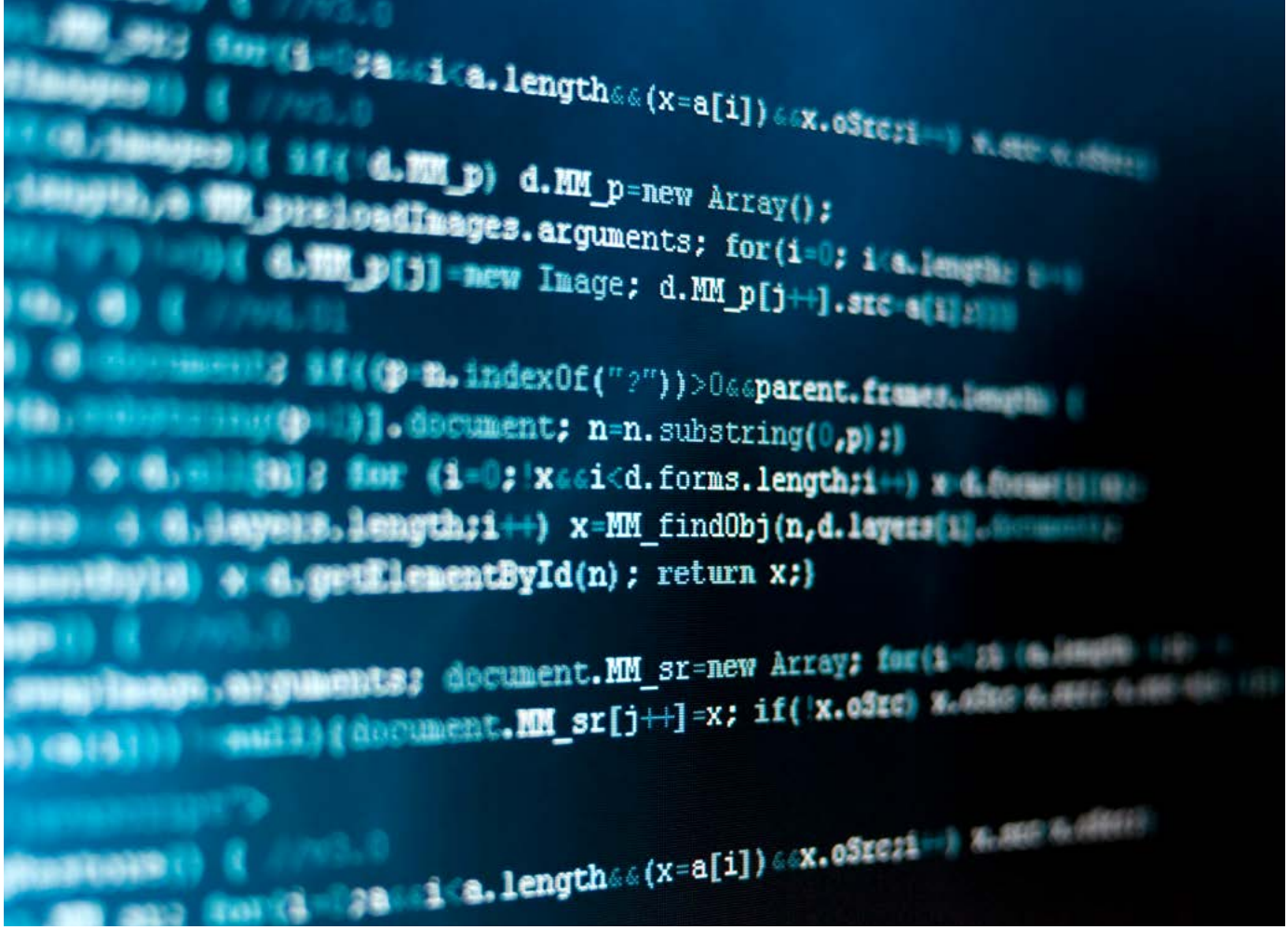
Securing success for your business

Digitalisation, IT/OT convergence and the growing cyber security challenge
siemens.co.uk/transform

SIEMENS



1. Cyber security post-pandemic

The pandemic highlighted the significance of precautions taken by both national and business infrastructure against the growing threats to their cyber security. As Ashling Cunningham, CIO at Irish Water, points out: "COVID 19... has shone a light on successes where the investments we had made really came good and ensured continuity across the business, customers, partners, supply chain and cyber environment."

2022 Government survey statistics show that in the last 12 months, 39% of UK businesses identified a cyberattack, a level consistent with previous surveys. However, the study also found that "enhanced cyber security leads to higher identification of attacks, suggesting that less cyber-mature organisations in this space may be underreporting.[i]"

The financial impact of attacks has risen during the pandemic. The Hiscox 2022 Cyber Readiness Report[ii] shows the median cost of cyber attacks for UK-based businesses has doubled in the past year. The report says the rising number of firms reporting incidents, and their increased severity, is a cause for concern, but also highlights that businesses are applying greater 'vigour' in their response to an attack.

Siemens held its inaugural Transform event in 2022, bringing together over two thousand British and Irish industry leaders. As well as experiencing the latest technology at the vast exhibition in Manchester Central, attendees exchanged their transformation experiences – covering digitalisation, sustainability and business resilience. This paper reflects the views and experiences of thought leaders shared during the event. As we now look to 2024 and beyond, the views of these forward-thinking experts provide the basis for this paper.

2. Digitalisation drives cyber security need

Manufacturing is a sector particularly vulnerable to cyber attacks. Brian Holliday, Managing Director of Siemens Digital Industries, UK&I comments: "It is critical to get the cyber basics right – right from the start – at a time when the manufacturing sector has become the number one sector under threat." A recent study by IBM[iii] has revealed that "for the first time in five years, manufacturing outpaced finance and insurance in the number of cyber attacks levied against these industries, extending global supply chain woes. Manufacturers have a low tolerance for downtime, and ransomware actors are capitalising on operational stressors exacerbated by the pandemic."

In the manufacturing sector, very specific cyber issues are preying on the minds of business managers. A cornerstone of digital transformation in manufacturing is the convergence of Information Technology (IT) systems and Operating Technology (OT) systems[iv]. Yet this very convergence opens the door to new cyber threats. The UK's National Cyber Security Centre notes that: "many businesses strive for improved OT process efficiency and reliability for their customers, which often results in increased connectivity to enterprise technologies and the Internet. This convergence has the potential to increase system vulnerabilities, but can be addressed by adopting sound risk management principles, which are the same regardless of the underlying system type."

"OT is defined as technology that interfaces with the physical world and includes Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS)."

National Cyber Security Centre

3. A holistic approach

In short, it is increasingly urgent for manufacturers large and small to address cyber security issues and challenges right from the start of their digital transformation journeys.

Stephen Phipson, CEO of UK Manufacturers' Association MakeUK corroborates the importance of the holistic approach, saying[v]: "More and more companies are at risk of attack and manufacturers urgently need to take steps to protect themselves against this burgeoning threat.

> " Businesses often don't realise the potentially devastating effects of a cyber attack on their business until it's too late,"
>
> **Katie Gallagher, co-founder of North West Cyber Resilience Centre.**

Failing to get this right could cost the UK economy billions of pounds, put thousands of jobs at risk and delay the supply of essential equipment to key public services and major national infrastructure projects."

Research conducted by MakeUK before the pandemic[vi] found that while 91% of businesses surveyed say they are investing in digital technologies in readiness for the 4th Industrial Revolution, 35% consider that cyber vulnerability is inhibiting them from doing so fully.

This suggests that opportunities are being missed and some businesses risk falling behind in the race to digitise.

A cyber attack in one business also has huge implications to others in a supply chain. One study found that nearly a third (30%) of manufacturers are experiencing disruption to trade through successful cyber attacks, with 28% also suffering disruption to supply chains.

The same research also noted that 60% of employees don't understand the cybersecurity implications of poor password hygiene. 24% also admit that they lack the skills to deal with cyber attacks.[vii]

4. Cyber security support for SMEs

Detective Superintendent Neil Jones of the North West Cyber Resilience Centre (NWCRC) points out the acute need for SMEs to have access to the means to protect themselves better - as the cyber threat mounts as a result of IT/OT convergence and cloud-based operational technology. He identifies five key areas for SMEs to prepare themselves. These are the same five areas of affordable, professional cyber security services which the Police-funded, not-for-profit NWCRC is bringing to smaller businesses in the region.

1. Security Awareness Training

2. Simulated Phishing Exercises

3. Network Vulnerability Assessment

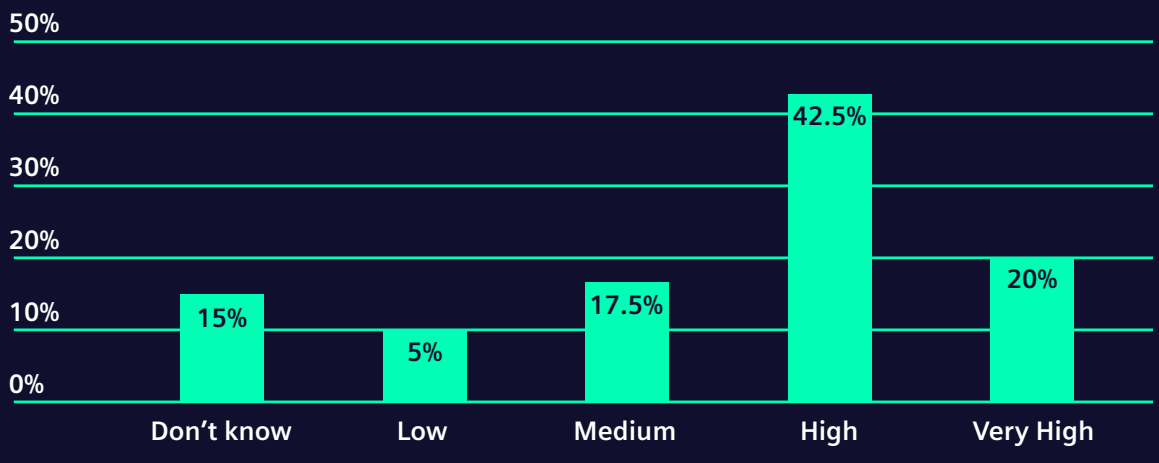
4. Website Vulnerability Assessment

5. Digital Footprint Assessment

Neil Jones notes that: "Any type of cyber attack can affect a business's ability to run its own operations and can easily spell the end of a business. There are numerous ways that business owners can protect themselves from this attack and train their employees to be aware of the multiple ways criminals can target businesses. Every single company should run regular cyber health checks as a standard procedure – much like having an emergency plan for fire – and ensure their employees have proper training."[viii]

So where is British and Irish industry at the moment? Bearing in mind the government's recommended emergency and resilience methodology[ix] of 'prepare', 'respond' and 'recover', a representative from the National Cyber Security Centre considers levels of preparation in the manufacturing sector are still mainly at the 'prepare' stage. Nevertheless, he notes that advisory literature is widely available[x], especially for smaller manufacturers who do not have in-house experts. This includes guidance[xi] from the industry via government initiative Made Smarter. Yet widespread implementation still has some distance to go for UK and Irish business.

How strongly would you rate your organisation's ability to detect and respond to a cyber attack?



Respondents at Cyber Security Challenge session, Siemens Transform 2022

5. Digitalisation, supply chain, and emerging vulnerabilities

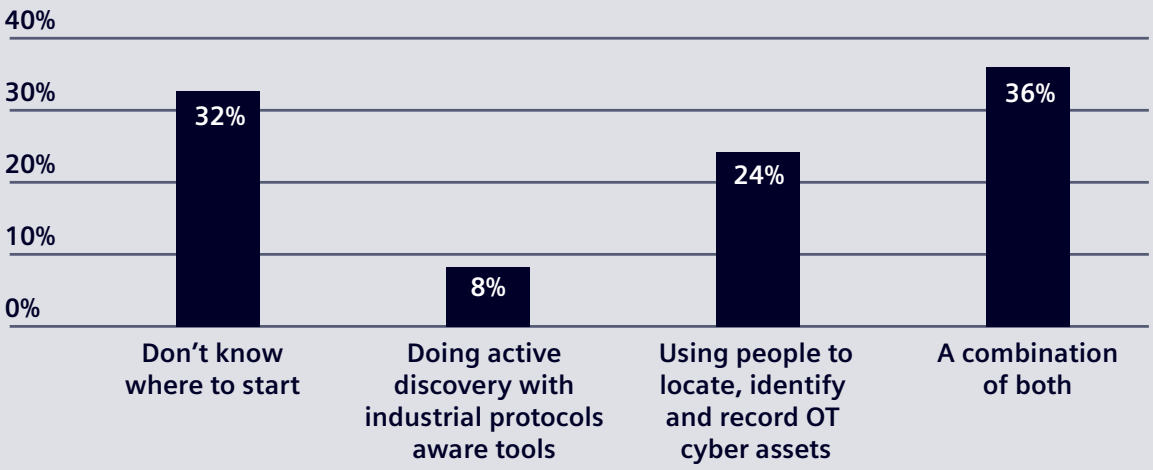
Digitalisation also brings a greater need to introduce and ensure cyber security maturity up and down the supply chain – embracing larger and smaller players. The UK Government's 2022 Cyber Security Incentives and Regulation Review comments: "as supply chains become increasingly interconnected, vulnerabilities in suppliers' products and services correspondingly become more attractive targets for attackers seeking to gain access to organisations. Recent high-profile attacks... demonstrate how seemingly small players in an organisation's supply chain can introduce disproportionately high levels of cyber risk into the wider economy."

Yet action needs to speed up. According to the latest Government analysis[xii], only 13% of businesses assess the risks posed by their immediate suppliers, with organisations saying that cyber security was not an important factor in the procurement process.

Expert discussions[xiii] have focused on two key areas of support to improve cyber security standards in manufacturing companies. They mainly focus on the introduction of mandatory training across the organisation[xiv], with better understanding of IEC 62443[xv] coming in for special mention. More broadly, training is seen as essential for all employees to gain a better understanding of how their day-to-day behaviours can either secure or open potential cyber-breaches.[xvi]

The ISA/IEC 62443 series of standards define requirements and processes for implementing and maintaining secure industrial automation and control systems (IACS). They provide a thorough and systematic set of cyber security recommendations. They're used to define the technical security measures and life cycle management of industrial communication networks against cybersecurity threats and attacks.

What is your approach for OT Cyber Assets Discovery?



Respondents at Cyber Security Challenge session, Siemens Transform 2022

Where digitalisation has created increased connectivity between OT and IT systems, the critical first stage is to analyse where these assets and their vulnerabilities might lie.
An expert panel of practitioners, hosted by Siemens, revealed their progress and techniques for identifying OT cyber assets (see graph).
The findings are positive, in that two thirds were actively doing so. However, there is clearly room for progress in the use of discovery software tools to enhance manual discovery processes. Greater sharing of implementation experience is widely tipped to help.

Indeed, in addition to OT asset discovery, there are wider calls for more sharing of positive experience around the use and implementation of widely available cyber security software applications.

Paul Hingley, Product Solution & Security Officer at Siemens, points out that: "Most of our customers are specifically looking for a holistic strategic approach to cyber security, in a partnership atmosphere, where we bring our shared knowledge of many organisations' experiences to optimise protection from the design stage onwards to final commissioning." Collaboration and sharing across industry is a frequent recommendation from global analysts. As KPMG notes: "To come up to speed more quickly, cyber leaders may want to reach out to others with relevant expertise - for example, vendors and partners who can share best practices."[xvii]

Working with expert partners – like Siemens – can help to strengthen companies' resources against potential vulnerabilities or attacks across processes. It is only through these increased sharing and collaboration efforts that businesses and sectors can stay up to date with the latest information and tools for security, and leverage these to the benefit of their operations.

Key Takeaways

- Digitalisation of the manufacturing sector is creating new cyber security threats and vulnerabilities through increased connectivity between IT systems and production-based OT systems
- This has accelerated the need for increased attention to cyber security measures, as recommended by industry associations and Government alike
- SMEs are the most exposed to cyber attacks, with lower awareness of the threat Landscape, fewer resources internally to address the issue and a reluctance to invest in cyber security in today's volatile markets
- Various regional and national initiatives have been put in place to help SMEs implement at least the basics of cyber security, at an affordable cost
- Connectivity throughout the manufacturing supply chain is making the vulnerability of small players a compelling issue for larger manufacturers
- In order to accelerate cyber security improvement across industry, there is a strong call for greater sharing and collaboration – between companies and between sectors – to communicate best practice about the successful implementation of cyber security software and solutions

References

i https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022
ii https://www.hiscox.co.uk/cyberreadiness
iii https://www.ibm.com/security/data-breach/threat-intelligence/
iv https://www.mckinsey.com/business-functions/operations/our-insights/converge-it-and-ot-to-turbocharge-business-operations-scaling-power
v https://www.makeuk.org/insights/reports/cyber-security-for-manufacturing
vi https://www.makeuk.org/-/media/eef/files/reports/industry-reports/cyber-report-2018.pdf
vii https://www.controlsdrivesautomation.com/IndustryUpdate
viii https://www.thebusinessdesk.com/northwest/news/2097188-north-west-business-briefs-together-north-west-cyber-resilience-centre-scholes-gym-electech-innovation-cluster-scale-to-sale
ix https://www.ncsc.gov.uk/collection/small-business-guidance--response-and-recovery
x ibid
xi https://www.madesmarter.uk/resources/publication-cyber-security-advice-for-business/
xii https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022
xiii Such as the Cyber Security Challenge session, Siemens Transform 2022
xiv https://www.itpro.co.uk/security/cyber-attacks/368824/most-business-leaders-only-prioritise-cyber-security-after-a-major-breach
xv https://industrialcyber.co/essential-guides/the-essential-guide-to-the-iec-62443-industrial-cybersecurity-standards/
xvi https://www.pwc.co.uk/issues/cyber-security-services/insights/five-key-employee-security-behaviours-that-can-reduce-cyber-risk.html
xvii https://www.mckinsey.com/~/media/McKinsey/McKinsey%20Solutions/Cyber%20Solutions/Perspectives%20on%20transforming%20cybersecurity/Transforming%20cybersecurity_March2019.ashx