
Executive Summary

December 2023

# Cyber4AM - Cyber Security for Advanced Manufacturing

**Introduction:**

Industry 4.0 has revolutionized manufacturing through digitization and connectivity, leading to a cyber-physical system. This increasing connectedness of the manufacturing environment to both customers and suppliers, brings new, inherent cyber security risks for manufacturing companies, in particular small and medium-sized enterprises (SMEs) and their supply chain, in both information technology (IT) and operational technology (OT) systems. Manufacturing SMEs need support with their cyber security maturity as they digitalise their factories. There is also a market opportunity for cyber security companies to better understand the potential vulnerabilities and needs of the manufacturing sector as it progresses towards Industry 4.0.

Cyber Security for Advanced Manufacturing (Cyber4AM) is an all-island, cross-cluster project run by Cyber Ireland and NI Cyber, funded by InterTradeIreland Synergy Programme. The opportunity exists to connect and leverage two of Ireland's strong industry sectors – manufacturing and cyber security – on an all-island basis. The project aims to:

1. Support the digitalisation and cyber security preparedness of Irish and Northern Irish Manufacturing SMEs.
2. Create business opportunities for Irish and Northern Irish cyber security companies in the Advanced Manufacturing sector.

This summary report provides an overview of the outputs of the Cyber4AM project and makes recommendations for further work.

**Project Outputs:**

- No. 20 Manufacturing SMEs cyber security maturity and needs were assessed (demand side).
- Identification of the cybersecurity solutions from Irish and Northern Irish companies, as well as education and training (Supply side).
- No. 10 cyber security companies' solutions and market capabilities assessed for advanced manufacturing.
- Report on the impact of industry 4.0 on cybersecurity in the manufacturing sector, including regulatory implications, challenges, attack methods.
- A project workshop event was held at the ISA Ireland OT Cybersecurity Conference (November 2023) to present and discuss the report findings and introduce manufacturing and cyber security companies.

**Global cyber security outlook:**

Cyber security attacks and threats are increasing globally. A divide has now emerged between cyber-resilient organisations and those that are struggling, which is worsened by factors such as the threat landscape, geopolitical instability, macroeconomic trends, industry regulation and adoption of new technologies.

The manufacturing sector has become one of the highest targeted sectors for cyber-attacks, with finance and the public sector. Across all sectors, SMEs are more vulnerable to cyber-attacks than large companies, and the impact of a cyber incident can be more detrimental to an SME – from a data breach, disruption to operations, financial costs and reputational damage. In addition to the business impact, cyber security breaches have the potential to cause harm to citizens and society, for example in utilities, food processing, pharmaceuticals and healthcare devices.

Amidst this, the cybersecurity economy grew exponentially faster than the overall global economy in 2022, and outpaced growth in the tech sector. The cyber security market globally is estimated to be worth $250 billion with a 15% growth rate.

**All-Island Cybersecurity Sector:**

Ireland and Northern Ireland have become a global hub for cyber security, many of the leading cyber security MNCs have operations here. There are almost 500 companies with over 7,000 employees in the sector in Ireland and 125 companies with over 2,700 employing in Northern Ireland.

**All-Island Manufacturing Sector:**

Manufacturing is a key sector of the Irish and Northern Irish economies, across biopharmaceuticals, med-tech, electronics, food production and more. The manufacturing sector accounts for 35% of Ireland's gross domestic product (GDP), more than twice the EU average, and employs 260,000 people. Similarly in Northern Ireland, Manufacturing accounts for 15% of gross value added (GVA), and 11% of employment. SMEs are the backbone of the manufacturing sector on the island of Ireland, which are part of global supply chains, and are adopting digital transformation.

**Fundamentals of Advanced Manufacturing:**

Advanced Manufacturing encompasses: Industry 4.0, Smart Factories, Smart Industry, Advanced Manufacturing, or Industrial Internet of Things (IIoT). There are four main features to consider:

1. Vertical networking using Cyber Physical Systems (CPSs) to create flexible, autonomous factories.
2. Horizontal integration via the Internet of Things (IoT), enabling real-time communication and insights across the production process.
3. Engineering innovations supporting the entire value chain, utilizing data analytics for optimization.
4. Increased efficiency through new technologies such as robotics, autonomous systems, machine learning, laser machining and nanotechnology.

Operational Technology (OT) plays a pivotal role in industries like manufacturing, utilities, energy and healthcare. OT encompasses the hardware and software systems that monitor and control physical processes, such as industrial machinery and infrastructure. OT deals with physical systems while, IT deals with digital systems.

**Cybersecurity Risks in Industry 4.0:**

The stages of Digitization, Visualization, and Digital Transformation in advanced manufacturing pose specific risks, such as:

- **Increased Attack Surface:** Interconnected devices create potential vulnerabilities, expanding the attack surface for cybercriminals.
- **Data Privacy Concerns:** Large data collection raises privacy issues and compliance challenges like GDPR, risking unauthorized access and breaches.
- **Supply Chain Vulnerabilities:** Interconnected supply chains can suffer from breaches in any segment, impacting the entire process due to varying cybersecurity levels among partners.
- **Lack of Standardization:** Inconsistent security protocols across devices and systems lead to security gaps and vulnerabilities.

**Key Cybersecurity Challenges for The Manufacturing Sector[1]**

- Phishing Attacks - Phishing attacks are a major threat to this sector, as employees can be tricked into leaking valuable data, including intellectual property and customer information.
- Supply Chain Attacks - Third-party vendors pose a risk, as they are often targeted by malicious actors as a way to gain access to sensitive systems or data within the manufacturing organization.
- Intellectual Property Theft - Attackers may target manufacturing organizations to steal valuable trade secrets, product designs, or customer data, which can be sold or used to gain a competitive advantage.
- Industrial IoT Attacks - Operators in this sector deploy connected devices to monitor and control production processes. These devices can be vulnerable to attacks, particularly if they are not properly secured.
- Ransomware Attacks - In the manufacturing sector, time is money, and any delay in manufacturing can result in significant losses. For this reason, ransomware attacks are particularly effective.
- Equipment Sabotage - Some malicious actors attempt to damage or disable critical equipment within a manufacturing facility to cause significant disruption to production processes.

This highlights the key facets of advanced manufacturing and associated cybersecurity risks in Industry 4.0.

[1] https://nis2directive.eu/manufacturing/

**Regulatory and Standards Landscape:**

The European Union's (EU) expansion of the NIS2.0 Directive will provide legal measures to boost the overall level of cybersecurity in EU member states by expanding the scope of the cybersecurity rules to new sectors and entities. The NIS2 directive is anticipated to have a substantial impact on the manufacturing sector as it will mandate that manufacturing entities are recognized as "important" under the NIS2 directive, which will result in:

- **Supply Chain Security** - It will require manufacturers to prioritize supply chain security.
- **Risk Management -** Manufacturing entities will need to implement risk management processes that consider the ever-evolving threat landscape.
- **Working with IT Providers -** manufacturing organisations may need to work more closely with IT service providers, such as Managed Security Service Providers (MSSPs) and cloud service providers, which could result in changes to existing business models and processes.
- **Cost and Competitiveness -** As manufacturers may need to allocate more budget towards cybersecurity initiatives, this could affect their bottom line, competitiveness, and potentially result in industry consolidation.

The EU's Cyber Resilience Act will implement cybersecurity requirements for products with digital elements such as connected home cameras, fridges, TVs and toys to ensure they are safe before they are placed on the market. This will result in increased responsibility for companies developing or manufacturing digital products by obliging them to provide security support and software updates to address identified vulnerabilities for at least five years. By mandating security updates on a minimum products' lifetime of five years, the new law will have a positive impact on companies focused on sustainability, including service providers in the after-sales market.

Implementing cybersecurity frameworks and standards support an organisation to protect their critical infrastructure and sensitive data, such as NIST2 or ISO 27001. The IEC (International Electrotechnical Commission) 62443 standard specifically addresses cybersecurity in industrial automation and control systems aiming to prevent and mitigate cyber threats and vulnerabilities that could affect critical infrastructure, including manufacturing facilities, power plants and other industrial environments.

**Cyber Security Solutions for Advanced Manufacturing:**

The advanced manufacturing sector requires specific cyber security solutions to address their needs across IT and OT environments. The main cyber security solutions provided for advanced manufacturing companies across IT and OT are from international vendors. Irish and Northern Irish cyber security companies need to better tailor their cyber security solutions to the needs of advanced manufacturing companies. Companies with cyber security expertise in sectors such as IT, finance and healthcare, could potentially expand into advanced manufacturing and cyber-physical systems through increased understanding and training in the unique vulnerabilities and challenges.

**Education and Training:**

Cybersecurity training, including IT security and employee awareness, can mitigate cyber risks in manufacturing. Universities and colleges offer cybersecurity education but there is specific training for OT security in manufacturing.

# Cyber Risk Analysis.

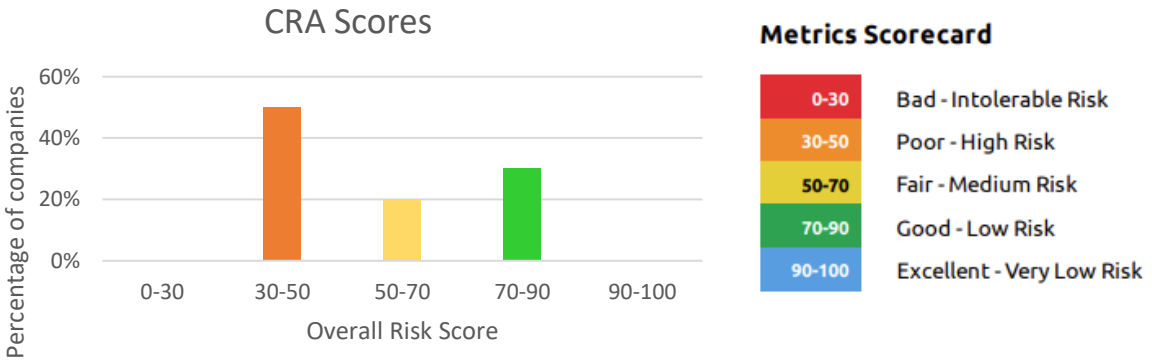
The Cyber4AM study involved 20 manufacturing SMEs, split between the Republic of Ireland (RoI) and Northern Ireland (NI), using Advanced Manufacturing techniques. This involved:

1. **Cyber Risk Assessment (CRA)** - was conducted to benchmark the participants' IT infrastructure and digital assets across the following domains: email, website, domain name server (DNS), internet protocols (IPs), networks, autonomous systems (AS).
2. **Semi-structured interviews** - were conducted to gather further detail and assess how ready each company is for a cyber-attack from an organisational development perspective, in particular OT cyber security risks.

**Key Findings of the CRA:**

The CRA unveiled varying risk levels among participating companies, emphasizing the need for greater understanding and proactive measures to address identified vulnerabilities and strengthen cybersecurity across different domains.

- **Overall Risk Assessment:** RoI companies averaged a medium risk score of 50, while NI companies scored lower at 40, signifying higher risk.
- **Domain:** A number of companies scored low (Bad, Poor or Fair) on their domain security.
- **Email:** Email security was strong, with no company having a poor or bad score.
- **Web:** Most companies in both RoI and NI have good website risk scores.
- **DNS:** Most companies in both RoI and NI have good DNS risk scores**.**
- **IP security:** has the lowest average score in both RoI and in NI.
- **Network Security:** every company had an excellent score for network risk.
- **Autonomous Systems (AS):** all the companies had an excellent or good score for AS risk.




**Key Findings of Cyber Readiness Interviews:**

- **Stage:** Most manufacturing SMEs believe they are at the early stages of Advanced Manufacturing - digitization.
- **Responsibility:** Companies have designated roles for overseeing cybersecurity, but only a few have dedicated cyber personnel.
- **Business Continuity Plans:** Around half of the companies have a business continuity plan, often influenced by insurance coverage requirements.
- **Cyber Risk Assessments:** Majority of companies have conducted CRAs previously but with varying coverage (IT only vs. IT and OT).
- **Cybersecurity Policy:** Half the manufacturing companies lack a cybersecurity policy.
- **Remote Work Security:** All companies with remote workers have considered the cyber security risks and have put in place protection for them, including multi-factor authentication log-ons and remote VPNs.
- **Cybersecurity Software:** 80% of companies have cybersecurity software in place, which covers some operational aspects of the business such as the shopfloor, engineering tools, production lines and supply chains.
- **Employee Awareness:** Employees are aware of cybersecurity but 90% of the companies believe their employees find cyber security language difficult or, somewhat difficult to understand.
- **Training:** 50% of the companies have no training in place to cover Operational Cyber Security**.**

- **Cyber Readiness:** Companies felt they were somewhat prepared for a cyber-attack. While no company believed they were "not ready", only 12% of companies believed they were completely prepared for an IT cyber-attack, and no company believed they were completely prepared for an OT cyber-attack.


***Figure: main cyber security challenges facing manufacturing SMEs.***

# Recommendations

**Awareness and Training:** The most common supports that companies believe would help them is targeted training and awareness programs for manufacturing SMEs. Additionally specialised training and courses suitable for industry to enhance companies' readiness for OT cyber-attacks is needed.

**Standards and Regulations:** Companies require support to implement cyber security standards and frameworks such as ISO27001 and IEC 6244. Additionally, awareness raising and support around pending regulations such as NIS2.0 and Cyber Resilience Acts is required.

**Comprehensive Cybersecurity Strategy:** Companies need to integrate cybersecurity more comprehensively into their business strategies as part of their digization plan.

**Cybersecurity and OEMs:** Original Equipment Manufacturers (OEM) need to improve the assessment and communication of cyber risk of their products with their manufacturing clients.

**Contingency planning:** While around half of the companies have a business continuity plan, it is interesting that this is often influenced by insurance coverage requirements. More work is needed to increase contingency planning, and to assess the scope and effectiveness of the planning.

**Cybersecurity Solutions:** Irish and Northern Irish cyber security companies need to better tailor their cyber security solutions and expertise to the needs of advanced manufacturing companies. This includes deeper understanding of the range of sub-sectors within advanced manufacturing, where their existing expertise can best be applied, and the capabilities they need to develop to address other sub-sectors.

**Cybersecurity Procurement:** It would be beneficial to understand more about how cyber security is procured across the range of sectors within advanced manufacturing. NI Cyber and Cyber Ireland could potentially collaborate with an advanced manufacturing industry cluster to explore this in-depth.