

Information Security Strategies for Industrial IoT environments:

A practical approach for Original Equipment Manufacturers



Radboud Universiteit

Author: **Stan van Duijnhoven** (stan.vanduijnhoven@ru.nl)

University Supervisors:

Prof. Güneş Acar (g.acar@cs.ru.nl)

Prof. Erik Poll (erik.poll@ru.nl)

IXON Internship Supervisor:

Dylan Eikelenboom, Security Officer (security@ixon.cloud)



This research internship thesis report and its accompanying material
was produced at IXON B.V. Beugen.

Submitted for the degree of Master's in Information Science
at Radboud University, Nijmegen.

June, 2023

Acknowledgements

I would like to express my deepest gratitude to my advisor Dylan Eikelenboom, whose guidance, support, and expertise were invaluable throughout the course of this research. Your insight and encouragement have been instrumental to the completion of this thesis.

I would also like to extend my sincere thanks to the University supervisors at Radboud University, especially Prof. Güneş Acar. Their guidance and support were also key to the success of this research.

Special thanks are extended to my colleagues at IXON. Their assistance, insightful comments, and thorough reviewing significantly helped in refining this research.

Abstract

This research project aims to investigate the current state of connected machine usage in industrial settings and provide guidelines and best practices for companies that are looking to make use of these devices in a secure and responsible manner. Through an extensive review of existing literature, case studies, and an expert interview, this thesis will provide a comprehensive set of recommendations for industrial companies seeking to leverage the benefits of connected devices while also mitigating the associated risks. This includes best practices for developing secure networks, methods for ensuring privacy compliance, approaches for ensuring data integrity, and strategies for minimizing operational costs associated with IoT implementation. Information security is important for industrial machine builders and equipment manufacturers as cyber attacks can lead to the loss of valuable intellectual property and sensitive information, production downtime, and even physical damage. This research aims to bridge the gap between the benefits and risks of cloud-based IoT device usage in industrial settings and provide a roadmap for companies to safely implement these technologies in their operations. In response to the challenges identified in this research, a Security handbook and Framework is developed and presented to assist industrial machine builders in navigating the complex world of cybersecurity.

Glossary of terms

- **Internet of Things (IoT):** A network of physical objects (devices, vehicles, buildings, etc.) that are embedded with electronics, software, sensors, and network connectivity, enabling them to collect and exchange data. IIoT is IoT in an industrial setting.
- **Industry 4.0:** The fourth industrial revolution, which consists of an ever-increasing level of connectivity for industrial machines to both factory software for planning and automated production, as well as cloud services for IoT purposes.
- **Cloud-based services:** Services that are hosted on the internet and accessed through a web browser or application.
- **Cyber attacks:** An attack on a computer system or network, usually with malicious intent.
- **Data breaches:** Unauthorized access to sensitive data.
- **Data integrity:** The accuracy and consistency of data over its entire life cycle.
- **Intellectual property:** A work or invention that is the result of creativity, such as a patent, trademark, or copyright.
- **Production downtime:** The time when a production process is stopped due to a malfunction or other issue.
- **Remote access:** The ability to access a computer or network from a remote location.
- **Scalability:** The ability of a system to handle an increased workload.
- **Security vulnerabilities:** Weaknesses in a computer system or network that can be exploited by attackers.
- **Third parties:** Entities that are not directly involved in a transaction or agreement, but may have an indirect interest in it.
- **Unauthorized access:** Access to a computer or network without permission.
- **Privacy compliance:** The process of ensuring that data is collected, stored, and used in accordance with applicable laws and regulations.
- **ISO27001** is a standard for information security management systems (ISMS). It provides a framework for managing sensitive information and maintaining its confidentiality, integrity, and availability.
- **ISO27017** is a code of practice for information security controls in the cloud. It provides additional security controls for cloud service providers and their customers.
- **ISO27701** is an extension to ISO27001, adding privacy information management controls. It covers the protection of personal data and assists organizations in complying with privacy regulations such as the General Data Protection Regulation (GDPR).

Table of Contents

1 Introduction	6
1.1 The importance of Information Security	7
2 Research Methodology	8
2.1 Research Questions	8
2.2 Research approach.	9
2.3 Literature study approach.	11
3 Literature study	12
3.1 Barriers to Effective Cybersecurity for Industrial Control Systems	13
3.2 Challenges in Deploying Cybersecurity Controls	14
3.3 Small to medium-sized organizations are especially vulnerable	14
3.4 Costs related to data breaches	15
3.5 Types of attacks	16
3.6 Roadmap to cybersecurity	17
3.7 NIST Cybersecurity Framework	18
3.8 Risks of SCADA systems	18
4 Subject Matter Expert interview	19
5 Research results	20
6 Conclusion	22
7 Practical implementation guide	23
8 Bibliography	24
Appendix A: Subject Matter Expert Interview	25
A.1 Interview approach	25
A.2 Interview	25

1 Introduction

The rapid advancements in technology, particularly the development and implementation of the Internet of Things (IoT), have significantly transformed the way industrial companies conduct their operations. This transformation, known as Industry 4.0, involves increasing connectivity among industrial machines, factory software for planning and automated production, and cloud services for IoT purposes. With IoT integration, companies can enhance efficiency, automation, and data-driven decision-making, ultimately leading to improved productivity and profitability.

A crucial technology enabling Industry 4.0 is the use of cloud-based services for remote access, data storage, and analysis. These services facilitate remote monitoring and control of industrial machines, reducing operational costs associated with manual supervision and maintenance, while providing a secure platform for sensitive data storage. Moreover, cloud-based services enable scalability and flexibility in operations due to their on-demand nature, allowing companies to adapt quickly to changing market conditions.

Although cloud-based services and connected machines offer numerous benefits, such as enhanced security and privacy (Kramer & Butler, 2019; Tissir et al., 2021), they may also introduce new risks that must be addressed for safe use. These risks include security concerns related to unauthorized access or malicious attacks, which could result in data breaches or loss of control over connected systems. Additionally, privacy concerns may arise from potential unauthorized data collection or misuse by third parties or malicious actors.

This research project aims to investigate the current state of connected machine usage in industrial settings and provide guidelines and best practices for companies seeking to utilize these devices securely and responsibly. Through an extensive review of existing literature, case studies, and an expert interview, this thesis will offer a comprehensive set of recommendations for industrial companies looking to leverage the advantages of connected devices while mitigating the associated risks. These recommendations will encompass best practices for developing secure networks that protect against unauthorized access or malicious attacks; methods for ensuring privacy compliance; approaches for ensuring data integrity; and strategies for minimizing operational costs associated with IoT implementation. By doing so, companies will gain a better understanding of the potential benefits and risks of using cloud-based IoT devices and make informed decisions on implementing these technologies in their operations. Ultimately, this research project aims to bridge the gap between the benefits and risks of cloud-based IoT device usage in industrial settings and provide a roadmap for companies to safely implement these technologies in their operations.

1.1 The importance of Information Security

Information security is of paramount importance for businesses in today's digital age, and this is especially true for industrial machine builders and equipment manufacturers. Machine builders and industrial equipment manufacturers are at an increased risk of cyberattacks because their systems are often integrated with other systems and networks, which creates multiple entry points for attackers to exploit. Additionally, industrial equipment often has a long lifecycle and strict production requirements, meaning downtime is not acceptable. These systems may not or can not be updated as frequently as other types of technology, making them more likely to contain security vulnerabilities.

Cyberattacks can have severe consequences for industrial machine builders and equipment manufacturers. A successful attack can lead to the loss of valuable intellectual property and sensitive information, production downtime, and even physical damage to equipment or harm to personnel. This can result in significant financial losses for the company in the form of lost revenue and fines, as well as damage to its reputation. Furthermore, a cyberattack on an industrial system can also have a ripple effect, causing cascading failures that can disrupt critical infrastructure and services, affecting not just the affected company but also its customers and even the broader community in the case of an organization that provides essential services (Eilts, 2020, Bobbert, 2019).

Despite the increased risk of cyber attacks, research on cybersecurity readiness and resilience in businesses often does not specifically address machine builders and industrial equipment manufacturers. However, many of the findings and recommendations from this research can be extrapolated and applied to this industry. For example, businesses in general are often found to lack the resources and expertise to adequately protect themselves from cyber threats (IBM Threat Intelligence Index 2023). This is especially true for machine builders and industrial equipment manufacturers, who may not have dedicated information security teams or may not be able to afford expensive cybersecurity solutions. This has made the manufacturing industry the top-attacked industry worldwide.

To address these challenges, machine builders and industrial equipment manufacturers should consider following industry best practices by taking a holistic approach to cybersecurity. This means identifying and assessing the risks to their systems, implementing appropriate controls to mitigate those risks, and regularly testing and monitoring their systems to ensure that they remain secure. It also means educating employees about the importance of cybersecurity and providing them with the necessary training to use systems safely and to recognize and report suspicious activity.

2 Research methodology

2.1 Research questions

The goal of this internship report is to research all the factors machine builders have to face and to translate this into concrete actions, written in their language to improve their overall security strategy. The end goal is a training and security package that we can offer machine builders as a standardized package.

The main Research Question is defined as follows:

- ❖ **How can Machine Builders be empowered in creating effective Information Security strategies?**

Six sub-questions that help answer the main research question are defined as follows:

- RQ1. What are common Cyber threats that industrial businesses face?
- RQ2. What are the costs for companies related to Information Security in defense and damages?
- RQ3. How are companies currently positioned to defend against modern Information Security threats?
- RQ4. What gaps in Security knowledge can be identified in companies?
- RQ5. What Information Security preparedness aspects are most challenging to implement?
- RQ6. What priority should Machine Builder companies have in their Information Security approach?

2.2 Research approach

In order to determine what threats industrial businesses face and answer the research questions, a literature review in combination with an expert interview is conducted. The body of (meta) research on cyber threats in industrial organizations is considerable, even if it may not all be specific to the machine-building industry. We estimate that it can still be applicable to discern general trends.

Research approach for RQ1: What are common cyber threats that industrial businesses face?

- Literature review: An extensive review of relevant literature will be conducted to identify the most common cyber threats that industrial businesses face. This will include articles, reports, and studies on cyber threats specific to the industrial sector, as well as general cyber threats that are relevant to all businesses.
- Case studies: A series of case studies will be conducted to examine real-world examples of cyber attacks on industrial businesses. These case studies will provide insight into the types of cyber threats that industrial businesses face and the impact they have on the affected companies.
- Expert interview: An interview with an expert in the field of industrial cybersecurity, particularly with machine-building industry professionals and experts, will be conducted to gather their perspectives on the most common cyber threats facing industrial businesses.

Research approach for RQ2: What are the costs for companies related to information security in defense and damages?

- Literature review: A literature review will be conducted to identify existing studies and reports on the costs associated with information security for businesses, including both defense and damages.
- Case studies: A series of case studies will be conducted to examine the costs of information security for industrial businesses that have been affected by cyberattacks. These case studies will provide insight into the financial impact of cyber attacks on industrial businesses, including the costs of defense and damages.
- Expert interview: An interview with an expert in the field of industrial cybersecurity, particularly within the machine-building industry, will be conducted to gather their perspectives.

Research approach for RQ3: How are companies currently positioned to defend against modern information security threats?

- Literature review: A literature review will be conducted to identify existing frameworks and methods that are used to measure the preparedness and maturity of companies when it comes to defending against modern information security threats.
- Expert interview: An interview with an expert in the field of industrial cybersecurity, particularly within the machine-building industry, will be conducted to gather their perspectives.

Research approach for RQ4: What gaps in security knowledge can be identified in companies?

- Literature review: A literature review will be conducted to identify existing studies and reports on gaps in security knowledge in companies.
- Case studies: A series of case studies will be conducted to examine the gaps in security knowledge that industrial businesses have.
- Expert interview: An interview with an expert in the field of industrial cybersecurity, particularly within the machine-building industry, will be conducted to gather their perspectives.

Research approach for RQ5: What information security strategy aspects are most challenging to implement?

- Literature review: A literature review will be conducted to identify existing studies and reports on the most challenging aspects of information security preparedness to implement.
- Case studies: A series of case studies will be conducted to examine the most challenging aspects of information security preparedness for industrial businesses.
- Expert interview: An interview with an expert in the field of industrial cybersecurity, particularly within the machine-building industry, will be conducted to gather their perspectives.

Research approach for RQ6: What priority should machine builder companies have in their information security approach?

- Expert interview: An interview with an expert in the field of industrial cybersecurity, particularly within the machine-building industry, will be conducted to gather their perspectives.

2.3 Literature study approach.

In this section, we explore the current literature on the subject of information security preparedness for industrial organizations. This research is performed with the goal of helping to answer the Main research question of this thesis. The 6 research questions function as sub-questions that aim to answer different aspects of the MRQ. Based on the combined results of the sub-questions, an answer is given to the main research question.

To conduct this literature research, we make use of a variety of sources and resources such as:

- Google Scholar (scholar.google.com)
- JSTOR ([jstor.org](https://www.jstor.org))
- Radboud University (online) Library
- Internal documentation and material at IXON
- DuckDuckGo (duckduckgo.com)

- Google Search (google.com)
- Academic databases such as IEEE Xplore and ACM Digital Library
- Papers from international conferences and journals related to information security
- Government and non-government websites related to information security preparedness for industrial organizations

3 Literature study

The use of Internet of Things (IoT) technology in industrial settings has grown rapidly in recent years, providing new opportunities for increased efficiency, automation, and data-driven decision-making. However, with the growth of Industrial IoT (IIoT) technology, the risk of cyberattacks has also grown, making it crucial for industrial equipment manufacturers to implement effective strategies for information security. In order to do this, it is essential to have an accurate assessment of their current level of information security preparedness. Meta studies have shown that industrial control systems are often considered to be particularly vulnerable to cyberattacks due to their reliance on legacy systems and lack of cybersecurity measures and that industrial equipment manufacturers often lack the resources and expertise to effectively secure their ICS (Bobbert, 2019) .

Additionally, small and medium-sized industrial equipment manufacturers often lack the resources and expertise to effectively implement cybersecurity measures and are often unprepared for the aftermath of a cyber attack. Furthermore, these manufacturers may be more likely to rely on informal, ad-hoc approaches to cybersecurity due to a lack of perceived value. In order to address these challenges, it is important for industrial equipment manufacturers to focus on implementing security by design principles, security testing, and incident response planning. Additionally, they should be aware of the government resources and guidelines available to help them improve their cybersecurity readiness and resilience. Furthermore, they should have a clear understanding of the standards and complexity of the cybersecurity controls, and they should set priorities and allocate resources in order to deploy these controls. It is also essential that they have a governance structure and fund a cybersecurity program in order to ensure successful outcomes. Finally, they should be aware of the role of the board in managing cybersecurity risks Assessing Security Preparedness.

When it comes to assessing the security preparedness of machine building organizations, utilizing the right framework is essential. A framework should take into account elements such as risk assessment, policy development, security education and training, and security incident response. Furthermore, the framework should be tailored to meet the unique needs of the machine-building industry so that all areas of risk are adequately addressed. For this reason, it is important to audit and update the framework on a regular basis to ensure that it is up-to-date with the changing landscape of information security threats and vulnerabilities. The National Institute of Standards and Technology (2018) conducted a study that looked at the challenges facing small and medium-sized industrial equipment manufacturers in securing their products and networks in IIoT environments. The study found that these manufacturers often lack the resources and expertise to effectively implement cybersecurity measures and that they are often unprepared for the aftermath of a cyberattack. The study also found

that these manufacturers are often reluctant to invest in cybersecurity measures due to a lack of perceived value and that they may be more likely to rely on informal, ad-hoc approaches to cybersecurity. The authors recommend that small and medium-sized industrial equipment manufacturers should focus on implementing basic cybersecurity measures such as firewalls, antivirus software, and incident response planning, and also should be aware of the government resources and guidelines available to help them improve their cybersecurity readiness and resilience. In addition to implementing basic cybersecurity measures, industrial equipment manufacturers should also have a clear understanding of the regulations and standards for cybersecurity in their industry, as well as the resources and guidelines available to help them improve their cybersecurity readiness. As such, it is important for industrial equipment manufacturers to have a governance structure in place that ensures proper security controls.

3.1 Barriers to Effective Cybersecurity for Industrial Control Systems

To be able to make an accurate assessment of the barriers that machine builders face when implementing information security strategies, a framework that is grounded in scientific methodology and industry experience is necessary. Utilizing the right framework is essential for organizations to be able to accurately assess their preparedness levels and to determine on which fronts they can still improve. Such a framework should include elements such as risk assessment, policy development, security education and training, and security incident response. Furthermore, the framework should be tailored to the unique needs of the machine-building industry in order to ensure that all areas of risk are addressed. Ideally the framework is also regularly audited and updated to ensure that it stays up-to-date with the changing landscape of information security threats and vulnerabilities.

Barriers to effective cybersecurity for industrial control systems have been researched by Chen, et.al (2020) in the Journal of Cybersecurity in Industrial Control Systems, and Jain, et.al (2018) in the Journal of Manufacturing Systems. These studies found that industrial control systems are often considered to be particularly vulnerable to cyber attacks due to their reliance on legacy systems and lack of cybersecurity measures and that industrial equipment manufacturers often lack the resources and expertise to effectively secure their ICS. Moreover, these ICS often have outdated operating systems and software, which can make them more susceptible to attack. Furthermore, the complexity of ICS networks can make it difficult to identify vulnerabilities or malicious activity. Additionally, many organizations are unable to prioritize cybersecurity measures due to budget constraints or organizational culture. As such, it is important for organizations that rely on ICS networks to invest in robust security solutions and training programs for employees in order to ensure their systems remain safe and secure from potential threats.

3.2 Challenges in Deploying Cybersecurity Controls

Deploying cybersecurity controls for industrial control systems (ICS) is an important challenge for machine builders in the Industrial Internet of Things (IIoT) environment. Setting priorities and allocating resources is essential for the effective implementation of cybersecurity measures. There is a need to understand the standards and complexity of cybersecurity controls as well. Risk assessment methods for ICS also need to be evaluated and improved to ensure that they address all areas of risk.

In terms of risk assessment methods, there is a need for better methods that take into account the contextual environment, the available knowledge, and the unique needs of the machine-building industry. Improving the reliability of probabilistic data, evaluating and validating assessment results, and providing tool support are all important considerations. It is essential for industrial equipment manufacturers in IIoT environments to be aware of the importance of cybersecurity readiness and resilience and to implement effective strategies to prevent and respond to cyberattacks (Urquhart & McAuley, 2018). To achieve this, industrial equipment manufacturers should focus on implementing security by design principles, security testing, incident response planning, and keeping updated on the regulations and standards for cybersecurity in their industry. They should be aware of the government resources and guidelines available to help them improve their cybersecurity readiness and resilience. By doing so, industrial equipment manufacturers will be better prepared to face cyber threats and protect their customers from harm. By taking the initiative to strengthen their cybersecurity posture, industrial equipment manufacturers will be able to gain a competitive edge as well as increase their overall efficiency and profitability.

3.3 Small to medium-sized organizations are especially vulnerable

A research paper by Darrell Eilts (2020) looks into the issue of cybersecurity preparedness among small enterprises. Experts in the field were consulted to identify crucial cybersecurity preparedness activities and establish a Cybersecurity Preparedness-Risk Classification (CyPRisT). Findings indicated that small businesses with higher levels of cybersecurity readiness were less vulnerable to cyberattacks. The study highlights the disparities between small businesses and larger corporations in terms of cybersecurity. It discusses a framework for improving small businesses' cybersecurity, and how to assess their level of preparedness. Additionally, the paper shows the correlation between various measures of cybersecurity preparedness and their impact on outcomes. The research discovered that small business leaders often lack the necessary vigilance towards cybersecurity risks and are ill-equipped to tackle cyber threats. By being informed about common cyber threats and implementing strategic planning for cybersecurity preparedness, decision-makers can better align their risk perception with their actual cybersecurity posture, thereby increasing the likelihood of maintaining business continuity in the face of cyberattacks or data breaches.

3.4 Costs related to data breaches

The increasing frequency of data breaches has become a major concern for organizations, as the cost of these breaches continues to rise. A recent research study by Steve Mansfield-Devine from IBM titled "The Cost of a Data Breach Report (2022)," analyzed 550 organizations that suffered data breaches between March 2021 and March 2022. The study revealed that 83% of organizations have faced multiple breaches, with 60% resulting in increased prices passed on to customers. Additionally, 79% of critical infrastructure organizations have not implemented a zero trust architecture, making them more susceptible to attacks. The report highlights that 19% of breaches were caused by compromise at a business partner.

The study delves into the various security vulnerabilities faced by organizations, from the cloud to critical infrastructure, and provides insights into the impact of ransomware and destructive attacks.

The average cost of a data breach in 2022 was \$4.35 million, a 2.6% increase from the previous year. The costliest average breach was experienced by critical infrastructure organizations, totaling \$4.82 million. The study found that utilizing security AI and automation can help organizations save an average of \$3.05 million. The United States continued to be the costliest country for data breaches, with other countries in the top five including the Middle East, Canada, the United Kingdom, Germany, and Brazil. The cost of a data breach is divided into four categories: notification costs, lost business costs, post-breach response costs, and average costs. The average cost of a breach decreased from \$1.59 million in 2021 to \$1.42 million in 2022, a 10.7% decrease, primarily due to decreased business costs. The average time it took to identify and contain a breach decreased from 287 days in 2021 to 277 days in 2022, a decrease of 10 days, which was linked to lower breach costs. The study also analyzed the cost and frequency of data breaches in different regulatory environments and found that highly regulated industries tended to have higher costs and longer times for identifying and containing a breach. The most common initial attack vector was phishing, and the most expensive type of breach was compromised credentials. The report found that the three factors that led to the highest cost increase were security system complexity, cloud migration, and compliance failures. The relationship between data breach costs and security AI and automation was also explored in the study. Organizations with fully deployed security AI and automation were able to detect and contain breaches much more quickly, with an average time of 249 days. Risk quantification techniques were also found to have a significant impact on data breach costs, saving organizations an average of \$2.10 million. Organizations that prioritized risks, threats, and impacts based on risk quantification had an average breach cost of \$3.30 million, \$2.10 million less than those that did not use risk quantification.

The study also looked at the impact of zero trust on the average cost of a data breach. Organizations that consistently applied zero trust across all domains had an average breach cost of \$3.45 million, while those in midstage or early adoption had an average cost of \$3.96 million, \$1.51 million higher than mature organizations. The study found that organizations that did not pay ransom demands faced higher average costs for a ransomware breach, with the ransom cost excluded from the calculation.

3.5 Types of attacks

The breaches are generally divided into 10 initial attack types, also called vectors. These include accidental data loss, cloud misconfiguration, phishing, insider threats, and stolen or compromised credentials. The average time it takes to identify and contain breaches is based on their initial attack vector.

In 2022, the most common initial attack vectors were stolen or compromised credentials (19%), followed by phishing (16%), cloud misconfiguration (15%), and a vulnerability in third-party software (13%). The costliest initial attack vector in 2022 was phishing with an average cost of USD 4.91 million. The other expensive initial attack vectors included business email compromise (USD 4.89 million and 6% of breaches), a vulnerability in third-party software (USD 4.55 million), and compromised credentials (USD 4.50 million).

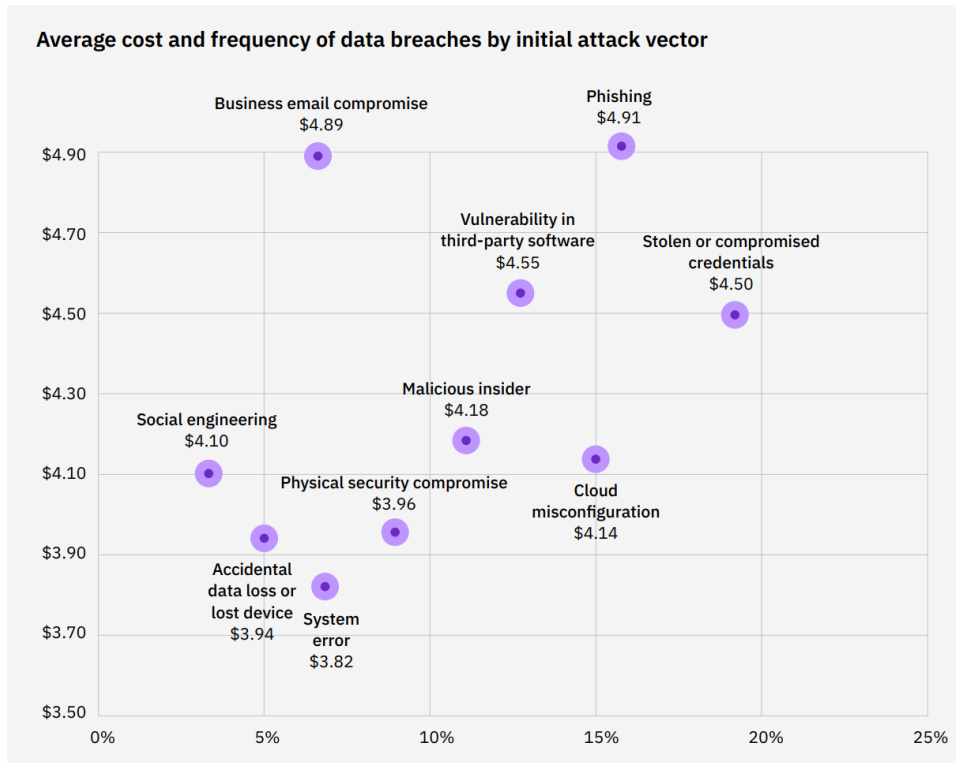


Figure 1: Average cost and frequency of a data breach in millions of USD

(taken from IBM Threat Index 2023, [5])

Attack vectors that had a longer mean time to identify and contain, such as phishing and business email compromise, were also among the most expensive types of breaches. Compromised credentials had the longest mean time to identify and contain a breach, at 327 days, which is 16.6% higher than the overall mean time to identify and contain a data breach. Business email compromise had the second-highest mean time to identify and contain (308 days) and was the second-costliest initial attack vector. Phishing had the third-highest mean time to identify and contain (295 days) and had the highest average cost of any initial attack vector (USD 4.91 million). Vulnerability in third-party software had the fourth-highest mean time to identify and contain a breach (284 days) and was above the overall average (277 days).

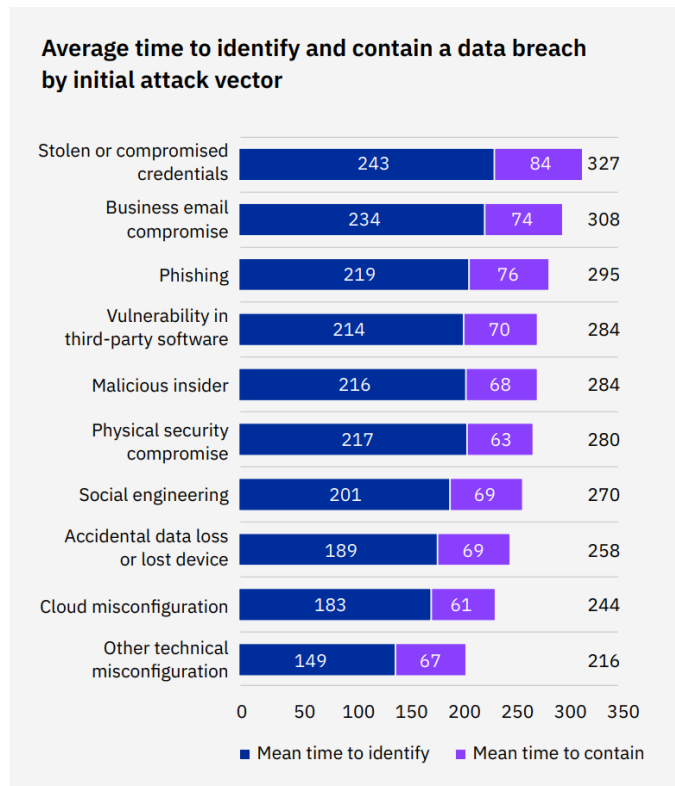


Figure 2: Average time in days to identify and contain a data breach

(taken from IBM Threat Index 2023, [5])

3.6 Roadmap to cybersecurity

The threat of cyberattacks is a growing concern not just for individuals but also for entire nations, their economies, and critical infrastructures. To address this challenge, a shift in approach to cybersecurity is necessary, including enhanced collaboration, government involvement, and a zero-trust security model (Kramer, 2019). These infrastructures must be prioritized and must be resilient in the face of cyberattacks. A strong partnership between the government and the private sector is crucial in achieving this goal. The current state of affairs, with nation-states possessing advanced cyber capabilities, highlights the need for greater government involvement. To establish a new cybersecurity model, a number of sector entities should be created to develop effective cybersecurity architectures, processes, and capabilities. The United States Department of Homeland Security has already set up a council that focuses on enhancing the resilience of the telecommunications, financial, and energy industries. To further bolster cybersecurity efforts, increased resources are necessary, with funding coming from public sources rather than companies, Kramer argues.

3.7 NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) has made a significant contribution to the field of cybersecurity with the development of the Cybersecurity Framework. This public-private collaboration is designed to help organizations manage their cybersecurity risk and includes five core functions: identity, protect, detect, respond, and recover. The framework can be used by those who are new to cybersecurity and is fully compatible with the original version. In 2018, NIST released the Cybersecurity Framework version 1.1, which was more adaptable to small businesses.

While there are many examples of risk management frameworks in the research literature, there have been few studies examining these frameworks in the context of small businesses, considering their limited ability to deal with the risk of cyberattacks. The growing adoption of the NIST Cybersecurity Framework among businesses (Tenable, 2016) highlights the need for empirical assessments of their cybersecurity posture, which can help to determine how well-prepared a business is to prevent and protect against cyber threats, as well as their ability to maintain business continuity during and after a cyber-attack. A crucial step in this process is the development of an instrument that can measure the level of cybersecurity preparedness.

3.8 Risks of SCADA systems

Industrial Control Systems (ICS), including SCADA (Supervisory control and data acquisition) systems, are widely used in various industries to control and monitor remote assets. Initially, ICS were primarily exposed to local threats due to the physical security of their components (Chen et al, 2015). However, the integration of ICS with IT networks has increased the risk of external cyberattacks. Protecting the availability and security of ICS is critical for safety, security, and profitability. To assess the risk, a mean failure cost (MFC) metric has been proposed, which quantifies the loss that each stakeholder may incur as a result of security violations or system breakdowns. SCADA systems are composed of various components that communicate with each other and are vulnerable to hardware, software, communication, and user authorization threats. To mitigate these risks, it is important to implement security and authentication protocols from the outset. A risk management cycle that includes risk framing, assessment, response, and monitoring can also be structured to manage the risk of SCADA systems.

4 Subject Matter Expert interview

The goal of this interview is to gain an understanding of how information security is applied in the machine building industry, learn where knowledge and expertise is lacking, and which systems and processes should be secured most urgently. The information gained will be used to help answer the research questions and build a foundation for the material that is aimed at supporting machine builders in their security efforts.

The transcript summary of this interview is attached as [Appendix A](#).

They were asked the following series of questions:

1. What are some of the biggest security headaches you see among machine building companies?
2. How do they handle the costs and financial impacts of information security measures and incidents?
3. What's the typical approach to defend against cyber threats and secure sensitive data?
4. Do you see any common trends or patterns when it comes to the preparedness and maturity of information security efforts among your customers?
5. What are the key knowledge and expertise gaps when it comes to information security in the machine building industry?
6. How do these companies usually feel about implementing comprehensive information security measures? Does it appear daunting or scary to them? Do they not have enough expertise in house to implement security measures and controls?
7. What kind of priority do you see machine building companies giving to information security in their overall strategy and decision making? For what reason?
8. Have you come across any interesting or surprising security incidents involving machine building companies?
9. How do these companies stay informed about the latest information security trends and developments?

5 Research results

Based on the review on the current scientific literature available, case studies and subject matter and an expert interview, the research questions composed in the research approach can be answered.

→ RQ1. What are common Cyber threats that industrial businesses face?

Common cyber threats that industrial businesses face include data breaches, unauthorized access, cyber attacks, and security vulnerabilities. Additionally, ex-employees that still have access rights after termination, and general cyber ignorance and inattention are established as threats. There is a general lack of understanding of security threats among machine-building companies. This especially results in an apparent lack of proper risk management, which includes estimating the likelihood of threats, focusing on the wrong risks, and inadequate measures to counter potential risks. These threats can lead to the loss of valuable intellectual property and sensitive information, production downtime, and even physical damage.

→ RQ2. What are the costs for companies related to Information Security in defense and damages?

It is apparent that there is a challenge of cost-benefit and risk analysis, suggesting that companies struggle to quantify the financial aspects of their security measures. It is clear that costs can stem from both implementing preventive measures and potential damages from security breaches, including financial losses, damage to the company's reputation, and potential legal repercussions. The costs for companies related to Information Security in defense and damages can be significant. Companies must invest in security measures to protect their data and systems from cyber attacks, as well as cover the costs associated with any data breaches or downtime that may occur.

→ RQ3. How are companies currently positioned to defend against modern Information Security threats?

Many machine-building companies are only starting to become security-minded and have a general lack of knowledge and preparedness when it comes to cybersecurity. with many overcomplicating things or lacking the necessary security knowledge. The preparedness varies significantly, with some companies even showing overreaction due to a lack of understanding. Formal and informal processes and adherence to standards such as the NIST Cybersecurity Framework, ISO27001, ISO27017, ISO27701 and IEC62443 could help companies evaluate and improve their security maturity.

→ RQ4. What gaps in Security knowledge can be identified in organizations?

The primary gap in security knowledge identified is risk assessment. Many companies struggle with estimating risks and likelihoods, which leads them to focus on the wrong areas that may not significantly impact security. Additionally, there's a significant gap in basic security practices, such as password management, access rights, and attention to security details.

To identify gaps in knowledge, a structural approach by organizations through an internal audit of their existing security measures and processes can be conducted. This helps to identify any areas where additional training or resources may be needed in order to ensure the security of their data and systems.

→ RQ5. What Information Security preparedness aspects are most challenging to implement?

Training and awareness-building can be particularly difficult due to the rapid fading of information and awareness. The technical aspects such as password management and access rights can also pose challenges. The fact that many see it as an obligatory measure rather than an integral part of their operations adds to the difficulty.

Additionally it is found that aspects related to privacy compliance cause difficulty, to ensure that they are compliant with applicable laws and regulations when it comes to the collection, storage, and use of data.

→ RQ6. What priority should Machine Builder companies have in their Information Security approach?

The highest priority for machine building companies should be fostering a security culture and securing management commitment. Every organization needs to start somewhere, even if that start is small, such as checking who has access to sensitive information. A risk-based approach should be adopted where the focus is on the threats that occur most often.

Additionally, if at all possible, they should ensure that their systems are regularly audited and updated to address any security vulnerabilities that may arise. Over time, companies should aim to improve and streamline their processes, with an emphasis on cutting unnecessary steps and ensuring that the security measures are effective. They should stay aware of developments in information security, either through government updates, RSS feeds, or third parties.

6 Conclusion

This thesis investigated common cyber threats faced by industrial businesses, the costs related to information security, companies' preparedness against modern threats, the gaps in security knowledge among businesses, the challenges faced in information security preparedness, and the priority that machine building companies should place in their information security approach. We found that industrial businesses face numerous threats, such as data breaches, unauthorized access, and ex-employees retaining access rights. There is an evident lack of understanding of security threats, which can result in improper risk management and inadequate measures to counter potential threats.

The costs of defense and damages associated with information security are significant. Companies often struggle with cost-benefit and risk analysis, suggesting a need for better financial quantification of security measures. Companies' positioning against modern threats is varied, but there is a general lack of preparedness and security knowledge, especially among machine-building companies. This lack of understanding often leads to overcomplication of security measures or an overreaction to threats. Nonetheless, adherence to international standards can aid in evaluating and improving security maturity.

Gaps in security knowledge are prevalent, particularly regarding risk assessment and basic security practices. Addressing these gaps requires a structural approach, including regular internal audits and identifying areas needing additional training or resources. The most challenging aspects of implementing information security preparedness are training and awareness-building. It's often seen as a mere obligatory measure rather than an integral part of operations. Technical aspects such as password management and access rights also pose challenges.

For machine-building companies, the primary priority in their information security approach should be building a security culture and securing management commitment. These companies should adopt a risk-based approach, focusing on the most prevalent threats and regularly auditing and updating their systems.

Overall, this thesis underscores the importance of a robust security culture within industrial businesses. It highlights the need for improved risk assessment, better cost-benefit analysis, and a stronger commitment to security from management. This commitment should include an understanding of security as an integral part of operations, not just an obligatory measure that only results in costs.

Future research could focus on developing effective training and awareness programs that address the knowledge gaps identified in this study. It could also explore the cost-benefit dynamics of implementing security measures in more detail, and how these dynamics influence companies' decisions and their overall approach to information security.

Despite the challenges, it is clear that there is a critical need for better information security in industrial businesses. By understanding the threats they face, the costs involved, and the necessary measures for defense, these businesses can better protect their assets, their employees, and their customers.

7 Practical implementation guide

In response to the challenges identified in this thesis, a Security handbook and Framework has been developed to assist industrial machine builders in navigating the complex world of cybersecurity. This guide is designed to be both accessible and approachable, allowing organizations to focus on control measures that align with their current level of cybersecurity maturity. The guide can be found on request to the author or attached to this document, and is titled:

“Building Cybersecurity for Industry 4.0: A Practical Handbook for OEMs”

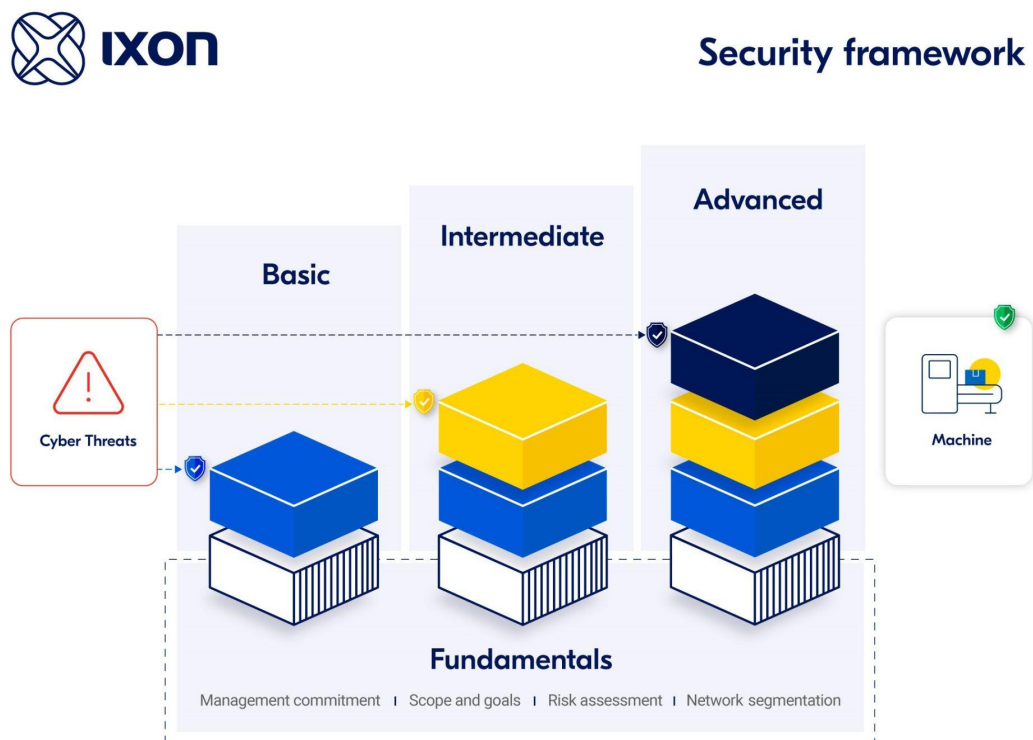


Figure 3: Security Framework from the security Handbook.

8 Bibliography

1. Auffret, J.-P., Snowdon, J. L., Stavrou, A., Katz, J. S., Kelley, D., Rahman, R. S., ... Warweg, P. (2017). Cybersecurity Leadership: Competencies, Governance, and Technologies for Industrial Control Systems. *Journal of Interconnection Networks*.
<https://www.worldscientific.com/doi/abs/10.1142/S0219265917400011>
2. Bobbert, Y. (2019). Cybersecurity readiness: An empirical study of effective cybersecurity practices for Industrial Control Systems. *Scientific Journal of Research & Reviews*, 2(3).
<https://doi.org/10.33552/sjrr.2019.02.000536>
3. Chen, Q., Abercrombie, R. K., & Sheldon, F. T. (2015). Risk Assessment For Industrial Control Systems Quantifying Availability Using Mean Failure Cost (MFC). *Journal of Artificial Intelligence and Soft Computing Research*, 5(3), 205–220.
<https://doi.org/10.1515/jaiscr-2015-0029>
4. Eilts, D. (2020). An Empirical Assessment of Cybersecurity Readiness and Resilience in Small Businesses (Doctoral dissertation, Nova Southeastern University). NSUWorks, College of Computing and Engineering. (1106). https://nsuworks.nova.edu/gscis_etd/1106
5. IBM Corporation. (2023). X-Force Threat Intelligence Index 2023.
<https://www.ibm.com/reports/threat-intelligence>
6. Kramer, F. D., & Butler, R. J. (2019). A roadmap to better cybersecurity. In *Cybersecurity, Changing the model* (pp. 5–20). Atlantic Council. <https://www.jstor.org/stable/resrep20932.5>
7. Mansfield-Devine, S. (2022). IBM: Cost of a Data Breach. *Network Security*, 2022(8).
[https://doi.org/10.12968/s1353-4858\(22\)70049-9](https://doi.org/10.12968/s1353-4858(22)70049-9)
8. Pool, J. H., & Venter, H. (2022). A Harmonized Information Security Taxonomy for Cyber Physical Systems. *Applied Sciences*, 12(16), 8080. <https://doi.org/10.3390/app12168080>
9. Tenable. (2016). Survey Report: Trends in Security Framework Adoption.
<https://www.tenable.com/whitepapers/trends-in-security-framework-adoption>
10. Tissir, N., El Kafhali, S., & Aboutabit, N. (2021). Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal. *Journal of Reliable Intelligent Environments*. <https://doi.org/10.1007/s40860-020-00115-0>
11. Urquhart, L., & McAuley, D. (2018). Avoiding the internet of insecure industrial things.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3083605

Appendix A: Subject Matter Expert Interview

A.1 Interview approach

The following questions were prepared to conduct an interview with a subject matter expert on the subject of industrial information system security:

1. What are some of the biggest security headaches you see among machine building companies?
2. How do they handle the costs and financial impacts of information security measures and incidents?
3. What's the typical approach to defend against cyber threats and secure sensitive data?
4. Do you see any common trends or patterns when it comes to the preparedness and maturity of information security efforts among your customers?
5. What are the key knowledge and expertise gaps when it comes to information security in the machine building industry?
6. How do these companies usually feel about implementing comprehensive information security measures? Does it appear daunting or scary to them? Do they not have enough expertise in house to implement security measures and controls?
7. What kind of priority do you see machine building companies giving to information security in their overall strategy and decision making? For what reason?
8. Have you come across any interesting or surprising security incidents involving machine building companies?
9. How do these companies stay informed about the latest information security trends and developments?

A.2 Interview

The following is an extensive summary of an interview held in March 2023 with the Security Officer of IXON, Dylan Eikelenboom.

Interviewer: What are some of the biggest security headaches you see among machine building companies?

Subject Matter Expert (SME): It varies per company. Usually for small and mid-sized businesses, the most common issue is a lack of knowledge. They know they should do something about security, but they don't know what to do or where to start. They ask uninformed questions about password requirements. It turns out they don't understand what it's all about, so they ask very generalized questions.

Companies that already have a security department often overcomplicate things. They don't allow cloud solutions out of principle. Sometimes, however, they do engage and ask for explanations or

certifications. They don't understand the risks well, so they overreact with tense responses. Their skepticism usually disappears after they have gained more security knowledge.

Risk management is very difficult and a significant problem. Cost-benefit and risk analysis are very challenging. This can be tackled by assembling a group of people from different departments to explain and estimate the risks from their own field. However, risk assessment still proves to be very difficult, even for experienced security people. It's nevertheless an important first step. You have goals that are threatened by risks. The risks are limited by taking measures.

Management commitment is the most important first step. After that, you can undergo training, which will help you better assess the risks. You just have to start somewhere. For example, by establishing a recovery plan. This can be as complicated as you want, with one scenario more difficult than the other. Just start with the things that occur most often. It's an iterative process where you just build on each other. Start small, even with informal things, and continuously improve. You can't get it right all at once.

Eventually, you can even market your security strategy. Sales and marketing may eventually use it, seeing the need for it. It's important to have an ambassador who keeps focusing on security. Starting is the most difficult part. Once everything is running a bit, it is easier to expand and improve. The first steps are harder than the last 1%.

Interviewer: What's the typical approach to defend against cyber threats and secure sensitive data?

SME: Many don't operate according to standards. It's just not ingrained yet, but it is expected to be in the future. Most organizations just start somewhere. In the last 1-2 years, they've become more security-minded. Standards are especially useful for those who are just starting. On passwords, training, and awareness is super important, but also difficult because this information fades over time. You must first have your processes in order. You need to develop the culture. Passwords are very important, so even an informal process is acceptable to start off.

For example, check who has access every month. Passwords, who has access? Use the principle of least privilege. No shared passwords. Be mindful of ex-employees. Ignorance or inattention is often the issue.

Interviewer: What are the key knowledge and expertise gaps when it comes to information security in the machine-building industry?

SME: Risk assessment. They can't make a good estimate of the risks. Especially the likelihood. They focus on the wrong things that don't have much effect.

Interviewer: How do these companies usually feel about implementing comprehensive information security measures? Does it appear daunting or scary to them? Do they not have enough expertise in-house to implement security measures and controls?

SME: It's often seen as an obligatory measure. There's a real lack of knowledge. The wrong people ask the questions. A security culture is important. You develop this mainly through emphasizing things from the top. Repetition is important. Security should come up every day in employees' work. They should think: "Oh yes, this is important for security, so that's why we do it."

Interviewer: Can you discuss any specific regulatory requirements or standards that machine-building companies need to comply with in regards to information security?

SME: Legislation will not be directed at machine builders so quickly. The government wants to prevent essential companies from running into problems. Factories will need to meet various requirements. They will relay things to machine builders. Ultimately, the factory is the one at risk. However, they therefore ask a lot of the machine builders and want support to resolve things.

Interviewer: In your opinion, what does the future of information security look like for the machine-building industry?

SME: 20 years ago, we started with product safety in this industry. That took a long time to become ingrained. We are now at the beginning of the curve with cybersecurity. More and more rules are coming from the government. By default, factories are beginning to expect it, but they are not yet demanding it. Gradually, this will likely continue, for example in the form of IEC62443 or a stripped-down version.

It's important where they are selling it. Large companies that are often attacked, like PepsiCola, have strict requirements. Small machine builders don't have the time, money, and knowledge for it. They get away with it as long as they don't have big customers.

Interviewer: How do machine-building companies stay up-to-date with the latest information security threats and trends?

SME: Some through the government, some through RSS feeds. Also through third parties, which is expensive, but much easier. You don't need expertise and time to put things in order in your company.

Interviewer: Can you share any success stories or best practices that machine-building companies have implemented in regards to information security?

SME: A partner factory, who already had ISO27001 certifications, was very informative. They made it clear that our company also needed to do something. Customers are still reluctant about their factory network security.

To prevent the security approach from becoming too bureaucratic and inefficient: Review twice a year to see if it's still effective. Cut unnecessary steps. Things that never go wrong don't need to be checked as much. You need to assess your risks. Do the risks increase if you don't do something?

Bureaucracy may be inevitable in larger companies with more management layers. But you should still streamline things well.

Interviewer: How do machine-building companies balance the need for security with the need for accessibility and ease of use for their employees and customers?

SME: Not everything you do with security has an effect. As long as people know why they do it, it can count on support and commitment from management. Again, there's a surprising lack of knowledge about Security at the management level. There are many opportunities to create documentation there. After all, everything starts with management commitment.



Building Cybersecurity for Industry 4.0:

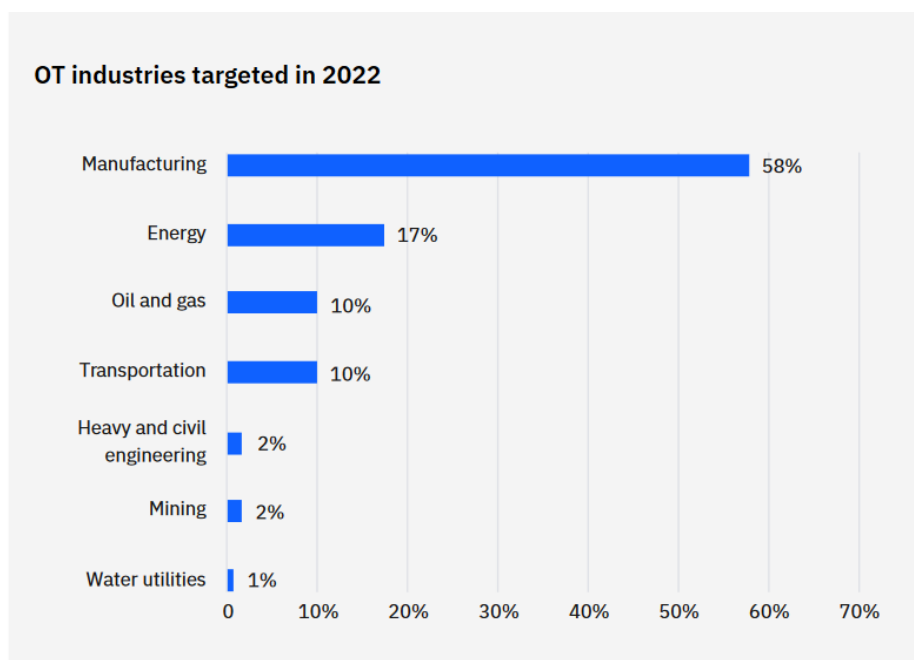
A Practical Guide for OEMs



Cybersecurity in Industry 4.0

As Industry 4.0 continues to revolutionize the manufacturing sector, machine builders find themselves at the forefront of this transformation. The increasing integration of cutting-edge technologies, such as the Internet of Things (IoT), artificial intelligence (AI), and advanced analytics, has brought new opportunities for growth and innovation. However, these advances also present new challenges in security.

Machine builders are now responsible for creating and deploying advanced machinery that is more connected and automated than ever before. This interconnectivity comes with increased cybersecurity risks. Whether you're assembling industrial-grade equipment or fine-tuning complex robotics, cybersecurity is just as vital as ensuring the mechanical integrity of your machines. In recent years, there has been a rise in cyberattacks that target the manufacturing sector, including machine builders.



OT industries targeted in 2022. Source: X-Force

Manufacturing was the most-frequently attacked industry in 2023, and this has been true for multiple years in a row¹. This is unsurprising as 65% of manufacturing environments run outdated, vulnerable firmware². More than 60% of victims end up paying the ransom in case of an attack, making the OEM industry an attractive target for hackers. Damages often run into the hundreds of thousands or even millions of dollars³.

¹ IBM Security (2023). 2023 X-Force Threat Intelligence Index. Retrieved from <https://www.ibm.com/security/data-breach/threat-intelligence>

² TrendMicro (2021). Manufacturing: A Prominent Target for Cyberattacks. Retrieved from <https://www.trendmicro.com/vinfo/ie/security/news/internet-of-things/>

³ Claroty (2021). The Global State of Industrial Cybersecurity: Resilience Amid Disruption. Retrieved from <https://claroty.com/resources/reports/the-global-state-of-industrial-cybersecurity>

Cyberattacks can have significant impact, including:

- × **Loss of intellectual property:** The theft of sensitive information, such as design specifications can severely impact a company's competitive advantage.
- × **Disruption of production:** Cyberattacks on industrial control systems (ICS) can result in downtime, causing delays in manufacturing processes and impacting a company's bottom line.
- × **Damage to reputation:** A successful cyberattack can affect a machine builder's reputation, leading to a loss of trust among customers and partners.
- × **Legal and regulatory consequences:** Non-compliance with data protection regulations can lead to fines, penalties, and legal liabilities.

To address these challenges and ensure the security of their machines and systems, machine builders must adopt a proactive approach to cybersecurity. By implementing cybersecurity measures, machine builders can protect their valuable assets, maintain the trust of their customers, and foster a culture of security within their organization.

The Security Framework explained

Machine builders face an ever-evolving landscape of cybersecurity threats. Navigating this terrain can be daunting, especially while cyberattacks are prevalent and can have a large impact on an organization. It's clear that taking cybersecurity measures is essential.

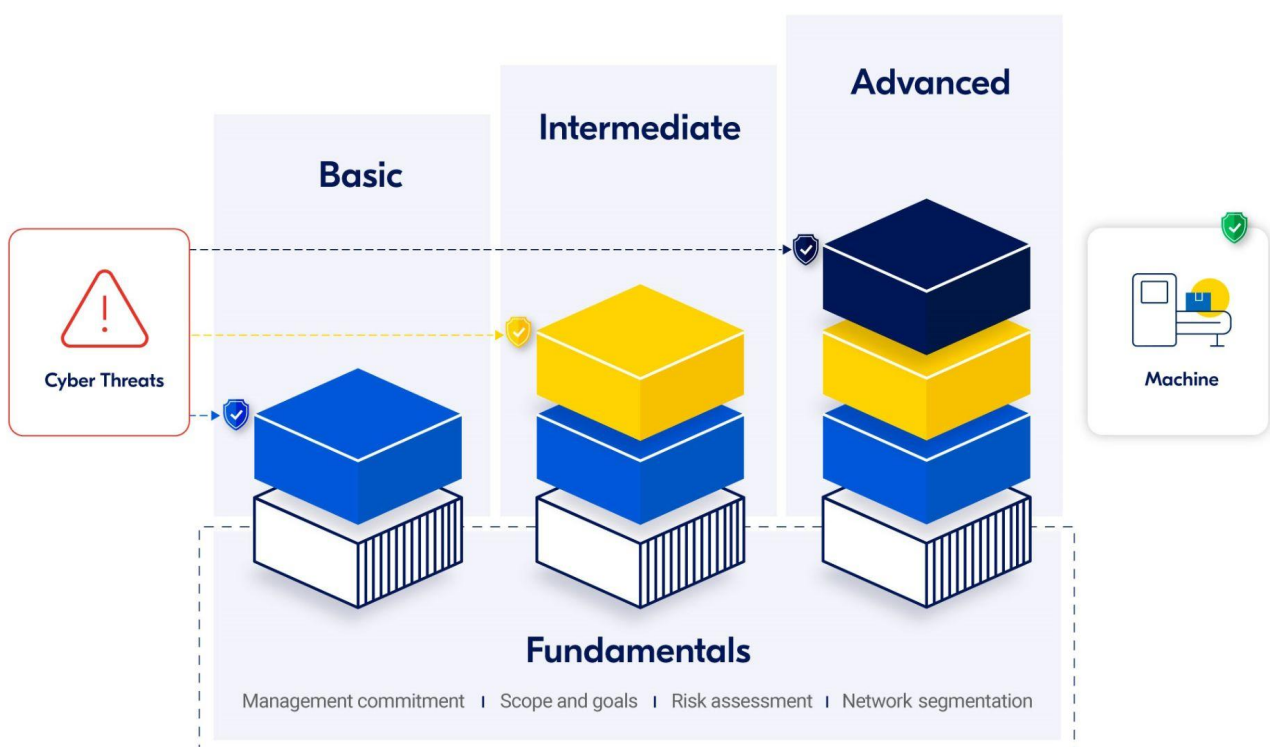
To aid in this challenging task, we've developed a straightforward, adaptable Security Framework to assist you in protecting your business. It is specifically designed to help industrial machine builders navigate the complex world of cybersecurity and protect their business, products, and customers from the cyber threats of Industry 4.0.

The accessible and approachable design, allows you to focus on control measures that are achievable for your organization at your current level of cybersecurity maturity. The framework is divided into four tiers of control measures: **Fundamentals**, **Basic**, **Intermediate**, **Advanced**. The first two form the foundation of your security strategy and implement easy-to-achieve security protections. These initial steps will help you establish a base security strategy and can be implemented by most organizations, regardless of their size or experience. The framework takes into account the importance of not only **technology** but also **people** and **processes**, alongside **machine**-related topics in building a strong cybersecurity foundation.

As you progress in your security journey, you may choose to tackle more complex and advanced controls, found in the **Intermediate** and **Advanced** tiers of the framework. These measures are designed to further enhance your organization's security capabilities and resilience against different and more sophisticated cyber threats.



Security framework



The importance of taking action

*The most important thing to remember is that you don't need to implement every control measure at once. You can gradually work through the framework at a pace that suits your organization's needs and resources. On the other hand, we do want to stress that it is vital to actually **start** doing things; don't put security off to a later date.*

Our aim is to help you by providing clear guidance and actionable steps, while still addressing the unique challenges and risks faced by the industry. We encourage you to start with the control measures that you feel are achievable and build on them as you gain confidence and expertise.

This security framework is based on international standards and best practices, including the ISO 27001, IEC 62443, and the NIST Framework. While this handbook is not a complete guide to achieving certification in these standards, implementing the measures outlined here will help prepare your organization for them. By following this framework, you will be taking significant steps towards compliance with these internationally recognized standards. You'll find further references to these standards throughout the handbook for further reading.

Content in this handbook

In the first part (which you are reading now), we explore the current security landscape in the age of Industry 4.0 and introduce how the IXON Security Framework can help you kickstart and guide your security strategy. The security topics ('Control Measures') used in the framework are introduced and explained at a high level, starting with the Fundamentals and Basics. This is meant to be a quick tour along all important topics and security protections we feel machine builders should be familiar with. No prerequisite knowledge is needed.

Because we feel that it is important to move beyond jargon buzzwords and generic phrases such as "improve security awareness", we present you with a practical Implementation Handbook. Here, you'll find concrete, actionable implementation guidance aimed at strengthening your cybersecurity posture, offering insights that extend beyond theory and dive into practical application. This section is especially important for those that are responsible for implementing the protections in the organizations. References are provided to additional reading and material such as specific sections of the ISO, NIST and IEC standards if you want to take your security to the next level and prepare for official certification.

We hope that you find this handbook to be a valuable resource in your cybersecurity journey and that it empowers you to build a more secure and resilient organization.

Fundamentals of Cybersecurity

At the core of an effective cybersecurity strategy are its foundational elements. These pillars lay the groundwork on which all other measures are built and form the bedrock of your cybersecurity strategy. Let's introduce each:

Management commitment

Like the captain steering a ship, the direction and priorities set by management can guide the entire organization. In the context of cybersecurity, management must demonstrate their commitment to establishing, implementing, and maintaining a competent security strategy.

Any security plans are dead in the water if management only considers security an unnecessary cost. However, when considering an average data breach can cost an organization millions in (reputational) damage, lost revenue and fines⁴, spending a small percentage of revenue on security becomes a logical move.

Good management commitment boils down to investing in the right people, with the right tools and the right amount of time and authority to improve security. Besides that, commitment means emphasizing the importance of cybersecurity at all levels of the organization, and ensuring cybersecurity is incorporated into decision-making processes. In essence, management commitment is the driving force that propels the cybersecurity strategy forward.

Scope and goals

After ensuring management is on board with security improvements, your security scope outlines the breadth and depth of the strategy – the systems, processes, and data it should protect, and the threats it guards against. The goals define measurable outputs of what the strategy aims to achieve – it could be protecting sensitive data, ensuring system availability, or complying with industry regulations. Defining clear and specific goals not only gives direction to the strategy but also provides a benchmark to measure its success.

Risk assessment

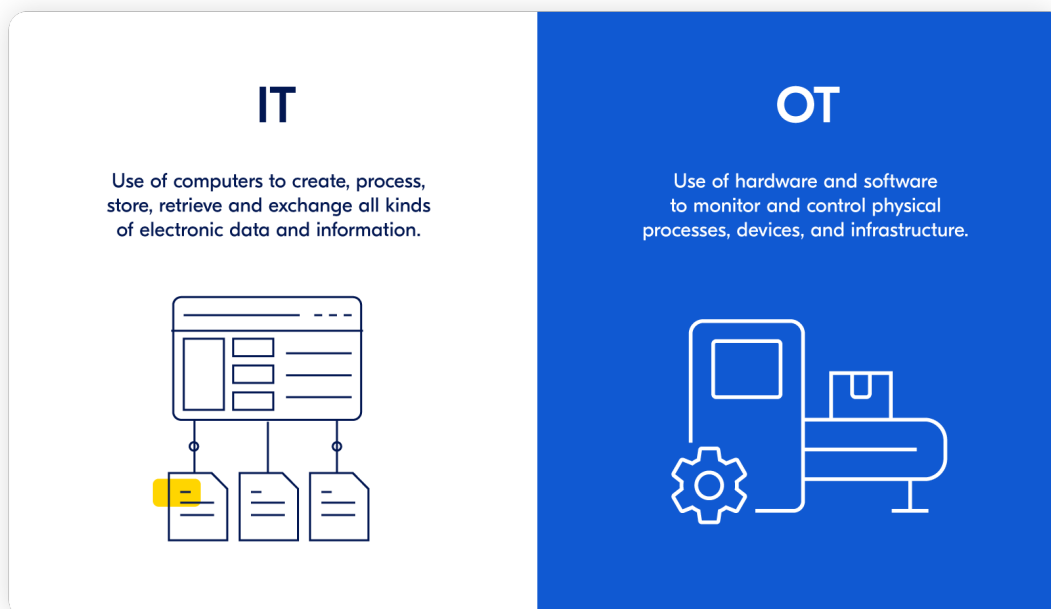
Risk Assessment forms the third foundational pillar. It is the process of identifying everything, within your scope, that could impact you in reaching your goals; listing potential threats and estimating the impact if such threats materialize. By assessing risks, you can prioritize your efforts on areas that pose the greatest threat to your operations.

⁴ IBM Security (2023). 2023 X-Force Threat Intelligence Index. Retrieved from <https://www.ibm.com/security/data-breach/threat-intelligence>

Network segmentation

The greatest source of vulnerabilities is outdated software. As OEMs are very aware, industrial machines are difficult to update and patch⁵. In an ideal world, machines are as easily updated as a laptop, but until then, network segmentation is a valuable tool. By separating the network your machines reside on from the network where the rest of OT and IT exists, you can better manage and control access, ensuring that a breach in one area does not compromise the entire network.

Information technology (IT) VS. Operational technology (OT)



⁵ SANS 2022 Survey: The State of OT/ICS Cybersecurity in 2022 and Beyond. Retrieved from: <https://www.nozominetworks.com/downloads/US/SANS-Survey-2022-OT-ICS-Cybersecurity-Nozomi-Networks.pdf>

Cornerstone of security

These fundamentals – Management Commitment, Scope and Goals, Risk Assessment, and Network Segmentation – form the cornerstone of any effective cybersecurity strategy. As we proceed to the subsequent chapters and implementation guidance detailing more specific measures and practices, remember that these all rest upon the strong foundation set by these fundamentals.





The following control measures are divided into distinct categories, each focusing on different aspects of organizational security:

- 🛡️ **People:** Control measures that focus on building a resilient workforce that is aware of security policies and responsibilities.
- 🛡️ **Processes:** Control measures that involve the establishment of effective policies, guidelines, and procedures to ensure that security best practices across the organization are consistently applied.
- 🛡️ **Technology:** Control measures that implement technical controls and security solutions to protect hardware, data and infrastructure.
- 🛡️ **Machine:** Control measures that emphasize the importance of incorporating security in machines from the ground up.

The following table shows the full overview of all the Control Measures covered in this guide, supported by their respective Fundamentals. In the subsequent chapters, we'll introduce each Control Measure briefly by category.



Control Measures

	People	Processes	Technology	Machine
 Advanced	A1 - Competencies & Training A2 - Threat intelligence	A3 - Incident response testing A4 - Maturity assessment A5 - Business continuity plan	A6 - Endpoint detection & response (EDR) A7 - Security Information and Event Management (SIEM)	A8 - Penetration testing A9 - Logging & Monitoring
 Intermediate	I1 - Access rights management I2 - Internal security audits I3 - Employee screening I4 - Hardware handling I5 - Security governance	I6 - Change management I7 - Supplier review I8 - Information hygiene I9 - Software development lifecycle	I10 - Network & Data encryption I11 - Backups	I12 - External communication I13 - Automated vulnerability assessment
 Basic	B1 - Onboarding & Awareness B2 - Secure offboarding B3 - Security activities planning	B4 - Document policies B5 - Incident response plan B6 - Incident reporting B7 - Risk treatment B8 - Physical access control	B9 - Firewalls & Antivirus B10 - Patch management B11 - Password management	B12 - Physical machine access B13 - Secure configuration
 Fundamentals	F1 - Management commitment	F2 - Scope and goals	F3 - Risk assessment	F4 - Network segmentation

People

Human resources

A security strategy is only as strong as its weakest link, which tends to be the people in an organization. This is why our journey into cybersecurity starts by recognizing that everyone in a team plays a role in maintaining it. This responsibility begins the moment a new member is welcomed aboard, through a structured **Onboarding & Awareness** process. This isn't just about explaining company rules. It's about training new hires on the latest cyber threats and the best ways to keep digital environments secure. Prior to welcoming these new hires, take steps to ensure their trustworthiness through **Background Checks**. As employees eventually move on to other jobs, carry out a **Secure Offboarding** process. This process makes sure that access rights are removed and any critical data stays within the organization. During their employment, it's a prudent idea to measure **Competencies and provide Training** in order to keep everyone's skills sharp and up to date.

Security culture

A cybersecurity approach doesn't stop with the employees—it goes right up to the way the organization is structured. This is where **Security Governance** comes in. It's the master plan that guides all cybersecurity efforts. Assign all security-related tasks to various people in the organization, which helps everyone know their role in keeping the organization safe. This plan includes **Planning Security Activities** ahead of time; carrying out activities, audits, workshops, and training sessions to stay a step ahead of threats. To reduce the chances of data getting into the wrong hands, it's important that people only have access to the data they need to do their jobs, through **Access Rights Registration**.

Identifying risks

Just like machines need regular checkups, so do information systems. To make sure everything is running smoothly and the rules are being followed, perform **Internal Security Audits**. To inform these audits and to make sure you're staying on top of the latest trends in cybersecurity, consider gathering **Threat Intelligence**. This goes beyond just keeping an eye on your own systems. It's about knowing what new dangers are out there and how you can be ready to protect yourself from them before they become a problem.

Finally, do not forget about physical assets (hardware). By having clear rules on **Handling Hardware**, such as how to store them securely and dispose of them correctly, you can reduce the risk of physical theft or damage.

Processes

Building the foundation

Setting up a clear and consistent process for developing, managing, and maintaining **Document Policies & Guidelines** is the first step towards securing your processes. These policies and guidelines are the roadmap that outlines the do's and don'ts for various situations. It ensures everyone understands their role in cybersecurity.

However, even with the best guidelines, incidents can (and will) occur. This is where a well-defined **Incident Response Plan** comes into play. This plan is the fire escape map of your cyber world—it defines the steps to be taken, the responsible parties, and the recovery process. Meanwhile, an effective **Incident Reporting Plan** equips team members with a clear protocol for reporting potential threats quickly. Lastly, a **Business Continuity Plan** acts as a survival guide for maintaining operations during and after a security incident, to ensure critical functions continue during a disruption and are swiftly restored to normal afterwards.

Another crucial process is the regular **Supplier Review**. Just as a machine builder ensures the quality of their materials, organizations must ensure their vendors adhere to necessary security standards to protect against potential vulnerabilities.

Management risk

Risk Treatment is a key component of cybersecurity, which involves assessing identified risks and deciding the best course of action—be it reducing, accepting, or transferring the risk. An equally crucial factor is **Physical Access Control**. Even in a digital world, the importance of physical security can't be overlooked, considering that servers, machines, and data all have a physical presence. Meanwhile, security should also be a top consideration throughout software development. The **Secure Software Development Lifecycle (SDLC)** is a crucial process for building secure software applications. This involves integrating security measures at every stage, from the initial design to deployment, ensuring that the systems developed are secure from the ground up.

Managing change

Effective **Change Management** is important in the rapidly evolving landscape of cybersecurity. This involves evaluating, approving, and implementing changes to systems or processes to minimize potential risks. Together with managing change, maintaining **Information Hygiene** is vital. This process involves regular cleanup of data stores, removing outdated information, and cautious sharing of information—akin to a health check for your data.

Testing and assessing

Preparing readiness for potential cyber threats is a major aspect of process-related security measures. **Incident Response Testing** is similar to conducting safety drills, ensuring your incident response plan functions effectively when a real threat emerges. This process often involves conducting simulations to test your team's readiness and the effectiveness of your response strategies. Likewise, a **Maturity Assessment** provides a holistic review of your Information Security Management System's readiness and capability to protect against cyber threats.

Technology

Preventive technology

Preventing a cyber-attack is always more efficient than dealing with its aftermath. That's why tools like **Firewalls and Antivirus** software form the bedrock of any cybersecurity infrastructure. Firewalls control network traffic to your systems like gatekeepers, while antivirus software scans for and neutralizes threats that may have found a way in. **Managing patches** in a timely way ensures that systems are protected against the newest threats.

Along with these first lines of defense, the role of **Password Management** is one of the most effective. By enforcing strong password policies and using password managers, unauthorized access can be prevented. **Network and Data Encryption** converts sensitive data into unreadable text, ensuring its confidentiality even if intercepted during transmission or storage.

Reactive technology

Despite preventative measures, it's essential to be prepared to react to attacks quickly and effectively. **Endpoint Detection and Response (EDR)** complements this by focusing on detecting, investigating, and mitigating suspicious activities on devices accessing your network. It's like an advanced diagnostic tool that not only identifies problems but also offers solutions. Working alongside EDR, **Security Information and Event Management (SIEM)** systems act as the central hub of security operations, gathering and analyzing data from various sources to provide an overview of the security status.

Recovery technology

Regardless of the strength of preventative and reactive measures, cybersecurity is not complete without a solid recovery plan. Regular **Backups**, made by creating copies of data and systems, provide a safety net, so that operations can be restored swiftly in case of data loss or system failure.

Machine

Baseline Security

To protect machines, setting up a secure baseline is crucial, beginning with restricting **Physical Machine Access**. It's not only about protecting digital access but also controlling who can physically interact with your machines. Restrict access to those who really need it. Similarly, **Secure Configuration** of machines means restricting digital access to ports, services and data.

Communication

Proper **External Communication** and documentation is an effective yet often overlooked aspect of cybersecurity. It includes developing a set of standard documents that outline guidelines and expectations for machine connectivity, supplier security, and terms of service.

Finding vulnerabilities

Regular **Automated Vulnerability Assessments** are part of a proactive strategy, helping to identify, and remediate potential weaknesses in information systems and networks. Going beyond automatic tests, **Penetration Testing** simulates authorized attacks on your machines or systems to uncover vulnerabilities before they're exploited by actual hackers.

Ongoing monitoring

Finally, keeping the environment secure requires ongoing vigilance. An effective way to do this is by setting up a **Logging and Monitoring** policy that allows for continuous tracking of machine activity, enabling quick detection and response to potential cybersecurity threats and system performance issues.

Key takeaways

We've introduced key concepts ranging from risk management to using technology tools to secure operations and machines. But the journey doesn't end here. Now, it's time to start putting this knowledge into action. Start small, but do start on any of the concepts introduced above. To make the concepts approachable, the next section offers specific, actionable implementation guidance for the control measures we introduced.

Part 2: Implementation Guidance

The following Implementation Handbook is your field guide, to help you navigate the practical application of the security concepts we've explored thus far. Here, you'll find actionable guidance aimed at strengthening your security posture, offering insights that extend beyond theory and dive into practical application.

This Implementation guidance aligns directly with the Control Measures detailed in the IXON Security Framework. This Framework acts as a compass for organizations looking to enhance their security practices. While it caters to a broad spectrum of industries, it pays specific attention to the needs and challenges of the machine builder industry.

As before, to simplify the journey, the Control Measures within the IXON Security Framework are divided into four main categories: **People, Processes, Technology, and Machine**. These categories form the pillars of a robust security strategy, underscoring the importance of a well-rounded, holistic approach to securing your organization.

The Control Measures are also structured according to their level of implementation complexity: **Basic, Intermediate, and Advanced**. All of these measures build on the **Fundamentals**, which need to be in place before subsequent strategies can be effective. This arrangement allows for a progressive approach to security, akin to building a structure from the foundation up. When you have the Fundamentals covered, we recommend starting with the Basic measures. These foundational steps offer substantial impact, often with minimal resource allocation, allowing you to secure quick wins and establish a solid base. As you grow more comfortable and proficient, you can move to the Intermediate and Advanced measures, continually enhancing your security posture and resilience.

The subsequent sections of this Handbook provide detailed, easy-to-follow guidance on implementing each Control Measure from the IXON Security Framework. We also present a look into how IXON as an organization approaches and implements these security concepts.

Remember that security is not a one-size-fits-all field, especially for diverse machine builders. The guidance should be adapted to fit the unique characteristics of your organization.

Fundamentals.....	15
Fundamental 1: Management commitment.....	15
Fundamental 2: Scope and Goals.....	16
Fundamental 3: Risk assessment.....	17
Fundamental 4: Network segmentation.....	18
Basic Control Measures.....	19
Control Measure B1: Onboarding & Awareness.....	19
Control Measure B2: Secure Offboarding.....	20
Control measure B3: Security Activities Planning.....	21
Control measure B4: Document policies & guidelines.....	22
Control measure B5: Incident response plan.....	23
Control measure B6: Incident reporting.....	24
Control measure B7: Risk treatment.....	25
Control measure B8: Physical access Control.....	26
Control measure B9: Firewalls & Antivirus.....	27
Control measure B10: Patch management.....	28
Control measure B11: Password management.....	29
Control measure B12: Physical machine access.....	30
Control measure B13: Secure configuration.....	31
Intermediate Control Measures.....	32
Control measure I1: Access Rights Management.....	32
Control measure I2: Internal security audits.....	33
Control measure I3: Employee screening.....	34
Control measure I4: Hardware handling.....	35
Control measure I5: Security governance.....	36
Control measure I6: Change management.....	37
Control measure I7: Supplier reviews.....	38
Control measure I8: Information hygiene.....	39
Control measure I9: Software Development Lifecycle.....	40
Control measure I10: Network and Data Encryption.....	41
Control measure I11: Backups.....	42
Control measure I12: External communication.....	43
Control measure I13: Automated vulnerability assessment.....	44
Advanced Control Measures.....	45
Control measure A1: Competencies and Training.....	45
Control measure A2: Threat intelligence.....	47
Control measure A3: Incident response testing.....	48
Control measure A4: Maturity Assessment.....	49
Control measure A5: Business Continuity Plan.....	50
Control measure A6: Endpoint Detection & Response (EDR).....	51
Control measure A7: Security Information and Event Management (SIEM).....	52
Control measure A8: Penetration testing.....	53
Control measure A9: Logging & monitoring.....	55
Appendix A: Control measures overview.....	56
Appendix B - IXON's Risk Assessment template.....	57

Fundamentals

Fundamental 1: Management commitment

Category	Threat types	Additional reading
Fundamental	Inadequate resources Lack of awareness Misaligned policies	ISO/IEC 27001:2022 - Section 5.1 IEC 62443-2-1:2010 - Section A.3.2.3

Management commitment is the foundation for any successful security strategy. It is crucial for the organization's management to prioritize security and allocate resources to promote an effective and efficient security strategy. Security is most effective when a proactive approach is taken to reduce risks, instead of a reactive posture by only taking action after a security incident has taken place.

Objective

The organization's management should demonstrate a strong commitment to the development, implementation, and maintenance of an effective security strategy. This commitment should be communicated to all employees and backed by adequate resources, clear objectives, and measurable outcomes to ensure alignment with the organization's goals and to create a security mindset from the top down.

Implementation guidance

To demonstrate and foster management commitment, consider the following steps:

- a. **Leadership involvement:** Management should actively participate in the development and implementation of the security strategy. Outline clear, measurable, and realistic objectives aligned with the organization's overall goals (Fundamental 2). These objectives will guide the development of all security policies and procedures.
- b. **Resource allocation:** Management should ensure that adequate resources, including personnel, financial support, and technology are allocated to support the security program. This includes investing in tools, training, and expertise.
- c. **Assign responsibilities:** Management should designate a member or a team to coordinate security matters. This individual or team should have the necessary authority, resources, and support to execute their responsibilities effectively.
- d. **Communication and awareness:** Management should communicate the importance of security to all employees, emphasizing the role each person plays in protecting the organization's digital assets, reinforcing the message of shared responsibility.
- e. **Management review:** At least once a year perform a management review. Together with management, regularly review all aspects of the security program and update whenever necessary. Consider the organization's goals and vision, policies, and the evolving security landscape.

Fundamental 2: Scope and Goals

Category	Threat types	Additional reading
Fundamental	Misaligned objectives Misaligned policies Waste of resources	ISO/IEC 27001:2022 - Section 4.3 IEC 62443-2-1:2010 - Section 4.3.2.2

In the machine builder industry especially, organizations need to balance their security measures with their core business objectives, and recognize the unique challenges and requirements of their sector. This makes outlining the organization's scope and goals of their security program especially important to provide clear direction and resource allocation.

Objective

Establish a clear scope for a security program, outlining the specific areas, systems, and processes that need to be secured. Additionally, the organization should define its goals, detailing the desired level of security and the specific objectives that can realistically be achieved.

Implementation guidance

To define the scope and goals of the security program, organizations should consider the following steps:

- a. **Identify boundaries:** Outline the boundaries of your cybersecurity strategy, including systems, departments, facilities, and assets to be protected. For machine builders this can involve identifying critical industrial control systems, intellectual property, and other sensitive information that requires protection. Regularly review the scope and choose whether you want to broaden it.
- b. **Set SMART goals:** Set goals for your cybersecurity strategy using the SMART framework. Each goal should be Specific, Measurable, Attainable, Relevant, and Timely. Examples of SMART goals:
 - ☒ Decrease successful phishing attacks by 90% over the next 6 months through improved email security protocols and employee training.
 - ☒ Achieve an average machine uptime of 99,5% for each month.
 - ☒ Implement secure communication protocols in 100% of our Industrial Control Systems within the next 6 months to protect data.
 - ☒ Ensure that at the end of the year at least 75% of all machines are segmented in their own network to reduce the likelihood of outdated software being exploited.
- c. **Align Goals with Business Objectives:** Ensure that your cybersecurity goals align with your broader business objectives. This alignment enhances the relevance of your cybersecurity efforts, making them an integral part of your overall business strategy rather than a standalone initiative.

Fundamental 3: Risk assessment

Category	Threat types	Additional reading
Fundamental	Inefficient allocation of resources Undetected system vulnerabilities Unidentified risks	ISO/IEC 27001:2022 - Section 5.1 ISO/IEC 27005:2018 - Section 8 IEC 62443-2-1:2010 - Section 4.2.3 NIST SP 800-30 NIST Risk Management Framework

Assessing risks is a vital part of creating a security program. It helps your organization prioritize possible threats and allows you to make decisions proactively. The results of these assessments should guide your cybersecurity strategy and decision-making.

Objective

Perform risk assessments to identify, analyze, and evaluate potential cybersecurity risks. This process should be systematic, repeatable, and consistent, taking into account the specific threats, vulnerabilities, and impacts that the organization may face.

Implementation guidance

Risk assessment starts with selecting an appropriate framework for assessing the risks that an organization faces. Refer to the Additional reading references above for established frameworks, or consider the following steps for an overview:

- a. Categorize critical assets: Identify the assets that are essential to your business operations. Sort them based on factors such as their value, sensitivity, or criticality to the organization's operations.
- b. Identify threats and vulnerabilities: Identify the possible threats and vulnerabilities that could affect your organization's goals. This might include outside threats, like cybercriminals and corporate spies, and inside threats, like actions by insiders or human errors.
- c. Assess risk levels: Determine the level of risk for each threat-vulnerability pair. This could be based on the potential impact of a successful exploit and the likelihood of the threat.
- d. Prioritize risks: Based on risk levels, prioritize the identified risks, focusing on those with the highest likelihood and impact. High-risk threats that could lead to significant damage should receive more immediate attention.
- e. Document findings: Document the findings of the risk assessment, including the identified goals, assets, threats, vulnerabilities, risks, and prioritization. This documentation will serve as a basis for the organization's risk management activities and informs future control measures and decisions.

IXON's approach

See IXON's Risk Assessment template in [Appendix B](#)

Fundamental 4: Network segmentation

Category	Threat types	Additional reading
Fundamental	Cross-network attacks Data breaches ICS attacks Unauthorized access	ISO/IEC 27002:2013 - Section 8.2 + 8.31 IEC 62443-2-1:2010 - Section 4.3.3.4 NIST SP 800-82

Network segmentation between IT (Information) and OT (Operational) networks is a fundamental measure that can significantly reduce the risk of cybersecurity incidents. It ensures that even if one part of the network is compromised, the attacker cannot easily move to other parts of the network.

Objective

Recognizing the difficulty of security patching in industrial machines once installed machines are operational, organizations should implement network segmentation between machines and IT and OT networks to not only enhance network security but also improve manageability.

Implementation guidance

To protect (often outdated) machines from cyberattacks, it is important to isolate them from the rest of the network. Make an inventory of all communication protocols from and to the machine and design a solution that protects all of them. Understand how the IT and OT networks interact and depend on each other.

The simplest solution to segment the networks is to employ a firewall separating the machine and its components from the OT- and IT-networks, ensuring:

- a. The firewall is configured to allow only necessary traffic
- b. The firewall is updated with the latest security patches
- c. The firewall is protected with proper access controls
- d. The firewall is physically protected

Basic Control Measures

Control Measure B1: Onboarding & Awareness

Category	Threat types	Additional reading
Basic People	Insider threats Phishing attacks Social engineering attacks Weak/compromised credentials	ISO/IEC 27002:2022 - Section 6.3 IEC 62443-2-1:2010 - Section 4.3.2.4 NIST SP 800-50

Objective

Develop and implement a training plan that includes guidelines on acceptable use, access control, incident response, and other relevant security practices. This plan should be introduced to new employees during the onboarding process and reinforced through regular awareness training tailored to the specific roles and responsibilities of each employee.

Implementation guidance

To create a strong security mindset among employees and promote a culture of security awareness, organizations should consider the following steps:

- a. Onboarding: Introduce new employees to the organization's cybersecurity policy and procedures during the first weeks of employment.
- b. Regular training sessions: Conduct training sessions that keep employees informed about the latest cyber threats and trends, as well as the organization's cybersecurity policies and procedures. These sessions may cover topics such as phishing, malware, and social engineering.
- c. Industry and role relevance: Ensure the training content is relevant to your market, and the specific roles of the employees.
- d. Reinforcement of key messages: Use posters, newsletters, and other communication channels to reinforce key cybersecurity messages and promote a culture of security awareness among employees.

IXON's approach

We foster a security culture through the following initiatives:

- ✓ Security onboarding presentations are provided to all new employees by the Security Officer within their first week of employment.
- ✓ All employees must complete a security e-learning course within their first month. Modules include: *Security Basics, Phishing, Privacy & GDPR, ISO/IEC Standards, and IXON's Security Policies.*
- ✓ Bi-annual security workshops are organized for relevant departments.
- ✓ An internal chat room to keep the team informed about the latest security developments, notable incidents, and policy changes.

Control Measure B2: Secure Offboarding

Category	Threat types	Additional reading
Basic People	Data leakage Insider threats	ISO/IEC 27002:2022 - Section 6.5 IEC 62443-4-1:2018 - Section 12.7

Objective

An offboarding process should be implemented to manage the departure of (potentially disgruntled) employees, whether they leave voluntarily or their contract is terminated. This process should be documented, with clearly defined roles and responsibilities.

Implementation guidance

Upon receiving notice of an employee's departure, the human resources (HR) department should promptly notify relevant stakeholders (e.g. IT and security) to ensure that the offboarding process begins in a timely manner. The following activities should be covered:

- a. Access revocation: The departing employee's access to all company resources should be revoked. This includes physical access to facilities, electronic access to systems and networks, and access to cloud-based services. Access revocation should be conducted methodically, considering all possible entry points, such as VPNs, email accounts, and shared drives.
- b. Asset recovery: The relevant parties need to ensure the return of all company property (e.g. laptops, phones, entry badges) and verify that sensitive information has been securely wiped from these devices.
- c. Business continuity: The departing employee's supervisor should ensure that critical knowledge and information related to their job responsibilities are transferred to other team members or documented for future reference. This may include project documentation, passwords, encryption keys, and other essential data.
- d. Contractual obligations and evaluation: The HR department should conduct an exit interview with the departing employee. This is an opportunity to remind the employee of confidentiality, non-disclosure, and non-compete agreements, if applicable.

Consider a method to track and document progress while executing this process, to ensure all steps are completed in an acceptable time frame.

IXON's approach

We secure the offboarding process in the following ways:

- ✓ A meeting is scheduled during the final week of employment to discuss task handover, hardware hand-in, and access rights.
- ✓ The Security Officer ensures that all access is revoked.
- ✓ The Hardware Service Desk wipes and factory resets laptops and mobile phones.
- ✓ An exit interview is conducted by HR.

Control measure B3: Security Activities Planning

Category	Threat types	Additional reading
Basic People	Negligence of activities	ISO/IEC 27002:2022 - Section 5.1 IEC 62443-4.1:2018 - Section 5.1 IEC 62443-2-1:2010 - Section 4.3.2.6

Objective

Maintain a planning that covers all activities of the organization's cybersecurity strategy, including risk treatment, incident response, and continuous improvement.

Implementation guidance

Consider the following steps when establishing a systematic approach to security activities planning:

- a. **Brainstorm:** Collaborate with all relevant personnel to decide on the security events for the upcoming period. These may include penetration tests, training workshops and other one-off projects.
- b. **Inventory of events:** Make an inventory of all recurring security events. Decide on the appropriate frequency for each event for your organization (once a year, once a month, etc.). This includes internal/external audits, management reviews, risk assessments etc.
- c. **Document:** Plan all recurring and non-recurring events in a clear overview, assign responsible persons to each item and/or add a deadline. These event owners are required to mark items as completed.
- d. **Evaluate:** Regularly evaluate the plan and ensure deadlines are met.

IXON's approach

Twice a year, we gather relevant employees to plan security events for the upcoming period. These, alongside recurring security activities, are tracked in a spreadsheet reviewed monthly by the Security Officer.

Each item contains:

- Name of the event
- Responsible person
- Deadline (if applicable)
- Status (Not started, In Progress, Completed)
- Completion date
- Reference to finished product (link to document, checklist, etc.)

This plan is reviewed once a month by the Security Officer, who discusses delays and other blocking issues with the responsible persons.

Control measure B4: Document policies & guidelines

Category	Threat types	Additional reading
Basic Processes	Misconfigurations Non-compliance with regulations	ISO/IEC 27002:2022 - Section 5.1 IEC 62443-2-1:2010 - Section 4.2.4.4 NIST SP 800-12

Objective

Establish a clear and consistent process for developing, managing, and maintaining cybersecurity policies, procedures, and guidelines. This process should ensure that documentation remains up-to-date, relevant, and accessible to all employees.

Implementation guidance

To create documentation that is readable and maintained, consider the following items:

- a. Define document structure: Establish a standard structure or template for all security documentation, including policies, procedures, and guidelines. This structure should ensure uniformity, readability and ease of navigation.
- b. Assign ownership: Assign each document to individuals or teams responsible for creating, updating, and maintaining them. Ensure each document is reviewed at least once a year.
- c. Distribute documents: Make the documents available to all employees in a way that makes it easy to reach. Ensure the document is understandable and does not create unnecessary confusion.

IXON's approach

At IXON, all documents are gathered in an information security management system, readable by all employees on an intranet. Documents consist of three types:

1. *Policies* outlining the rules employees must follow.
2. *Procedures* explaining how tasks should be carried out.
3. *Guidelines* detailing best practices to consider.

Control measure B5: Incident response plan

Category	Threat types	Additional reading
Basic Processes	Data breaches Denial of service attacks Ransomware attacks	ISO/IEC 27002:2022 - Section 5.24 - 5.28 IEC 62443-2-1:2020 - Section A.3.4.5 NIST SP 800-61

Objective

Establish and maintain an incident response plan outlining the procedures to follow in the event of a cybersecurity incident. The plan should at a minimum detail the types of incidents it applies to and the roles and responsibilities of those involved.

Implementation guidance

To develop and implement an effective incident response plan, consider the following steps:

- a. Define incident types and attack surface: Clearly define the types of incidents addressed, the assets and systems that require protection.
- b. Assign roles and responsibilities: Identify individuals and teams responsible for handling the incident, and any external resources that may be required. Assign clear roles and responsibilities for accountability and efficient communication during an incident.
- c. Develop incident response procedures: Create a set of detailed procedures outlining the specific steps to be taken in the event of a cybersecurity incident.

IXON's approach

Our Incident Breach Protocol distinguishes between minor and major incidents. Major incidents trigger the following action plan:

- 1) Incident verification; Check if the incident is legitimate.
- 2) Task force briefing; Brief all relevant employees on the situation.
- 3) Containment; Take the necessary steps to ensure the incident can not spread to additional systems.
- 4) Initial reporting; Notify relevant authorities, partners and customers.
- 5) Recovery; Ensure the system is operational again.
- 6) Root cause analysis; Discover how and when the incident happened.
- 7) Closure reporting; Notify that the incident is resolved, explain the steps taken and lessons learned transparently.
- 8) Long-term improvement; Use the incident, root-cause analysis and other findings to discuss improvements to the IXON Cloud, the reporting and the incident process.

Control measure B6: Incident reporting

Category	Threat types	Additional reading
Basic People	Delayed detection of breaches Inadequate incident response	ISO/IEC 27002:2022 - Section 5.24 IEC 62443-3-3:2019 - Section 10 NIST SP 800-61

Objective

Incorporate an incident reporting procedure into your organization's overall cybersecurity strategy. The procedure should be well-documented, user-friendly, and easily accessible to all employees.

Implementation guidance

Simplicity and clarity are crucial for the procedure. Consider the following aspects:

- a. Designated contact point: Appoint a dedicated point of contact responsible for managing security reports. Ensure that this person can be reached through various channels, such as email, phone, instant messaging, or in person.
- b. Reporting guidelines: Consider designing a template that outlines the information to be included in the report.
- c. Employee training and engagement: Emphasize the importance of timely reporting, even if the employee is unsure whether the incident is a genuine threat.
- d. Acknowledgement and reward: Encourage incident reporting by acknowledging and rewarding employees, thereby reinforcing its importance and creating a positive feedback loop that motivates others to do the same.

IXON's approach

We have a dedicated person available via email, internal chat, phone, or in person. The importance of timely reporting is emphasized during the onboarding of new employees. Reported security incidents are treated as learning opportunities, not grounds for punishment.

Control measure B7: Risk treatment

Category	Threat types	Additional reading
Basic Processes	Various	ISO/IEC 27002:2022 - Section 5.1 IEC 62443-3-2:2020 - Section 4.7 + 4.8 IEC 62443-2-1:2010 - Section 4.3.2.3 NIST Risk Management Framework

Objective

Document and implement a risk treatment procedure that aligns with their risk management approach and cybersecurity objectives. This procedure uses the input from the risk assessment (Control Measure F3) and details how and when unacceptable risks should be addressed. Results are collected in a risk treatment plan.

Implementation guidance

Using the input from the risk assessment, develop a procedure that:

1. Flags unacceptable risks: Decide on criteria for when assessed risks are too great to accept (based on score, discussion, etc.)
2. Risk treatment methods: Evaluate and select appropriate risk treatment options based on the organization's risk appetite and resource constraints, ensuring compliance with applicable regulations and industry standards.
3. Document: Record each risk in a risk treatment plan. This plan should contain all necessary information for the treatment of the risk, including, but not limited to:
 - a. Risk owner (responsible person)
 - b. Planned treatment
 - c. Implementation deadline
 - d. Current status
4. Regularly evaluate the plan and ensure deadlines are met. Update the plan based on new insights during the risk assessment.

IXON's approach

Whenever IXON's risk assessment is updated (which is at least twice a year, but also when new risks are identified) the security officer, alongside all knowledgeable stakeholders, goes through the list and flags all unacceptable risks based on their risk score. Each risk is discussed and added to our risk treatment plan. We decide on realistic actions for risk reduction and assign an owner to each risk. Each month, the security officer reviews the risk treatment plan to ensure no activities are delayed.

Control measure B8: Physical access Control

Category	Threat types	Additional reading
Basic Processes	Tampering with critical systems Theft of equipment or information Unauthorized physical access	ISO/IEC 27002:2022 - Section 5.15 IEC 62443-2-1:2010 - Section 4.3.3 IEC 62443-4-1:2018 - Section 5.9 IEC 62443-4-2:2019 - Section 14.6 NIST SP 800-53 PE

Objective

Establish policies and procedures for effective physical access control, to ensure the security of facilities and critical assets.

Implementation guidance

To create effective physical access control, organizations should consider the following strategies:

- a. Secure sensitive areas: Identify and secure areas within the facility requiring restricted access, such as server rooms, manufacturing floors, or storage areas for sensitive materials.
- b. Access control mechanisms: Deploy access control mechanisms like key cards, biometric systems, or electronic access control systems to restrict entry to sensitive areas and provide an audit trail.
- c. Monitor and secure perimeters: Utilize security cameras, alarms, and other surveillance equipment to monitor facility perimeters. Secure fences, gates, doors, and windows with appropriate locking mechanisms.
- d. Visitor management: Develop a visitor management system to audit access for guests, contractors, and other temporary personnel. Issue temporary access cards, require visitors to sign in and out, and provide escorts for individuals needing access to sensitive areas.

IXON's approach

Access to IXON's facilities is only possible with an electronic keycard. Each employee has their own card and card usage is logged. Several secure areas are identified and require elevated privileges to access. Visitors are required to register in the lobby and must be accompanied by an IXON employee at all times.

Control measure B9: Firewalls & Antivirus

Category	Threat types	Additional reading
Basic Technology	Malware Network intrusion Ransomware Unauthorized access Viruses	ISO/IEC 27002:2022 -Section 8.20 + 8.21 IEC 62443-2-1:2020 - Section 4.3.4.3.8 IEC 62443-3-3:2013 - Section 9 NIST SP 800-41

Objective

Implement a combination of firewalls and antivirus software to protect their information systems and networks from malicious software and unauthorized access. These security measures should be kept up-to-date and configured according to industry best practices.

Implementation guidance

To effectively implement firewalls and antivirus software, organizations should consider the following steps:

- a. Firewall deployment: Deploy firewalls at strategic points in the organization's network, such as at the perimeter, between subnets, and around critical systems to establish a security barrier between internal and external networks.
- b. Firewall configuration: Configure the firewall according to the principle of least privilege, allowing only necessary traffic and blocking all other connections by default. Regularly review and update firewall rules to ensure they remain effective.
- c. Antivirus software installation: Install antivirus software on all endpoint devices, including servers and workstations. Ensure the antivirus software does not interfere with the performance or operation of critical applications.
- d. Regular updates: Keep firewalls and antivirus software up-to-date with the latest security patches, signatures, and definitions.
- e. Monitoring and alerting: Set up monitoring and alerting for both firewalls and antivirus software to detect and respond to security incidents quickly. Review logs and alerts to identify potential threats and take appropriate action.

IXON's approach

- ✓ All endpoint devices (laptops, mobile phones, etc.) are equipped with professional antivirus software, which collects data in an administrative panel.
- ✓ Generated alerts are forwarded to the Security Officer and hardware specialists.
- ✓ Scans are performed automatically on a weekly basis.
- ✓ Network traffic is monitored by an intrusion detection firewall with restrictive rules to only allow expected traffic.
- ✓ Updates are installed every week.

Control measure B10: Patch management

Category	Threat types	Additional reading
Basic Technology	Exploitation of known vulnerabilities Malware infections	ISO/IEC 27002:2022 - Section 8.8 IEC 62443-2-1:2020 - Section 4.3.4.3.7 IEC 62443-2-3:2015 - All NIST SP 800-40

Objective

Establish and maintain a patch management policy to ensure timely identification, evaluation, and application of security patches for all software, firmware, and operating systems used in their environment.

Implementation guidance

To implement effective patch management, consider the following steps:

- a. Vulnerability monitoring: Regularly monitor authoritative sources such as vendor websites, security mailing lists, and cybersecurity organizations for the identification of new vulnerabilities and the availability of security patches.
- b. Risk assessment: Evaluate the potential impact of identified vulnerabilities on the organization's information systems and operations, considering factors such as the severity of the vulnerability and the affected systems.
- c. Patch evaluation and testing: If necessary, review and test security patches in a controlled environment before deployment. This helps ensure that the patch does not introduce new issues or conflicts that may disrupt operations.
- d. Patch monitoring and verification: Monitor and verify the successful application of patches, ensuring that all affected systems are updated and secure. This may involve using vulnerability scanning tools, configuration management systems, or other monitoring solutions.

IXON's approach

IXON's security team is subscribed to a number of mailing lists and news outlets regarding new vulnerabilities and security patches. If a vulnerability is applicable to IXON in some way, a risk assessment is performed to determine how big the impact is. Updates to critical systems (CRM, IXON Cloud, Financial systems) are first deployed in staging or testing environments to ensure they do not break functionalities. Afterwards, all systems are double-checked to ensure their security post-update.

Control measure B11: Password management

Category	Threat types	Additional reading
Basic Technology	Account hijacking Brute force attacks Credential theft Unauthorized access	ISO/IEC 27002:2022 - Section 5.17 IEC 62443-4-1:2018 - Section 12.7 IEC 62443-4-2:2018 - Section 5.5 NIST SP 800-63B

Objective

Develop and implement a password management policy that provides guidelines on password creation, storage, and usage. The policy should enforce strong password practices to reduce the risk of unauthorized access to the organization's information systems and networks.

Implementation guidance

To establish an effective password management policy, consider the following:

- a. Password complexity: Require passwords to meet minimum complexity standards. Set a minimum password length in line with modern best-practices, to reduce the likelihood of successful brute force attacks.
- b. Password reuse: Prohibit password reuse across multiple accounts or systems, as this can increase the risk of unauthorized access if a single password is compromised.
- c. Account lockout: Where possible, implement account lockout mechanisms to temporarily lock accounts after a specified number of failed login attempts, reducing the risk of successful brute force attacks.
- d. Multi-factor authentication: Where possible, use multi-factor authentication (MFA) to supplement password-based authentication, requiring users to provide at least two separate forms of proof for their identity.
- e. Monitor password leaks: Monitor for leaked passwords and promptly require affected users to change their passwords.

For ease of implementation, passwords should be stored in a password manager that employs strong encryption and hashing techniques, such as bcrypt, scrypt, or Argon2.

IXON's approach

In order to maintain secure passwords, IXON uses the following management policies.

- ✓ An organization-wide Password manager is mandatory. This password manager automatically scans for reused, weak and leaked passwords.
- ✓ Randomly generated passwords consist of at least 20 characters, PBKDF2 encrypted with 600.000 hashing iterations (as per 2023 OWASP standard)
- ✓ MFA is enforced where possible.

Control measure B12: Physical machine access

Category	Threat types	Additional reading
Basic Machine	Information leaks Physical tampering Theft or damage to equipment Unauthorized access to machines	ISO/IEC 27002:2022 - Section 7.1 IEC 62443-2-1:2010 - Section 4.3.3 IEC 62443-4-1:2018 - Section 5.9 IEC 62443-4-2:2019 - Section 13.6 + 14.6 NIST SP 800-53 PE

Objective

Establish a physical security policy to protect their machines from unauthorized access, tampering, theft, or damage.

Implementation guidance

To implement an effective physical security strategy for machine access, consider the following aspects:

- a. Secure areas: Establish protected zones where machines and equipment are housed, allowing access to these zones only to authorized personnel. Integrate access control mechanisms [CM B8].
- b. Physical protection: Use physical barriers, such as locked cabinets or secure enclosures, to protect sensitive machines and equipment. Prohibit (indirect) access to network ports, USB ports and other communication networks connected to the machine. Ensure that the barriers are robust and resistant to attacks.

Control measure B13: Secure configuration

Category	Threat types	Additional reading
Basic Machine	Compromised machines Data breaches Industrial control system attacks Malware infection Unauthorized access	ISO/IEC 27002:2022 - Section 8.9 + 8.27 IEC 62443-4-1:2015 - Section 12.4 IEC 62443-2-3:2015 - Section B.8.5 NIST SP 800-70 NIST SP 800-53 CM-3

Objective

Establish a process for securely configuring machines to reduce the risk of unauthorized access, data breaches, and other cybersecurity threats.

Implementation guidance

To implement secure configuration of machines, consider the following steps:

- a. Principle of least functionality: Disable unnecessary functions, services, and applications that could lead to security vulnerabilities. Consider closing unused network ports on the device.
- b. Access controls: Implement role-based access controls to regulate user access to administrator privileges, ensuring that only authorized personnel can modify settings. Employ strong authentication methods to prevent unauthorized access [CM B11].
- c. Security patches and updates: We recognize that installed machines are often infeasible to update, due to uptime requirements, quality approval requirements and unavailability of patches. However, ensure your operating systems, firmware, and applications have the latest security patches and updates whenever possible.
- d. Hardening communication protocols: Configure machines to utilize secure communication protocols and encryption techniques. This will protect data transmission between machines and external systems.

Intermediate Control Measures

Control measure I1: Access Rights Management

Category	Threat types	Additional reading
Intermediate People	Data breaches Privilege escalation attacks Unauthorized access	ISO/IEC 27002:2022 - Section 5.16 IEC 62443-3-3:2019 - Section 5.3 NIST SP 800-53

Objective

Develop an access rights policy that defines the principles and guidelines for granting, modifying, and revoking access to an organization's information systems, networks, and physical facilities. The policy should be based on the principle of least privilege, ensuring that individuals only have the necessary level of access to perform their responsibilities.

Implementation guidance

To implement an effective access rights registration process, consider the following steps:

- a. Authorization: Collaborate with relevant supervisors or department heads to determine the appropriate level of access based on the individual's job role. Subsequently, configure the individual's access rights following the access control policy, which may involve creating user accounts, assigning access permissions, and configuring security settings.
- b. Documentation: Maintain a record of all granted access rights, including the individual's name, job role, access permissions, and the date the access was granted.
- c. Periodic Reviews: Regularly review access rights to identify and rectify discrepancies. Schedule these reviews or perform them in response to specific triggers, such as changes in job roles or departmental reorganizations.
- d. Access Rights Revocation: Revoke access rights promptly when an individual leaves the organization or is terminated. Coordinate this process with the organization's secure offboarding procedures [CM B2].

IXON's approach

When an IXON employee requires access to a new portal or solution, a request is made to their department lead or the security officer. They evaluate the necessity of the requested access. IXON utilizes a tool to catalog all vendors, including all portals and other logins. This tool also documents all SaaS solutions and associates the individuals with access to each solution. This approach grants us a complete overview of all access rights within the organization. On a monthly basis, the security officer audits this list, identifying and flagging any entries that warrant removal. This structured and diligent process maintains a secure, efficient, and transparent approach to access rights within IXON.

Control measure I2: Internal security audits

Category	Threat types	Additional reading
Intermediate People	Misconfigurations Security policy violations Unpatched vulnerabilities	ISO/IEC 27002:2022 - Section 5.35 IEC 62443-4-2:2019 - Section 6.10 NIST SP 800-53A

Objective

Implement a regular internal security audit process to assess the organization's adherence to policies and identify risks and areas for improvement. The audit process should validate the effectiveness of existing security controls, ensure compliance with applicable regulations and standards, and demonstrate a commitment to cybersecurity.

Implementation guidance

To conduct effective internal security audits, consider the following key components:

- a. **Training:** Ensure that the people performing the internal audit are appropriately trained. Internal auditors should be unbiased and critical.
- b. **Planning:** Develop an audit plan outlining the scope, specific security controls to be evaluated, methodologies to be used, resources required, and a timeline for the audit. Ensure that tasks are divided in a way that the internal auditors do not encounter a conflict of interest (e.g. auditing their own work). Note that subsequent audits may focus on different aspects of the organization.
- c. **Execution:** Carry out the audit according to the plan. Review the organization's security policies, procedures, and documentation to ensure alignment with industry best practices and regulatory requirements.
- d. **Reporting:** Create a detailed report that documents the results, highlights security risks or improvement opportunities, and provides recommendations for remediation.
- e. **Follow-up:** Prioritize and implement the recommended remediation actions, collaborating closely with the organization's IT and security teams. Conduct a follow-up assessment to confirm that the findings have been addressed.

IXON's approach

We have an internal audit team consisting of four members from different departments (Sales, Finance, IT). In pairs, they perform quarterly internal audits. Each audit has a different scope or "theme", e.g. Password management or intra-departmental communication. They cover this theme from every angle (written documentation, international standards, industry best practices) and conduct interviews with employees. In doing so, they document all risks and improvement opportunities. This report is discussed with the security team, who score each risk and decide on remediation or improvement projects.

Control measure I3: Employee screening

Category	Threat types	Additional reading
Intermediate People	Corporate espionage Fraud Insider threats	ISO/IEC 27002:2022 - Section 6.1 IEC 62443-2-1:2010 - Section 4.3.3.2 NIST SP 800-12

Objective

Implement a process for background checks for prospective employees to verify their credentials, qualifications, work history, and identify potential red flags, while complying with applicable laws and regulations.

Implementation guidance

Consider the following key steps when conducting effective employee background checks:

- a. Determine the scope: Base the scope of the background check on the specific requirements of the job role and the organization's risk tolerance. You may want to include common elements like employment history verification, education verification, criminal record checks, and reference checks.
- b. Comply with regulations: Make sure the background checks comply with applicable laws and regulations. Do not request more information than you need.
- c. Obtain consent: Obtain consent and authorization from the applicant before conducting a background check, ensuring that the consent is informed and voluntary.
- d. Evaluate results: Carefully review and evaluate the background check findings, considering any potential red flags in the context of the job role.

IXON's approach

IXON, as a EU-based organization, must comply with all regulations regarding background checks. Generally speaking, we look at an applicant's publicly available education and work history and may request a reference from a previous employer. Depending on the level of seniority of the job role, we may include more verification steps.

Control measure I4: Hardware handling

Category	Threat types	Additional reading
Intermediate People	Data leakage Hardware-based attacks Physical theft or tampering	ISO/IEC 27002:2022, Section 5.11 + 7.8 IEC 62443-4-1:2018 - Section 12.5 NIST SP 800-53 PE

Objective

Develop a policy for managing your physical assets during their entire lifecycle to help reduce theft, unauthorized access, and damage.

Implementation guidance

Consider the following key components when developing a hardware handling policy:

- a. Asset inventory: Keep a current list of all your hardware assets, grouped by importance and sensitivity. Give extra security and monitoring to those of higher value.
- b. Access control: Limit access to hardware assets based on job roles. Use physical access controls [CM B8] and track who has access to high-value assets.
- c. Commissioning: Set up guidelines on how to configure newly acquired hardware. Ensure no hardware is issued before it has been configured to specifications.
- d. Maintenance and patches: Set up routines for regular hardware maintenance. This should include timely updates and patches to fix security issues [CM B10].
- e. Disposal and decommissioning: Create a process for securely getting rid of deprecated hardware assets. Make sure to back up sensitive data and/or wipe it when necessary.

IXON's approach

At IXON, we use a SaaS solution to manage an inventory of all hardware storing sensitive data. Our most critical assets are securely stored in designated areas. Each new piece of hardware is configured by our service desk, which enables disk encryption, installs antivirus software, updates the operating system, and registers the device.

The installed antivirus software also automatically updates the device's software and generates alerts for detected security issues. Lastly, our service desk ensures the safe decommissioning of unused hardware by completely erasing all data from hard disks.

Control measure I5: Security governance

Category	Threat types	Additional reading
Intermediate People	Compliance violations Inadequate response to incidents	ISO/IEC 27002:2022, Section 5.2 and 5.37 IEC 62443-4-1:2018 - Section 5.4 NIST SP 800-53

Objective

Create a security responsibility (governance) plan that assigns responsibilities of all security-related tasks to individuals within the organization, fostering a culture of shared responsibility and accountability.

Implementation guidance

To effectively formalize security responsibilities within the organization, consider the following steps:

- a. Identify key roles: Identify roles within the organization that have a direct or indirect impact on security, including IT, security, management, operations, and other departments interacting with sensitive data and systems.
- b. Identify security tasks: Identify security-related tasks that are crucial for meeting or maintaining security objectives (similar to the activities of CM B3).
- c. Define responsibilities: Using the security roles and tasks as input, define the specific security responsibilities and expectations for each person.
- d. Document: Document the defined responsibilities in a formalized plan, distribute the information to relevant personnel and make it available to stakeholders. Ensure employees receive sufficient training and guidance on their responsibilities.

IXON's approach

We maintain a document detailing the responsibilities for each role. Employees may be part of several roles and then have responsibilities belonging to each of these. Roles include:

- Security Officer
- Internal auditor
- Team lead
- Quality manager
- etc.

Responsibilities are written down as simply as possible and are used to onboard new employees. As an example, see the following Job description for the role "DevOps Engineer":

- ✓ Maintaining the IXON Cloud infrastructure
- ✓ Design and development of infrastructure code and configurations

Control measure I6: Change management

Category	Threat types	Additional reading
Intermediate Processes	Misconfiguration of systems Unauthorized changes Vulnerabilities during updates	ISO/IEC 27002:2022 - Section 5.37 and 8.32 IEC 62443-2-1:2010 - Section A.3.3.5.3.12 NIST SP 800-53 CM-3

Objective

Create a clear process for managing changes to processes and documents. Change management is a structured approach to manage modifications to any existing cybersecurity documents, processes, or policies within an organization. This approach aims to minimize potential risks, ensure consistency and maintain audit trails.

Implementation guidance

To effectively manage changes, consider implementing the following practices in your change management process:

- a. Standardized process: Change Management should follow a clearly defined, standardized process, which includes stages such as proposal, review, approval, implementation, communication, and review post-implementation.
- b. Review and approval: Every change proposal must be reviewed by the responsible stakeholders. They will assess the change, including its potential impact on the organization's security and whether it aligns with the organization's goals.
- c. Ensure version control: Consider version control for all security documentation, including a record of document revisions, authorship, and approval history.
- d. Backout plan: Think about a contingency plan in case a change causes unanticipated negative effects. This is especially important when making changes to critical security policies and processes.

IXON's approach

We have a formalized procedure to manage changes in a controlled manner within the management system of IXON. It defines the scope of change management (what changes undergo this process) and the steps taken. The changes are drafted in hidden documents in our intranet. All documents contain:

- ✓ An owner, responsible for keeping it up to date and reviewing it at least twice a year.
- ✓ A version history table with details who changed what at which time.

When a change is made, the document owner requests approval from a reviewer with adequate know-how. The reviewer can approve or reject the changes before they are published.

Control measure 17: Supplier reviews

Category	Threat types	Additional reading
Intermediate Processes	Insider threats from subcontractors Supply chain attacks Third-party data breaches Vendor risks	ISO/IEC 27002:2022 - Section 5.19 and 5.20 ISO/IEC 27036-2:2014 - All IEC 62443-2-1:2010 - Section 4.2 NIST SP 800-161

Objective

Establish a formal process for assessing supplier cybersecurity practices and integrate this into the organization's overall supply chain risk management strategy.

Implementation guidance

To effectively manage cybersecurity risks in the supply chain, consider implementing the following practices in your supplier review process:

- a. **Supplier selection:** Develop policy requirements and criteria for selecting suppliers, based on the sensitivity of the data they have access to. Evaluate suppliers' adherence to industry standards, such as ISO/IEC 27001 and IEC 62443, as well as their history of security incidents and breaches.
- b. **Contractual agreements:** Incorporate cybersecurity requirements into contractual agreements with suppliers, including clauses related to data protection, incident response, and regular security assessments. Ensure suppliers understand their obligations and are held accountable for meeting these requirements.
- c. **Regular reviews:** Conduct regular reviews of supplier cybersecurity practices, assessing their security policies, procedures, and controls. This may involve on-site audits and remote assessments.
- d. **Incident reporting:** Create a process for monitoring and reporting security incidents involving suppliers. Include guidelines for communication and escalation, as well as requirements for suppliers to notify the organization of any incidents that may impact their products or services.

IXON's approach

All suppliers undergo a thorough risk assessment, an initial evaluation before engagement, and periodic performance evaluations. Suppliers are rated based on their importance to daily operations and the sensitivity of information they store, which ranges from 'critical' to 'none'. This informs the frequency of performance reviews, from yearly to less frequently.

If a supplier has potential to influence the confidentiality, integrity, and availability of IXON's sensitive information and personally identifiable information, they will be subject to an additional information security evaluation.

Control measure I8: Information hygiene

Category	Threat types	Additional reading
Intermediate Processes	Data breaches Malware infections Phishing attacks Social engineering attacks	ISO/IEC 27002:2022, Section 5.17 + 8.1 IEC 62443-4-2:2019 - Section 7.3 + 7.6 NIST SP 800-61

Objective

Develop practices and promote habits that maintain the health and security of information systems, including minimizing unnecessary data collection and storage, maintaining data accuracy, and securing data against unauthorized access or alteration.

Implementation guidance

To promote good information hygiene habits among employees, consider implementing the following policies:

- a. Email and communication security: Establish guidelines for safe email and communication practices, such as not opening suspicious attachments, verifying the sender's identity before responding to emails, and using secure communication channels for sensitive information.
- b. Safe web browsing: Provide guidance on safe web browsing habits, such as using reputable websites, enabling browser security features, and being cautious when downloading files or clicking on links. If possible, block unsafe websites on the organization's network.
- c. Data handling and storage: Implement data handling and storage policies to ensure that sensitive information is stored securely and is accessible only to authorized personnel. This may include encryption, secure file transfer protocols, and data access controls [CM I10].
- d. Clear screen: Ensure employees lock their devices with a password, pin code or biometrics whenever they are not present. Configure this to happen automatically after a period of inactivity.
- e. Clean desk: Ensure that employees clean up their working area when they are away (e.g. at the end of a working day). Store confidential information (such as contracts, intellectual property and blueprints) in a safe place.
- f. Teleworking & BYOD: Establish policies for employees working remotely from home and for employees using personal devices for work. Consider enforcing the same requirements as for organization-owned devices.

Control measure I9: Software Development Lifecycle

Category	Threat types	Additional reading
Intermediate Processes	Injection attacks Privilege escalation Software vulnerabilities	ISO/IEC 27002:2022, Section 8.25 IEC 62443-4-1:2018 - Section 7 (SD) + 8.4 NIST SP 800-160

Objective

Establish and maintain a Secure Software Development Lifecycle (SDLC) policy that incorporates security best practices at each stage of development.

Implementation guidance

A general software development lifecycle consists of a number of phases, including design, development, testing and deployment. Consider the following measures for each phase:

- **Design:** Create clear security requirements for software applications and systems, aligning with industry standards and best practices. Take special care with areas related to authorization, encryption and administrator privileges.
- **Development:** Ensure software adheres to secure coding practices, such as input validation, output encoding, and least privilege principles, to reduce the likelihood of vulnerabilities and exploits. Train developers in secure coding techniques and provide them with tools to facilitate secure development practices. Require a peer review process, where each software change has to be approved by a knowledgeable colleague. Consider separating development, testing and production environments, to ensure changes do not affect running systems.
- **Testing:** Conduct thorough security testing during the development lifecycle, such as penetration testing and vulnerability assessments. Automate security tests wherever possible. Validate that security requirements have been met.
- **Post-deployment:** Consider methods to monitor correct performance of the software and machines. Enable alerting to respond to stalled software. Collect logs for troubleshooting and auditing purposes.

IXON's approach

IXON's software development lifecycle is rooted in Agile practices with SCRUM teams, where security and customer value is prioritized. To maintain the security integrity of the software, IXON employs OWASP SDLC principles at all stages of development and maintains documents on security standards. Code is developed and tested in separate virtual environments, mimicking production settings, and upon completion, is reviewed by another developer for quality assurance before deployment. IXON ensures data security with strict access controls, data encryption standards, and constant authorization checks. Software modifications and patches occur as needed, tracked in the GIT versioning system. After deployment, the software is monitored in real-time for possible issues.

Control measure I10: Network and Data Encryption

Category	Threat types	Additional reading
Intermediate Technology	Data breaches Eavesdropping Man-in-the-middle attacks	ISO/IEC 27002:2022 - Section 8.24 IEC 62443-4-2:2019 - Section 8.5 NIST SP 800-175B

Objective

Implement network and data encryption to protect sensitive information from unauthorized access, tampering, and eavesdropping during transmission and storage.

Implementation guidance

To develop a network and data encryption strategy, consider the following steps:

- a. Identify sensitive data: Determine the types of data that require protection, such as intellectual property, customer information, and confidential business data. Assess the sensitivity level of the data based on the potential impact of unauthorized access, modification, or disclosure.
- b. Encrypt data in transit: Implement encryption protocols, such as Transport Layer Security (TLS) or Secure Shell (SSH), to protect data transmitted over networks. Ensure that secure encryption settings are used and that outdated or insecure protocols are disabled.
- c. Select encryption algorithms: Choose appropriate encryption algorithms and key lengths that provide a suitable level of security for each data type. Consult the latest resources and standards, such as OWASP<linkje>.
- d. Encrypt data at rest: Apply encryption methods, such as file or disk encryption, to protect sensitive data stored in databases, file systems, and employee devices.
- e. Key management: Establish a key management process to generate, distribute, store, and revoke cryptographic keys securely. Ensure that cryptographic keys are securely stored.

IXON's approach

At IXON, we have documented which cryptographic methods and algorithms are used for each system and information type based on *Classification of Confidentiality*. Methods include:

- Hashing (e.g. PBKDF2 and Argon2id)
- Authentication (e.g. RSA)
- Encryption (e.g. Bitlocker for Windows, Filevault for MacOS, etc.)
- TLS Ciphers (e.g. AES-256)

Control measure I11: Backups

Category	Threat types	Additional reading
Intermediate Technology	Data loss Hardware failures Human errors Natural disasters Ransomware attacks	ISO/IEC 27002:2022 - Section 8.13 IEC 62443-4-1:2019 - Section 11.5 + 11.6 NIST SP 800-34

Objective

Develop and implement a backup plan to protect critical data and systems against data loss and other threats, ensuring the continuity of their operations.

Implementation guidance

To create an effective backup plan, consider the following steps:

- a. Identify critical data and systems: Determine which data and systems are critical to the organization's operations and prioritize them for backup. This may include customer data, intellectual property, manufacturing data, and system configurations.
- b. Backup frequency and retention: Establish the frequency of backups and the retention period based on the criticality of the data, the organization's risk tolerance, and any regulatory or compliance requirements. For example, critical data may require daily or even hourly backups, while less critical data may be backed up weekly or monthly.
- c. Backup storage locations: Store backups in (multiple) secure locations to minimize the risk of data loss due to a single point of failure. This may include a combination of onsite, offsite, and cloud storage options, ensuring that at least one copy is stored offsite to protect against localized threats such as natural disasters.
- d. Backup encryption: Encrypt backup data to protect it from unauthorized access, both during transmission to the storage location and while at rest. Use strong encryption algorithms to ensure the confidentiality and integrity of the backup data [CM I10].
- e. Backup testing: Regularly test the backup process to ensure that the data can be successfully restored in the event of an incident. This may involve restoring a sample of the backup data to a test environment and verifying its integrity and usability.

IXON's approach

At IXON, we have made an inventory of all sources of data that are essential to ensure business continuity in the event of a disaster. Each of the data sources has their own backup policy, based on how often that data changes and the limits of the software/solution used. Critical IXON Cloud data is backed up every 4 hours, stored offsite. If a backup is unsuccessful or incomplete, an alert is generated and sent to our operations team. Each month, a backup is tested to ensure that the data is valid.

Control measure I12: External communication

Category	Threat types	Additional reading
Fundamental	Compliance issues Inadequate information sharing Miscommunication errors	ISO/IEC 27001:2013, Section 7.4 IEC 62443-3-3:2019 - Section 9.5 NIST SP 800-53 - PL

Objective

Develop a systematic approach to external communication that ensures clear understanding and shared responsibilities between your organization, its customers, and suppliers. Clear and consistent documentation can strengthen relationships with partners, clarify security responsibilities, and reduce the risk of miscommunications that could lead to security vulnerabilities. It can also enable you to be proactive to customer questions by having documentation readily available.

Implementation guidance

- a. **Communication procedures:** Establish procedures for external communication, ensuring that all correspondence is clear, concise, and appropriately secured. This includes emails, phone calls, reports, and other forms of communication.
- b. **Content and responsibility:** Specify what information should be shared, with whom, and who in your organization is responsible for communicating this information. This will help ensure consistency and prevent the release of sensitive data.
- c. **Standard documentation:** Develop standard templates for common communication items, such as security incident reports, system updates, and policy changes. Standard documents can streamline the communication process and ensure all necessary details are included.

We recommend starting with creating the following documents. They should be clear, easy to understand, and accessible to all customers and stakeholders.

- ☒ **Machine Connectivity:** Detail how the machines should be connected to external networks. It should provide guidelines for secure configuration, data transmission, and maintenance, ensuring that customers have the information needed to integrate your machines securely.
- ☒ **Supplier Security:** Provide a list of suppliers you use. Define the security requirements for suppliers, detailing the expected security measures and protocols they must adhere to. This document should be provided to all suppliers to clarify your security expectations and reinforce shared responsibilities. Include a
- ☒ **Terms of Service:** Outline the terms and conditions of your services, including security practices and data handling procedures, as well as legal rights and obligations.

Control measure I13: Automated vulnerability assessment

Category	Threat types	Additional reading
Intermediate Machine	Configuration weaknesses Exploitable software flaws Security misconfigurations Unpatched software vulnerabilities	ISO/IEC 27002:2022 - Section 8.8 IEC 62443 4-1:2018 - Section 9.4 NIST SP 800-37 and NISTIR 8011

Objective

Implement a process for conducting automated vulnerability assessments to identify, prioritize, and remediate potential weaknesses in information systems and networks.

Implementation guidance

To conduct effective automated vulnerability assessments, consider the following steps:

- a. **Assessment tools:** Choose appropriate automated vulnerability assessment tools that can scan machines and other network-based devices for potential weaknesses. These may include IP-cameras and routers. The selected assessment tools should support the specific technologies and OS used within the machine and the network devices, and should be able to detect and report on known vulnerabilities, configuration weaknesses, and security misconfigurations.
- b. **Analyze:** Review the results of the assessment to identify, prioritize, and remediate potential weaknesses. This may involve validating the reported vulnerabilities and assessing the potential impact on the machine and factory.
- c. **Remediate:** Implement appropriate measures to address identified vulnerabilities, such as applying patches, implementing configuration changes, or deploying compensating controls.
- d. **Reassess:** Regularly repeat vulnerability scans to discover new vulnerabilities and to validate that previous remediations were successful.
- e. **Report:** Generate reports to track progress and demonstrate compliance with internal policies and external regulations. Share these reports with relevant stakeholders, such as senior management, to ensure that they are informed of the organization's vulnerability management efforts.

Advanced Control Measures

Control measure A1: Competencies and Training

Category	Threat types	Additional reading
Advanced People	Insider threats Misconfigurations Phishing attacks Social engineering attacks	ISO/IEC 27002:2022 - Section 6.3 ISO/IEC 27021:2017 IEC 62443-2-1:2010 - Section 4.3.2 NIST SP 800-50

Objective

Develop and implement a training program that addresses the specific competencies required for different roles within the organization. By developing and implementing this training program, organizations can build a resilient and knowledgeable workforce that is equipped to face cybersecurity challenges.

This control measure builds on the training foundation created in CM B1.

Implementation guidance

To develop a policy that ensures sufficient and relevant competencies and training, consider the following key steps:

- a. Define competencies: Define the specific competencies required for different roles within the organization.
- b. Assess needs: Conduct an assessment of the organization's current cybersecurity capabilities and identify skill and knowledge gaps that need to be addressed.
- c. Encourage learning: Management should stimulate everyone in the organization to continue improving themselves, especially in security-related topics. This can be done with a study budget or hours that employees can allocate for training.
- d. Training programs: Identify appropriate training programs that address the defined knowledge gap, considering factors such as the target audience, learning outcomes, and available resources.
- e. Iterate and adjust: Evaluate the effectiveness of the training programs and make adjustments as needed to further strengthen competencies and knowledge to ensure they continue to meet the organization's needs and the evolving cybersecurity landscape.

IXON's approach

At IXON, improving competencies and providing relevant security training is a significant priority across multiple roles. In a Training Plan, the security-focused competencies necessary for all roles in our organizations are listed.

For example, our CEO, as the overseer of all operations, maintains a leadership role in reinforcing the importance of security, working in tandem with our Security Officer who is the primary authority on IT vulnerabilities, threat detection, and implementation of security controls. To stay updated with evolving security practices, the Security Officer is mandated to undergo training on the latest security issues and best practices, at a minimum of 10 hours every quarter. A study budget is available for this. This data is recorded in Training Records to be able to review everyone's progress.

Control measure A2: Threat intelligence

Category	Threat types	Additional reading
Advanced People	Emerging threats Zero-day exploits	ISO/IEC 27002:2022 - Section 5.7 NIST SP 800-30

Objective

Ensure a proactive approach to monitoring emerging threats and vulnerabilities to better protect the organization from harm. Gathering threat intelligence is essential for timely response, maintaining an adaptive security posture, and ensuring regulatory compliance. The quality of this intelligence will influence the effectiveness of other Control Measures.

Implementation guidance

To effectively watch for threats and to stay informed about the latest cyber risks, consider the following methods and resources:

- a. Threat Intelligence platforms: Organizations can gather threat intelligence themselves, but making use of platforms that provide real-time information about emerging threats, vulnerabilities, and attack trends is more feasible. Threat intelligence may be gathered from independent providers or advisors, government agencies or threat intelligence groups.
- b. Security news and blogs: Monitor security-focused news outlets and blogs for articles about new threats, and other developments in the cybersecurity landscape.
- c. Industry reports and publications: Review regular reports on the state of cybersecurity (in manufacturing) produced by cybersecurity organizations and research institutions.
- d. Security conferences and events: Attend industry conferences, webinars, and other events to learn from experts in the field and stay updated on new developments in cybersecurity.
- e. Internal sharing and collaboration: Encourage employees to share relevant security news, research, and insights within the organization to foster a culture of shared responsibility and awareness.

IXON's approach

In addition to the security team being subscribed to mailing lists and news outlets regarding new vulnerabilities and security patches, IXON is partnered with commercial, independent and governmental cybersecurity organizations to stay informed about the latest developments in the cybersecurity field. Emerging threats are subjected to a risk assessment, with which we can prioritize changes to code and policies.

Control measure A3: Incident response testing

Category	Threat types	Additional reading
Advanced Processes	Inadequate response to incidents	ISO/IEC 27002:2022 - Section 5.27 IEC 62443-2-1:2020 - Section 4.3.4.5 NIST SP 800-61

Objective

Establish a process for conducting regular incident response tests to validate the effectiveness of their incident response plan (CM B5) and identify areas for improvement.

Implementation guidance

To conduct effective incident response testing, consider the following steps:

- a. Define testing objectives: Determine the objectives of the incident response test, such as evaluating the organization's ability to detect, respond to, and recover from a specific type of cybersecurity incident, or assessing the effectiveness of communication and coordination between different teams during an incident.
- b. Develop test scenarios: Create realistic test scenarios that simulate potential cybersecurity incidents relevant to the machine builder industry. These scenarios should be based on the organization's risk assessment and take into account unique industry-specific threats, such as attacks on industrial control systems, intellectual property theft, or supply chain disruptions.
- c. Conduct the test: During the execution of the test, observe and evaluate the organization's response to the simulated incident, including the effectiveness of communication, coordination, decision-making, and technical capabilities.
- d. Analyze results: Analyze the results of the incident response test to identify areas for improvement in the processes. This may involve reviewing test observations, conducting debriefing sessions with involved stakeholders, and comparing the organization's response to established best practices.
- e. Update incident response plan: Based on the findings from the incident response test, update the organization's incident response plan to address identified gaps. This may involve revising policies, procedures, roles, and responsibilities, as well as implementing new technologies or training initiatives.

IXON's approach

We regularly simulate table-top exercises to test our Incident response plan (CM B5). This ensures that all security staff involved in potential security incidents are familiar with the necessary steps in order to save valuable time during a breach. To prepare simulations, the Security Officer creates realistic scenarios involving specific aspects of the organization that are under attack. The response to the simulated incident by the security staff is observed and measured for effectiveness, speed, and adherence to protocols. The results are discussed and improvements are incorporated into the plan.

Control measure A4: Maturity Assessment

Category	Threat types	Additional reading
Advanced Processes	Ineffective cybersecurity measures Misaligned security priorities Undetected vulnerabilities	ISO/IEC 27002:2022 - Section 5.36 and 8.8 IEC 62443-4-1:2018 - Section 4.2 NIST Cybersecurity Capability Maturity Model

Objective

Conduct regular maturity assessments of an organization's cybersecurity program. The results should be documented and integrated into the organization's overall risk management and cybersecurity strategy.

Implementation guidance

To conduct an effective maturity assessment, consider the following steps:

1. **Define assessment scope:** Determine the scope of the maturity assessment, focusing on critical aspects of the organization's cybersecurity program, such as policies, procedures, technologies, and training initiatives. Take into account machine builder-specific challenges such as industrial control systems, intellectual property protection, and supply chain security.
2. **Select assessment model:** Choose a maturity assessment model that is appropriate for the organization's size, complexity, and industry such as the NIST Cybersecurity Capability Maturity Model (C2M2).
3. **Conduct the assessment:** Evaluate the organization's cybersecurity program against the selected maturity assessment model, identifying strengths and areas for improvement. This may involve reviewing policies, procedures, and other documentation, as well as conducting interviews with stakeholders and performing technical assessments of security controls.
4. **Analyze results:** Analyze the results of the maturity assessment to determine the organization's overall cybersecurity maturity level. Identify gaps between the organization's current state and the desired maturity level, and prioritize areas for improvement based on risk, impact, and feasibility. Where applicable, implement these changes into the Risk Treatment plan [CM B7].

Control measure A5: Business Continuity Plan

Category	Threat types	Additional reading
Advanced Processes	Hardware or software failures Natural disasters Supply chain disruptions	ISO/IEC 27002:2022, Section 5.29, 5.30 IEC 62443-2-1:2010, Section 4.3.2.5 NIST SP 800-34

Objective

Establish a business continuity plan (BCP), which includes the identification, assessment, and prioritization of critical business functions, as well as strategies for maintaining their operation during disruptions.

Implementation guidance

To develop and implement an effective BCP, consider the following steps:

- a. Business impact analysis: Carry out a business impact analysis (BIA). This analysis should find important business functions, check their weak spots, and decide how long each function can be down before it becomes a problem. The BIA should also include the financial, operational, and reputational impacts of disruptions.
- b. Recovery strategies: Develop recovery strategies for each critical business function, outlining the actions required to restore operations as soon as possible. These strategies may include alternative processes, backup systems, or the use of external resources, such as cloud-based services or third-party providers.
- c. Incident response plan: Integrate the BCP with the organization's incident response plan [CM B5], ensuring that roles and responsibilities are clearly defined and that the appropriate personnel are trained to respond to disruptions effectively.
- d. Communication plan: Establish a communication plan that outlines how information will be shared with stakeholders, including employees, customers, suppliers, and regulators, during and after a disruption. This plan should also include procedures for providing regular updates on the status of recovery efforts.

IXON's approach

IXON's Business Continuity Plan is aimed at a swift and efficient recovery of IT services and data in case of a major incident. The plan takes into account various major incidents including power failures, natural disasters, and security breaches which may disrupt operations at IXON's headquarters, hardware production, or compromise digitally stored information and cloud services.

Should the headquarters become unavailable, employees are equipped to continue work remotely using resources stored on cloud servers. In case of a disruption in the hardware production process, safeguards such as large components stocks, dual-sourcing, fire prevention controls, and trained personnel are in place to limit impact on customer orders.

Control measure A6: Endpoint Detection & Response (EDR)

Category	Threat types	Additional reading
Advanced Technology	Data exfiltration Insider threats Malware infections Unauthorized access	ISO/IEC 27002:2022 - Section 8.1 + 8.7 + 8.16 IEC 62443-4-2:2019 - Section 10.4 NIST SP 800-53 SI-3

Endpoint Detection and Response (EDR) is a category of security tools that monitor end-user hardware devices across a network (known as endpoints) for suspicious activities. It collects information from these devices and uses advanced analytics to spot patterns that might indicate a threat. If a threat is found, EDR tools can take various actions, like disconnecting the affected device from the network or stopping harmful processes.

Objective

Implement an Endpoint Detection & Response (EDR) solution to continuously monitor, detect, and respond to cybersecurity threats targeting endpoints. The EDR tool should be able to deal with complex threats.

Implementation guidance

To effectively implement an EDR solution, consider the following steps:

- a. **Select an EDR solution:** Pick an EDR tool that matches your organization's specific needs, risk profile, and device infrastructure. Think about the tool's ability to find and respond to complex threats, how easy it is to install, how well it can grow with your needs, and how well it works with your existing security tools.
- b. **Deploy the EDR solution:** Set up the EDR tool on all devices in your organization, like desktop computers, laptops, servers, and mobile devices. Make sure the EDR tool is set up correctly to maximize effectiveness and avoid interruptions to regular activities.
- c. **Integrate with existing security tools:** Ensure the EDR tool works well with your other security tools and systems, like Security Information and Event Management (SIEM) or alerting systems. This will help you respond in a coordinated way to any threats you find.
- d. **Update and maintain:** Keep the EDR solution up-to-date with the latest threat intelligence, malware signatures, and software patches. Use official (community) rules and thresholds for monitoring and detecting potential security incidents. These rules and definitions should be updated automatically.

Control measure A7: Security Information and Event Management (SIEM)

Category	Threat types	Additional reading
Advanced Technology	Data breaches Insider threats Unauthorized access	ISO/IEC 27002:2022 - Section 8.15 IEC 62443-4-2:2019 - Section 10.3 NIST SP 800-137

A SIEM is a system that continuously collects and analyzes data from across the network to spot abnormal activity or potential threats. If it finds something suspicious, it alerts the security team for quick action. It also maintains a record of security incidents, aiding in meeting various cybersecurity regulations.

Objective

Implement a Security Information and Event Management (SIEM) system to monitor, analyze, and manage security events and incidents in real-time. The SIEM system should be configured to collect and correlate data from multiple sources, enabling organizations to detect, respond to, and prevent potential security threats more effectively.

Implementation guidance

To deploy and maintain an effective SIEM system, consider the following steps:

- a. Identify data sources: Determine the sources of security-related data that the SIEM system will collect and analyze. These may include log files, network traffic data, and system events from various devices, applications, and infrastructure components. Authorization and administrator events are especially important, to ensure login attempts and admin overrides are monitored.
- b. Choose a hosting option: Depending on the specific sources and needs of the organization, you may need to deploy SIEM components yourself, or purchase an all-in-one SaaS-solution.
- c. Deploy SIEM components: Implement (or purchase) the necessary SIEM components, such as log collectors, event processors, and analytics engines. Make sure the SIEM system can grow and change with the organization's needs.
- d. Configure correlation rules: Develop and configure correlation rules that enable the SIEM system to identify patterns and relationships between security events, which may indicate potential security incidents. These rules may be based on community rulelists or use AI to detect anomalies.
- e. Incident response integration: Integrate the SIEM system with the organization's existing incident response processes and tools. This may involve configuring automated alerts, response actions, or communication channels.

IXON's approach

In order to quickly detect any anomalies in our network or services, IXON collects logs and metrics generated by its servers whenever possible. The logs are collected in a central, secure platform where they can be accessed by authorized users. The logs are collected by

a SIEM system that evaluates the information against a large dataset of industry-leading rules.

Control measure A8: Penetration testing

Category	Threat types	Additional reading
Advanced Machine	Data breaches Exploitation of vulnerabilities Industrial control system attacks Unauthorized access	ISO/IEC 27002:2022 - Section 8.8 IEC 62443-4-1:2018 - Section 9 NIST SP 800-115

Objective

Conduct regular penetration tests on industrial machines to identify exploitable vulnerabilities and to test security controls. It's important to note that penetration testing should only be performed with prior consent and should be done in a way that doesn't disrupt the normal operations of the organization. Penetration tests can be conducted internally or by independent security firms.

Implementation guidance

A penetration test typically consists of the following phases.

- a. **Planning and preparation:** Define what should be tested and accomplished in the test. This includes pinpointing which systems will be under scrutiny, the techniques to be employed, and the extent of the simulated attack. Gathering preliminary data such as system configurations and network structures will also aid in identifying potential soft spots. The following steps are usually outsourced to a competent third party:
 - **Reconnaissance:** The tester collects as much information as possible about the target system. Techniques such as network and port scanning, along with vulnerability scanning, can be used to gain an understanding of the system, discover potential entry points, and highlight vulnerabilities.
 - **Attack:** This is the phase where the penetration tester tries to exploit the identified vulnerabilities to gain access to the system.
 - **Post-attack analysis:** Once the system has been breached, it is evaluated what a real attacker could do. This could range from stealing sensitive data, disrupting the system, or even establishing a foothold for further attacks.
 - **Reporting:** A report is created that describes the results of the penetration test, detailing the actions taken, vulnerabilities discovered, successful exploits, and suggestions for improvements.
- b. **Remediation:** Based on the report, the identified vulnerabilities should be fixed. This could involve anything from updating software, tweaking configurations, enhancing firewall rules, or even replacing systems that are too vulnerable. If vulnerabilities can not be fixed, they need to be accepted in the risk assessment process.
- c. **Retesting:** After the vulnerabilities have been addressed, it's important to retest the system to ensure the fixes are effective.

Pentesting should be an ongoing process, as new vulnerabilities can be introduced over time. Incorporate penetration tests into the Activities Planning (CM B3) so they are not forgotten.

IXON's approach

IXON regularly conducts penetration tests on hardware, software and infrastructure components by partnering with a professional security firm. Together with the security firm, a penetration test is planned, where we define which component requires testing, as well as the scope and goals of the tests and any additional security questions or concerns.

If possible, tests are performed on test environments/hardware. Otherwise, it is stressed upon the pentester that they should not take actions that could actively disrupt or break normal operations of the organization or its services. After execution of the test, a detailed report of discovered vulnerabilities is delivered. We consider the vulnerabilities as improvement opportunities by incorporating them into our Risk treatment plan for remediation.

Control measure A9: Logging & monitoring

Category	Threat types	Additional reading
Advanced Machine	Advanced persistent threats Data breaches System performance issues Unauthorized access	ISO/IEC 27002:2022 - Section 8.5 IEC 62443-3-3:2013 - Section 4.2.4 NIST SP 800-92

Objective

Establish a logging and monitoring policy to detect, analyze, and respond to machine-related cybersecurity threats and system performance issues. Ensure there is no excessive logging of personal and sensitive data with regards to privacy concerns.

Implementation guidance





To implement an effective logging and monitoring policy, consider the following steps:

- a. **Set up logging:** Configure hardware and applications so they generate and save log data in a secure, private and standardized way. This involves setting up log generation parameters, specifying storage locations, and setting up access controls to protect them from unauthorized changes. Do not log sensitive or personal information without a strictly necessary and legal reason. Ensure log entries are timestamped.
- b. **Log retention:** Formulate a policy for log data retention and disposal, keeping in mind all legal, regulatory, and operational requirements. Decide how long to keep each type of log data and determine safe ways to delete sensitive information. Consider setting up a centralized platform that collects logs from various systems. This ensures that logs can be readily accessed in case of an incident to save valuable time during the investigation of evidence trails.
- c. **Monitoring:** Consider the need for collecting and analyzing system parameters, such as CPU, memory, disk size, etc and machine-specific data, such as production data, error states, OEE, etc. Only collect data that is actually useful and legally allowed in order to keep it manageable.
- d. **Analysis:** Set up a process for studying log, system and machine data and making reports to support the policy's goals. This might involve using automated tools to monitor logs, deciding when to make reports, and what to do when problems are found in the logs. Ensure compliance with international Privacy standards when processing data, such as the GDPR.

Appendix A: Control measures overview



Control Measures

	People	Processes	Technology	Machine
 Advanced	A1 - Competencies & Training A2 - Threat intelligence	A3 - Incident response testing A4 - Maturity assessment A5 - Business continuity plan	A6 - Endpoint detection & response (EDR) A7 - Security Information and Event Management (SIEM)	A8 - Penetration testing A9 - Logging & Monitoring
 Intermediate	I1 - Access rights management I2 - Internal security audits I3 - Employee screening I4 - Hardware handling I5 - Security governance	I6 - Change management I7 - Supplier review I8 - Information hygiene I9 - Software development lifecycle	I10 - Network & Data encryption I11 - Backups	I12 - External communication I13 - Automated vulnerability assessment
 Basic	B1 - Onboarding & Awareness B2 - Secure offboarding B3 - Security activities planning	B4 - Document policies B5 - Incident response plan B6 - Incident reporting B7 - Risk treatment B8 - Physical access control	B9 - Firewalls & Antivirus B10 - Patch management B11 - Password management	B12 - Physical machine access B13 - Secure configuration
 Fundamentals	F1 - Management commitment	F2 - Scope and goals	F3 - Risk assessment	F4 - Network segmentation

Appendix B – IXON’s Risk Assessment template

Asset	Owner	Threat	Cause	Consequence	Likelihood score	Impact score	Risk (L x I)	Existing controls	Risk decision
IXON Cloud platform - centralized logging	R&D Software Architect	Incomplete data	Reaching the capacity of our centralized logging application	Alerts are not sent, incidents are not detected (as quickly)	3	4	12	Weekly capacity monitoring by Operations	Reduce
Personnel - Security Officer	CEO	Permanent unavailability	There is no replacement for this person	Important decisions regarding security can no longer be made. Tasks related to the ISO27001 are no longer performed. Security monitoring and vulnerability detection may be affected	1	4	4	The CEO, department leaders and the Process manager can take over tasks	Accept
Computers, laptops & mobile phones employees	User of the device	Theft/loss	Inadequate physical protection	Data may be accessed	2	2	4	IXON HQ is protected by an intrusion prevention and detection system	Accept

An explanation of terms used in this table can be found on the next page.

Explanation of columns:

Asset: The actual item that is being threatened

Owner: Who is responsible for identifying and managing the asset and associated risks

Threat: Type of attack

Cause: How could the threat materialize

Consequence: Explain what would happen in layman's terms if the threat is exploited

Likelihood score: Calculate or estimate how likely it is to happen (score of 1 to 5)

Impact score: Calculate or estimate how severe the impact is (score of 1 to 5)

Existing controls: Describe the currently implemented rules/guidelines/technical controls that help reduce the likelihood or impact of the threat

Risk decision: Choose if the risk is acceptable and if not, what to do with it (reduce, insure, transfer, etc.)