Author(s): Simola, Jussi; Takala, Arttu; Lehkonen, Riku; Frantti, Tapio; Savola, Reijo

Title: The Importance of Cybersecurity Governance Model in Operational Technology Environments

Year: 2024

Version: Published version

The Importance of Cybersecurity Governance Model in Operational Technology Environments

Jussi Simola, Arttu Takala, Riku Lehkonen, Tapio Frantti and Reijo Savola
University of Jyväskylä, Finland

jussi.hm.simola@jyu.fi
arttu.h.takala@jyu.fi
riku.p.Lehkonen@jyu.fi
tapio.k.frantti@jyu.fi
reijo.m.savola@jyu.fi

Abstract: There is a common will to unify regulation in the Western world regarding overall security, including cybersecurity. European cyber security regulations aim to create a foundation and guidelines for international standards in various industries and the operation of critical infrastructure. Protected critical infrastructure is a common goal for Western allies. Allies of NATO and EU member states mainly support the anti-aggression policy in Europe. The unstable situation in the world forces states to find solutions that represent the thoughts of the allies. Defending common values is crucial when the purpose is to protect critical infrastructure and vital functions in societies. The research will demonstrate the industrial needs of IT/OT-related cybersecurity governance. The study analyzes EU-level cybersecurity requirements and how those requirements affect standardization regarding cybersecurity governance in the operational technology environment. There will be four primary governance levels: Political, Strategical, Operational and Tactical. Many criminal state-linked operators do not care about international agreements or contracts. Some rogue states have even taken to inciting violations of international agreements. We cannot trust the loose contracts between states anymore. The research will find the main challenges concerning the cybersecurity governance of the industrial organizations that use operational technology-related technology in their daily businesses. We have seen that Information and Operational Technology are based on something other than similar threats and risk basements. Operational Technology related threats threaten the cyber-physical ecosystem where anomalies affect the physical world, so operational functions of equipment, devices, sensors, components, and production lines are interrupted. As a result, continuity management and supply chain management are compromised. The study's primary purpose is to describe the cybersecurity governance elements of the OT environment for enhancing situational awareness. Standardizing the cybersecurity level among industrial stakeholders requires EU member states to have a national cybersecurity strategy that follows main EU-level guidelines. Despite the EU member states' implementation level of the regulation, the EU-level cybersecurity requirements obligate companies to take steps to solve future cybersecurity challenges.

Keywords: Governance Model, Cybersecurity Strategy, Supply Chain Management, Continuity Management

1. Introduction

The research will enhance the understanding of the challenging situation that affects critical infrastructures' operational technology environment. The research will find the main challenges concerning the cybersecurity governance of the industrial organizations that use operational technology-related technology in their daily businesses. The basic describtion of governance means the atmosphere where something must steer and govern. Suppose we look at the practise of daily business. Many challenges and factors steer the business environment. Business Continuity and supply chain management are crucial elements that must be beneficial and strengthened, especially in critical sectors. Decision makers with public safety actors must create workable environments where enterprises can work in a way that supports the national overall security strategy.

We live in a digitalized and networked world where the cyber ecosystem depends on energy availability and supply chain. Cybersecurity governance management is crucial at all levels of global security, where state-level public safety actors and companies in different vital business sectors are connected via stakeholders. The EU member states and allies of the Western military alliance NATO recognize the need for collaboration and integration of “codes” in cybersecurity strategy plans. Collaboration requires common situational awareness capabilities at all levels. Continuity management does not mean separating things from critical infrastructure protection. Public safety organizations need to collaborate with the companies. Therefore, we need a coherent system that allows public safety organizations to gather required safety critical information for the decision-support mechanism.

IT/OT Cybersecurity governance more than just standardization, protocols, or guidelines. It is much more than that. Cybersecurity governance is a part of the overall corporate governance management system. It is also a part of company strategy, working culture, and daily routines. Employees are not separate parts of Cyber-physical ecosystems. Governance requires cohesion between the crucial elements of the cyber-ecosystem. The importance of the well-organized governance model is emphasized according to the size of the company.

CSG (Cybersecurity governance of operational technology in sector-connected smart energy networks) project significantly increases the effectiveness and efficiency of cybersecurity of smart energy networks and other operational technology. The project aims at considerable cost savings and scalability through enhanced incident management, data gathering, and Artificial Intelligence based automation.

The first research paper of the CSG project (Simola, et al.2023) concentrates on the research environment. The second paper concentrates on technical information-sharing requirements of the Operational technology environment. The third paper continues and describes the crucial elements affecting the supply chain and continuity management. Enhancing cyber situational awareness is the European Union's common aim in the OT/ICS environment.

2. Central Concepts

2.1 Operational Technology Governance

Regarding NIST (2023), Operational Technology governance should consist of the policies, procedures, and processes for managing the organization's regulatory, legal, risk, environmental, and operational requirements. Enterprises in the industrial environment should establish an effective OT cybersecurity governance capability, develop a process, and assign responsibilities and accountability to appropriate roles in the corporate risk management function (NIST, 2023). According to the NIST (2023), the Operational Technology Governance process includes the following minimum requirements. a) The OT cybersecurity policy is established and communicated. b) OT cybersecurity roles and responsibilities are coordinated and aligned with the internal roles and external partners. c) legal and regulatory requirements regarding OT cybersecurity, including privacy, are understood correctly and managed. d) The cybersecurity risks are integrated into corporate risk management processes (NIST, 2023). According to the NIST, features of the Cybersecurity Governance strategy may consist: Accountability frameworks – Decision-making hierarchies - Defined risks related to business objectives – Mitigation plans and strategies – Oversight processes and procedures NIST.

2.2 Operational Technology as a Part of Critical Infrastructure

Operational Technology systems consist of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that aid together to achieve an objective (e.g., manufacturing, transportation of matter or energy) (NIST, 2023). Business sectors are interconnected industrial sectors of critical infrastructures that are often based on "system of systems” architecture. Electrical power transmission and distribution grid industries use distributed SCADA control technology to operate interconnected and dynamic systems consisting of a large amount of public and private utilities and rural cooperatives for supplying electricity to customers (NIST, 2023).

Supervisory control and data acquisition (SCADA) systems are used in distribution systems that integrate data acquisition with data transmission systems and Human Machine Interface (HMI) software by providing a centralized monitoring and control system for process inputs and outputs. SCADA systems collect information from the field to the control center and display the information with graphics and texts. Operators may monitor and control an entire system from a central location almost in real time (NIST, 2023). Individual systems enable controlling operations or tasks, which can be automatic and can be performed by operator commands. Used hardware consists of a control server, communications equipment, and remote terminal units (RTUs) and/or (Programmable Logic Controller (PLCs) that control local processes by actuators and monitor sensors. The software of the communications hardware allows information and data sharing and is programmed to inform what parameter ranges are acceptable and what measures launch when process variables are out of range (NIST,2023). An intelligent electronic device (IED) is a protective relay, that may communicate directly to the control server. IEDs provide a direct interface to control and monitor equipment and sensors (NIST, 2023).

2.3 C2 and SOC

Command and Control Center refers to operative control processes and procedures of military actions. Functionalities and work tasks changed to the Computer Emergency Response Center, which later changed to the Security Operations Center, including different functionalities and actions that control, monitor, and supervise customers’ networks (Vielberth et. al. 2020).

2.4 Cyber-Physical Systems (CPS)

According to the (NIST, 2017) Cyber-physical systems (CPS) consist of smart systems that include engineered interacting networks of physical and computational components. Interconnected and integrated systems provide new functionalities to improve quality of life and enable technological advances in critical areas, such as personalized health care, emergency response, traffic flow management, smart manufacturing, defense and homeland security, and energy supply and use. In addition to CPS, (Industrial Internet, Internet of Things (IoT), machine-to-machine (M2M), smart cities, and others) describe similar or related systems and concepts. OT/ICS industrial environment very often consists of SCADA (Supervisory control and acquisition) for control and monitoring functions. There is a significant overlap between concepts of CPS and IoT, such that CPS and IoT are sometimes used interchangeably; therefore, the approach described in this CPS Framework should be considered equally applicable to IoT (NIST, 2017). Figure 1 illustrates, the interconnection between systems of systems-level thinking and human factors is crucial in designing cyber-physical systems.

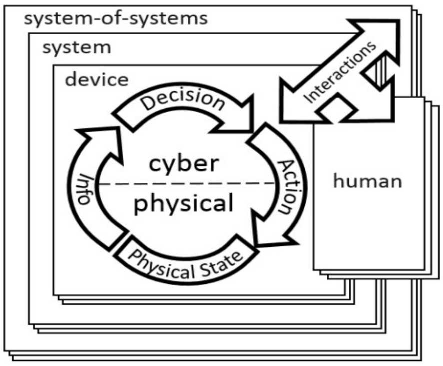

Figure 1: System of Systems Thinking in Cyberphysical Systems (NIST, 2017)

The managing level must guide enhanced measures into their business strategy. If different management levels do not include business-related cybersecurity requirements in their strategic plans, it will reduce the efficiency of the daily working processes. Decision-makers must take into account the industry and organizational culture to achieve a common understanding level. Cybersecurity training about the business vision and mission is important because if humans do not internalize and apply the requirements for the daily work, business continuity is at risk of interruption.

2.5 Situational Awareness

It has been said that humans are the weakest factors in the business environment. As Mica Endsley argued, it is important to create common understanding and mental model within the team and between the team members for reducing overlapping work (Endsley, 1995). According to Endsley (1998), “Situation awareness is the perception of the elements in the environments within the volume of time and space, the comprehension of their meaning, and the projection of their status in the near future.” Perception is an essential ability in the industrial environment. The formation of situational awareness requires several elements that are connected to each other. Humans cannot process large volumes of data, quickly and consistently. Flexible autonomy should provide a smooth, simple, seamless transition of functions between humans and the system. Regulations of the European Union set new requirements for the formation of cyber situational awareness. Human or automated systems are essential factors that enhance communication methods, procedures, information gathering, and sharing. Mechanisms for that are under development.

2.6 Information Exchange

Information-sharing mechanisms are essential for the formation of situational awareness. EU Member states should have a common model to share different kinds of information. **Figure** 2 below illustrates four popular types of information sharing (MITRE, 2018)

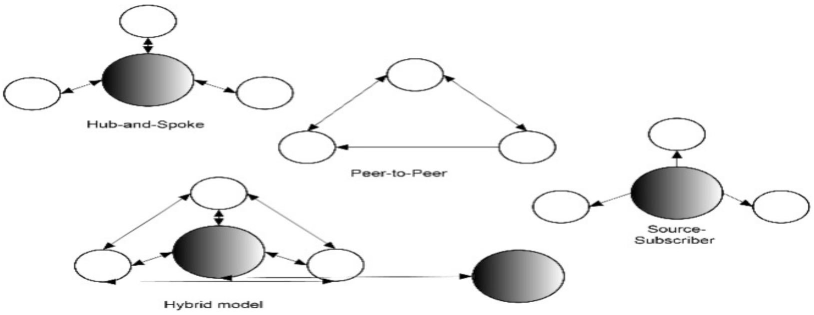

Figure 2: Information sharing models modified from MITRE, (2018)

Few existing cybersecurity information-sharing architectures exist. The fourth hybrid model is the combination of others.

Hub-and-Spoke - Several data producers and consumers share information with each other, but instead of sending it directly, the information is sent to a central hub, which then handles dissemination to all the other spokes as appropriate. This model can be viewed as being like e-mail distribution lists, where a sender provides a message to a mailing list service, which then forwards the message to all list members.

Peer-to-peer - A group of data producers and data consumers organize direct relationships with each other. Members share directly with each other in a mesh pattern. The group may have a single governing policy, but all sharing exchanges are between individuals.

Source-Subscriber - A single entity publishes information to a group of consumers. This is a common model in commercial environments, where the data source is a vendor, and the subscribers purchase access to the vendor's information. This is also a common model for free alerts from some authoritative source (MITRE, 2018).

2.7 Supply Chain and Continuity Management

The supply chain ecosystem may consist of public and private sector entities (e.g., acquirers, suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers) (NIST,2022). Enterprises depend on the supply chain to provide products and services to enable the enterprise to achieve its strategic and operational objectives. Identifying cybersecurity risks throughout the supply chain is complicated by the information asymmetry that exists between acquiring enterprises and their suppliers and service providers. The NIST Special Publication (2022) describes the practices and controls for Cybersecurity Supply Chain Risk Management (C-SCRM). It applies both information technology (IT) and operational technology (OT) environments and is inclusive of IoT. Like IT environments that rely on ICT products and services, OT environments rely on OT and ICT products and services, with cybersecurity risks arising from ICT/OT products, services, suppliers, and their supply chains (NIST,2022).

3. Background of the Research

3.1 Cybersecurity Cooperation between the United States and the European Union

According to (ENISA, 2013) the US and the EU will enhance cooperation on Cybersecurity. In practice, this means, for example, that the Cybersecurity & Infrastructure Security Agency (CISA, 2023) and the European Union Agency for Cybersecurity (ENISA) will enforce collaboration. The arrangement consists of the following points:

To build cyber situational awareness and capacity to enhance cyber resilience, including facilitating participation as third-state representatives in specific EU-wide cybersecurity exercises or training and the sharing and promotion of cyber awareness tools and programs.

Best practice exchange in the implementation of cyber legislation, including on key cyber legislation implementation such as the NIS2 Directive (European Parliament, 2022), incident reporting, vulnerabilities management, and the approach to sectors such as telecommunications and energy.

Information sharing to increase common situational awareness: including a more systematic sharing of knowledge and information in relation to the cybersecurity threat landscape to increase the common situational awareness to the stakeholders and communities and in full respect of data protection requirements. A work plan will operationalize the Working Arrangement and regular reporting at the EU-US Cyber Dialogues is foreseen (ENISA, 2023).

3.2 Common Approach to Critical Infrastructure Protection and Resilience

Defining critical infrastructure sectors has been one of the main aims of the Western world in terms of securing overall security (DHS, 2013; DHS, 2015). Maintaining cyber resilience has been an essential goal in the protection work. It has also been seen in the European Union that an overall cybersecurity strategy as a part of the security strategy is needed. Finland is a new full member of NATO, and it that w for the security culture even though Finland has been an important "support member" for years.

3.3 Towards the Common European Cybersecurity Regulation

The European Union will unify all member states' cybersecurity-related master plans (ENISA, 2023; European Parliament, 2022). These plans will change the almost the whole atmosphere because the given period for the implementation is short. Organizations' business priorities and objectives are crucial elements.

Overall management of continuity management requires the implementation of Public or private related organizations' cybersecurity guidelines. the Cyber Resilience Act (CRA) supports the goals of the NIS2, and NIS2 supports the aims of the CER Cyber Resilience directive. CRA sets requirements for the manufacturing process of digitalized products, industrial companies, and cyber security training methods for the personnel and management of security operations (European Commission, 2022a, 2022b,2022)

We have seen that there is an increasing challenge in the development of loyalty between the EU member states (Gyori, 2023). Some states do not care enough about the trust and overall security of the Western world. Therefore, state leaders need more supervision on how to reach the goals. Critical Infrastructure protection requires a common understanding of situational awareness in developing cybersecurity strategy as a part of the other security plans.

The challenges in energy sector have proven how important is it to create common-specific frameworks for energy sectors. Energy distribution is crucial in critical infrastructure protection and energy supply chain management. Ensuring that energy power and distribution systems work is crucial for a sustainable and stable energy supply.

The regulations are partly obliged to ensure that European Union member countries deploy and standardize cybersecurity-related regulations. A member state must recognize EU-level regulation, and the ultimate responsibility for compliance lies with organizations. Critical infrastructure must be protected against cyber-physical threats, and humans, technology, and processes must be ensured for continuity management. Cybersecurity is an uncontrolled situation if there is no operational-level understanding and connection about the cybersecurity requirements in processes, technical solutions, and human actions between the organizations and within the working groups or employees.

3.4 Relationship Between the Cybersecurity Governance Model and Regulatory Framework

The European Commission has set the security of supply for critical infrastructure protection because the aim is to protect and maintain the continuity of supply around the European Union. Member States must identify the critical entities for the sectors regarding the CER directive (European Commission, 2020b). The list of essential services is the basis for the risk assessment and identifying the critical entities (European Commission, 2020b). The focus is to strengthen the EU's resilience against online and offline threats, from cyberattacks to crime, risks to public health, or natural disasters. Energy supply and distribution protection forms occasional basement to all critical sectors.

The project research is based on the testbed work and the regulatory factors that support each other. There are many opinions in scientific discussions about what cybersecurity governance means. Others think that it means only business or technical level aspects, but others expand the understanding of the meaning of the overall cybersecurity governance. The ENISA (2023b) defines Cybersecurity Governance by Savas and Karatas (2022) as follows*:* "Operation of decision-making processes" which increase and ensure "participation, transparency, and accountability in taking measures related to cyberspace together with the mechanism of international agreements, strategies, laws, measures, regulations, and standards that interlock in the best way". There are several definitions in academic publications, but this selected form follows the main line of the definitions. ENISA uses four upper-level stages that steer the implementation procedures at the national level. As ENISA (2023b) argues, European Union member states have been required to adopt a National Cybersecurity Strategy. The order of the concepts may differ, but those governance steps by ENISA (2023b) are as follows.

a) The political level consists of political processes, Roles, responsibilities, and legal measures including international cooperation. Public-private partnerships (PPP) help build connections between the public and private sectors and ensure the implementation of actions responding to the industry´s needs. Enhanced cybersecurity governance requires a common international language for cyber defence. Legal measures should be inclusive and have general validity to ensure that all institutions, organizations, and related stakeholders are committed to the National cybersecurity strategy, its governance model, and the implementing actions. b) The strategic level of governance consists of the strategy itself, coordinating and its implementation and risk identification and mitigation. The crucial point of that is connected to the processes of designing the strategy and designing its governance mode to ensure continuity and coherence. Strategic elements of identifying and mitigating risks require strong cooperation and collaboration between the actors. Stakeholders such as political actors supported by consults and working groups are essential factors, for example, in budgeting and resource allocation. According to the strategic elements of risk identification and mitigation, a coherent approach across all government entities and critical infrastructure operators should be aimed for. A common approach for risk identification and mitigation, which is coherent across the different actors, promotes information-sharing and enhances cooperation. c) Operational governance comprises elements of raising awareness by using efficient incident response and information sharing and exchange. (ENISA, 2023). Operational governance focuses on developing cybersecurity across all sectors of a nation´s society, economy, and government. Specialized bodies of the stakeholders, such as Computer Security Incident Response Teams (CSIRTs) or Computer Emergency Response Teams (CERTs), government officials, and consulting and training bodies are actively involved in the set-up and execution of this governance layer. Society and population are essential parts of this layer. The goal of enhancing situational awareness consists of training, education, and community building within the complete population. Proactive and reactive functionalities of Incident response mechanisms and information sharing by CSIRTs or CERTs are crucial elements in this layer. d) Technical and tactical levels consist of international standards, technical guidelines and recommendations, and the use of technology, tools, and certification schemes. Technology and technical elements are part of the implementation of the strategy. Definitions of the standards and their use form the basis for this layer. Tools and certification schemes will enhance technical governance. NIS2 directive consists of crucial views on the importance of certification and highlights the member states to require essential and important entities to certify ICT products, ICT services, and processes under European certification schemes (ENISA, 2023b). Those four levels affect the whole cybersecurity environment. In addition to this, we must think on technical, processes, and human levels, which are sources of vulnerabilities but also possibilities to enhance the cyber ecosystem.

NIS2 will set new standards for all companies despite the organization's size, but it concentrates on bigger ones. There will be sanctioned requirements (European Parliament, 2022), but some policies are less mandatory. Small-size enterprises cannot avoid regulatory requirements because the European Union has decided that every enterprise must consider regulations regardless of member countries' situation of enactment. EU member states must also create a mechanism to ensure cybersecurity for small and medium-sized organizations. It is essential that small enterprises understand how cybersecurity requirements affect their business in the future and change their business culture (Schreider, 2019). Vendors are in a crucial position to remain cybersecurity level enough to fulfill the supply chain-related requirements that are under implementation. According to the European Parliament (2022), each Member State "should ensure that national cybersecurity strategy provides for a policy framework for enhanced coordination within that Member State between its competent authorities under this Directive and those under Directive (EU) 2022/2557 in the context of information sharing about risks, cyber threats, and incidents as well as on non-cyber risks, threats and incidents, and the exercise of supervisory tasks. The competent authorities should cooperate and exchange information without undue delay, in relation to the identification of critical entities, risks, cyber threats, and incidents as well as in relation to non-cyber risks, threats, and incidents affecting critical entities, including the cybersecurity and physical measures taken by critical entities as well as the results of supervisory activities carried out about such entities" (European Parliament, 2022).

4. Research Approach and Research Methodology

The laboratory environment at the University of Jyväskylä generates new information about cybersecurity-related technical issues. Components, devices, and software from stakeholders form a new base of knowledge for the governance model development work. The created and tested use cases create crucial technical obstacles that generate added value for the operators of the ICS environment. Combining information from sector-based enterprises, analysis of external requirements, and results from the testbed generate a suitable solution for the actors of the critical infrastructure. Results from the testbed produce a new knowledge base into divided classes that are possible to connect to the different kinds of external and internal requirements that have been considered in the analysis of the ICS-related environment. In this research, we have used the Delphi method (Garson, 2012). Professional team members also have skills in analyzing the research data.

According to (Nunamaker, Minder Chen, and Purdin, 1991), the multi-methodical approach consists of four case study research strategies: theory building, experimentation, observation, and systems development research based on systematic analysis of gathered data. We have used Yin´s case study research strategy (Yin,2014), which concentrates on only limited research problems and questions. In this research, our focus is on the question: What are crucial factors and elements that may set obstacles for enhanced continuity management and supply chain as a part of cyber situational awareness in the OT/ICS environment? We have used official literature sources such as official publications and academic publications in this work. In this research, we concentrate on external industry-specific supply chain-related cybersecurity requirements. Figure 3. illustrates how the basement of the CSG-project has been constructed.

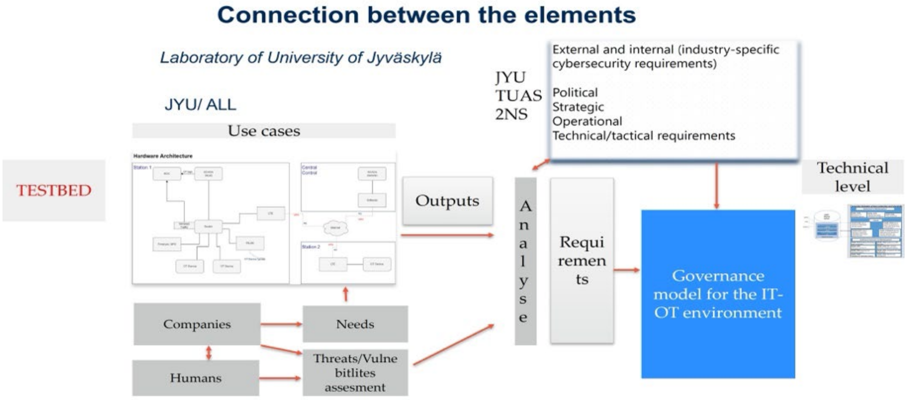
Connection between the elements
Laboratory of University of Jyväskylä
JYU/ ALL
Use cases
Hardware Architecture
TESTBED
Outputs
JYU
TUAS
2NS
External and internal (industry-specific cybersecurity requirements)
Political
Strategic
Operational
Technical/tactical requirements
Technical level
A n a l y s e
Requi remen ts
Governance model for the IT-OT environment
Companies
Needs
Humans
Threats/Vulne bitlites assesment

Figure 3: Basic Elements from the CSG testbed

From a governance viewpoint, a systematic system of system-level thinking requires splitting organizational functions into several layers as follows in Figure 4 (Pöyhönen & Lehto, 2020). The figure illustrates how decision-making levels Strategic, operational, and technical are connected to the comprehensive system view from an organization's cybersecurity environment.

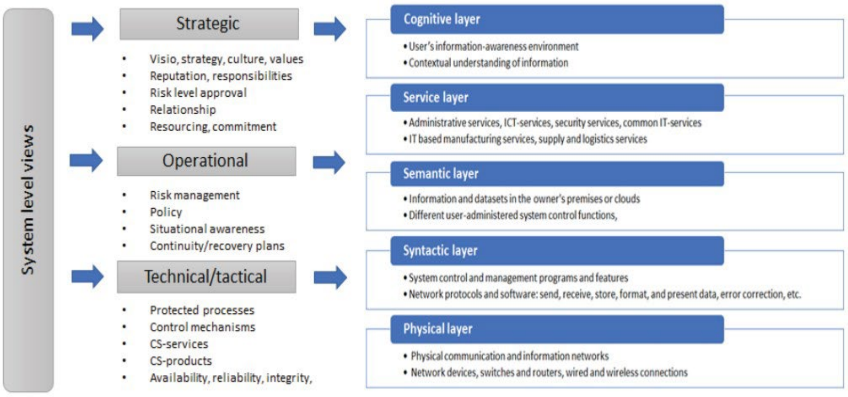
System level views
Strategic
Visio, strategy, culture, values
Reputation, responsibilities
Risk level approval
Relationship
Resourcing, commitment
Operational
Risk management
Policy
Situational awareness
Continuity/recovery plans
Technical/tactical
Protected processes
Control mechanisms
CS-services
CS-products
Availability, reliability, integrity,
Cognitive layer
User's information-awareness environment
Contextual understanding of information
Service layer
Administrative services, ICT-services, security services, common IT-services
IT based manufacturing services, supply and logistics services
Semantic layer
Information and datasets in the owner's premises or clouds
Different user-administered system control functions,
Syntactic layer
System control and management programs and features
Network protocols and software: send, receive, store, format, and present data, error correction, etc.
Physical layer
Physical communication and information networks
Network devices, switches and routers, wired and wireless connections

Figure 4: Organizations cyber governance and trust-based Cyber security architecture framework (Pöyhönen & Lehto, 2020)

Continuity management and protecting the supply chain are linked to all layers. The national cybersecurity strategy and directives combined affect all layers. The main aim is to enhance cybersecurity situational awareness. It is not possible without analysing the requirements of the Cognitive, service, semantic, syntactic, and physical layers. Third-party services, components, equipment, devices, but also human resources set a fundamental framework in the industrial environment.

5. Findings

System of system -level thinking is crucial when the main goal is to achieve a common understanding of the situation concerning the cybersecurity requirements in the industrial environment. The continuity management and supply chain obstacles set challenges for daily businesses. Vital functions are dependent on workable continuity and supply chain management. A gap between the understanding of operational business reality and the created strategy on the enterprise's board level forms a crucial problem in the formation of cyber situational awareness. Therefore, every internal organizational stage should have a logical and coherent information-sharing mechanism and methods that have been created in the same way. Information sharing and exchange problems are emphasized from the internal world to the external world and vice versa.

At the strategic level, there must be deeper cooperation between the European Union member states. National Computer Emergency Response agencies must create a mechanism that allows real-time information sharing between countries. Common language means common “language”, taxonomy, and procedures for how to act against the weak signals of cyberattacks. It requires more funding possibilities to create a straight way to collaborate. It is not enough that the Cyclone group meets once a month. The formation of situational awareness requires that national authorities exchange information in real time with the EU-level cybersecurity authority and cybersecurity authorities of other member countries.

At the operational level, the construction of the shared information is more important. It is not relevant to share data that does not create added value. Actors of the operational level should have the competence to understand how technology communicates and how humans communicate. Perception of the events is a crucial factor in this. NIS2 requires coherent information sharing about the vulnerabilities; proactive monitoring features are also required to be connected to the European Union strategy-based cybersecurity requirements (European Parliament, 2022). SCADA systems are core cyber-physical systems that are connected to the other equipment in the industrial environment. Therefore, the content of the gathered data from the physical OT environment is essential. Reporting requirements and continuity management requirements are connected to the process of maintaining situational awareness. Security operations centers (SOC) service providers have an official-based mandate to exchange information that is needed to protect critical infrastructure. Another challenge may arise from contracts that have been made with the enterprises. How effectively does the National Cybersecurity Authority monitor the agreements and maturity level of the supervision procedures? External auditing processes are needed concerning the SOC´s features and capabilities. Despite that, It is possible that Artificial Intelligence-based solutions may generate added value, especially when gathering information from outside the OT environment. Comparing data to existing threat information and by using OSINT tools and other relevant sources, it is possible to create information that is stated at the strategy level and another stakeholder at the operational level.

At the tactical and technical level, enterprises must take into account the security features of the components, system suppliers, and equipment manufacturers, as Figure 5 illustrates. It also illustrates how vulnerabilities are connected to every stage of the use of products and services. CRA directive from the European Commission (2022) will set new certification requirements for digital components and software. From the viewpoint of the supply chain that is essential when the aim is to manage risks and vulnerabilities. OT-related enterprises have to implement their procedures, processes, technologies, and human interactions in a way that the European Union regulations require.

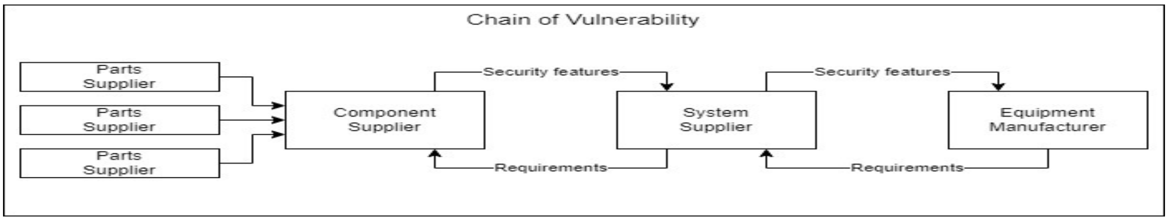

Figure 5: Chain of vulnerability

Figure 6 illustrates how the use of standards is connected to the cyber-physical industrial environment and will enhance continuity management as a part of the cybersecurity governance model. The protection of the supply chain requires ongoing auditing concerning the products and services. Analyzing the 3rd party risks, the essential problem is related to the agreements. How to ensure that 3rd party service and product providers achieve and follow the requirements that partners have been obliged to? Standardization is the answer, but NIS2 requires human resource training, Intentional and unintentional human errors caused by lack of training. The Cyber Resilience Act requires the production and designing of CE-marked products that fulfill cybersecurity requirements, and service providers have to have the same level of understanding about the cybersecurity requirements.

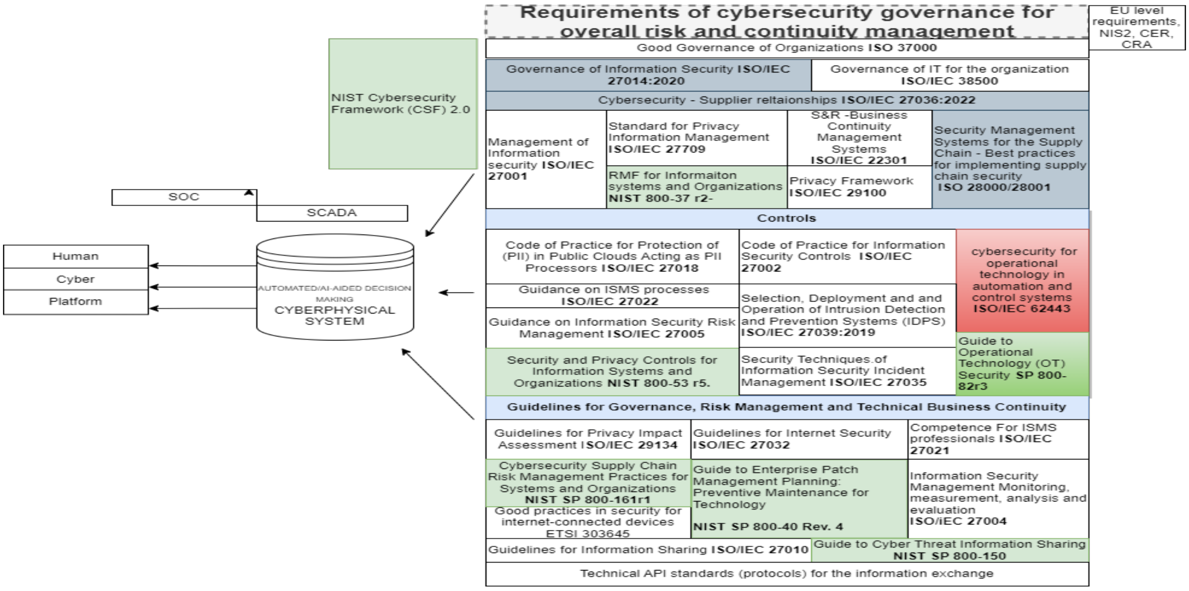
Requirements of cybersecurity governance for overall risk and continuity management
EU level requirements, NIS2, CER, CRA
Good Governance of Organizations ISO 37000
Governance of Information Security ISO/IEC 27014:2020
Governance of IT for the organization ISO/IEC 38500
Cybersecurity - Supplier reltaionships ISO/IEC 27036:2022
Management of Information security ISO/IEC 27001
Standard for Privacy Information Management ISO/IEC 27709
S&R -Business Continuity Management Systems ISO/IEC 22301
Security Management Systems for the Supply Chain - Best practices for implementing supply chain security ISO 28000/28001
RMF for Informaiton systems and Organizations NIST 800-37 r2-
Privacy Framework ISO/IEC 29100
Controls
Code of Practice for Protection of (PII) in Public Clouds Acting as PII Processors ISO/IEC 27018
Code of Practice for Information Security Controls ISO/IEC 27002
cybersecurity for operational technology in automation and control systems ISO/IEC 62443
Guidance on ISMS processes ISO/IEC 27022
Selection, Deployment and and Operation of Intrusion Detection and Prevention Systems (IDPS) ISO/IEC 27039:2019
Guidance on Information Security Risk Management ISO/IEC 27005
Guide to Operational Technology (OT) Security SP 800-82r3
Security and Privacy Controls for Information Systems and Organizations NIST 800-53 r5.
Security Techniques.of Information Security Incident Management ISO/IEC 27035
Guidelines for Governance, Risk Management and Technical Business Continuity
Guidelines for Privacy Impact Assessment ISO/IEC 29134
Guidelines for Internet Security ISO/IEC 27032
Competence For ISMS professionals ISO/IEC 27021
Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations NIST SP 800-161r1
Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology NIST SP 800-40 Rev. 4
Information Security Management Monitoring, measurement, analysis and evaluation ISO/iEC 27004
Good practices in security for internet-connected devices ETSI 303645
Guidelines for Information Sharing ISO/IEC 27010
Guide to Cyber Threat Information Sharing NIST SP 800-150
Technical API standards (protocols) for the information exchange
NIST Cybersecurity Framework (CSF) 2.0
SOC
SCADA
Human
Cyber
Platform
AUTOMATED/AI-AIDED DECISION MAKING
CYBERPHYSICAL SYSTEM

Figure 6: Requirements of the Cybersecurity Governance

6. Discussion and Conclusion

The international regulation indicates that cybersecurity should be coordinated from the EU level to the EU member countries. It has been seen that differences between member countries' regulations affect cohesion. Member states must create implementation with other countries. Similar implementation of regulation between countries and the sectors of critical infrastructure is important in terms of maintaining situational awareness of the Western world. We need to understand how states share information in cross-boarding events. Industrial environments are not separate entities from other factors in the cyber ecosystem. How to react to different kinds of cyber threats is crucial; therefore, a cybersecurity governance model must also be implemented between the nationalities. The CyClone group mechanism (European Parliament, 2022) supports maintaining common situational awareness and understanding but requires a much more holistic understanding. It is not enough that there is an upper-level hub to share information. Crucial are practical functionalities and processes. Information-sharing mechanisms must be created in a standardized way. A common taxonomy and information-sharing methods must mean the same things to all stakeholders at different stages. If the EU member state does not follow common regulations and guidelines, information exchange does not support the protection of critical infrastructure. The common Governance model for the industrial environment should be based on standards related to business processes, technologies, human resource management, risk management, and standardized information-sharing methods. The management of 3rd party-related risks in supply chain management is essential for business continuity. Every member state must use the same basement in its management of the supply chain. Critical infrastructure protection requires that possibilities of vulnerabilities in internet-connected devices, equipment, and software are minimized.

Acknowledgments

The research was supported by Business Finland (grant number 10/31/2022) and the University of Jyväskylä.

References

CISA (2023) Cybersecurity Practices for Industrial Control. Systems. https://www.cisa.gov/sites/default/files/publications/Cybersecurity_Best_Practices_for_Industrial_Control_Systems.pdf

Department of Homeland Security (2013) National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience.

Department of Homeland Security (2015) Emergency Services Sector-Specific Plan.

ENISA (2023a) Cisa and Enisa to enhance their cooperation. https://www.enisa.europa.eu/news/cisa-and-enisa-enhance-their-cooperation

ENISA (2023b) Building Effective Governance Frameworks for the Implementation of National Cybersecurity Strategies.

Endsley M. (1995) Towards a theory of situation awareness in Dynamic Systems. Human Factor 37(1)

Endsley M. R.,(1988) "Design and evaluation for situation awareness enhancement." in Proceedings of the Human Factors Society 32nd Annual Meeting, pp. 97-101

European Commission. (2020a) The EU's Cybersecurity Strategy for the Digital Decade. Brussels. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020JC0018

European Commission. (2020b) Proposal for a directive of the European Parliament and of the Council on the resilience of critical entities. COM (2020) 829 final. 2020/0365 (COD). Brussels, 16 December

European Commission. (2022) Proposal for a regulation on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020

European Parliament. (2022) Directive 2022/2555 Network and Information Security (NIS2)

Garson, G. D. (2012) The Delphi method in quantitative research. Asheboro, NC: Statistical Associates Publishers. Available from: https://faculty.chass.ncsu.edu/garson/PA765/delphi.htm, retrieved 24.12.2023.

Gyori, B. (2023) The U.S. says it is concerned about Hungary´s relationship with Russia. Retrieved: February 18, 2023

MITRE (2018) "Trusted Automated eXchange of Indicator Information — TAXII™ Enabling Cyber Threat Information Exchange,"

NIST (2023) NIST Special Publication SP 800-82r3 Guide to Operational Technology Security

NIST (2022) NIST Special Publication SP 800-161r1 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

NIST (2017) NIST Special Publication 1500-201 Framework for Cyber-Physical Systems: Volume 1, Overview

Nunamaker, J., Minder Chen, J. R., & Purdin, T. (1991) Systems development in information systems research. (3), 89-106

Pöyhönen, J., & Lehto, M. (2020) Cyber security: Trust-based architecture in the management of an organization‘s security. In T. Eze, L. Speakman, & C. Onwubiko (Eds.), ECCWS 2020: Proceedings of the 19th European Conference on Cyber Warfare and Security (pp. 304-313). Academic Conferences International. Proceedings of the European conference on information warfare and security

Schreider, T. (2019) Building an Effective Cybersecurity Program, 2nd Edition, Rothstein Associates, Incorporated, Brooksfield. Available from: ProQuest Ebook Central. [19 February 2024].

Simola J., Takala A., Lehkonen R., Frantti T., Savola R. (2023) Developing Cybersecurity in an Industrial Environment by Using a Testbed Environment. 22th European Conference on Cyber Warfare and Security ECCWS-2023. The Hellenic Air Force Academy. Athens, Greece.

Savaş, S., Karataş, S. (2022) Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. Int. Cybersecur. Law Rev. 3, 7–34. https://doi.org/10.1365/s43439-021-00045-4