Architecture Framework for Cyber Security Management

Jouni Pöyhönen and Martti Lehto
University of Jyväskylä, Jyväskylä, Finland

jouni.a.poyhonen@jyu.fi
martti.j.lehto@jyu.fi

Abstract: The smooth operation of contemporary society relies on the collaborative functioning of multiple essential infrastructures, with their collective effectiveness increasingly hinging on a dependable national system of systems construction. The central focus within the realm of cyberspace revolves around safeguarding this critical infrastructure (CI), which includes both physical and electronic components essential for societal operations. The recent surge in cyber-attacks targeting CI, critical information infrastructures, and the Internet, characterized by heightened frequency and increased sophistication, presents substantial threats. As perpetrators become more adept, they can digitally infiltrate and disrupt physical infrastructure, causing harm to equipment and services without the need for a physical assault. The operational uncertainty of CI in these cases is obvious. The linchpin of cyber security lies in a well-executed architecture, a fundamental requirement for effective measures. The framework of this paper emphasizes organizational guidance in cyber security management by integrating the cyber security risks assessment and the cyber resilience process into overall continuity management of organizations business processes.

Keywords: Critical Infrastructure, Architecture Framework, Risks Assessment, Resilience

1. Introduction

The smooth operation of contemporary society relies on the collaborative functioning of multiple essential infrastructures, with their collective effectiveness increasingly hinging on a dependable national system of systems construction. The dependability of this system construction is intricately tied to cyber security, and consequently, the confidence placed in the business processes of organizations integrated into the overall system. Moreover, dependability is interconnected with the usability, reliability, and integrity of data within the operational framework, where cyber threats continuously escalate due to menacing scenarios in the digital realm.

A system of systems (SoS) refers to a compilation of autonomous systems, each capable of independent operation, that collaboratively interoperate to attain additional desired capabilities (Dahmann, 2015). In cyber world Information and Communication Technology (ICT), Industrial Control Systems (ICS), and other Operational Technology (OT) systems as fundamental elements of SoS. Additionally, a comprehensive understanding of users, various processes, and the flow of data and information between these components is crucial for grasping the broader context of the SoS approach.

One of cyber security research areas is to utilize a system of systems (SoS) approach specifically critical infrastructure (CI) protection against harmful attacks and unexpected behaviors. It enables a holistic view of the organization’s cyber security. According to our experiences, SoS is well-suited to cyber security research projects that enhance comprehensive security, including people, processes, and technology, requiring to understand the organization and its operation as well as business processes as a whole system and inseparable parts of the critical infrastructure actors in the cyber world.

The objective of this paper is to outline the structure of a cyber security architecture suitable for an organization, enabling the description of management measures tailored to the organization's needs in all situations of cyber security challenges. The paper integrates risk assessment methodologies with resilience development model to offer organizations a comprehensive approach to continuity management. There is a limited amount of literature discussing papers on organizational holistic cyber security frameworks from this perspective.

2. Dilemma of Known and Unknown Threats

In cases of disturbances, the characteristics of the cyber operational environment include their development at high speed and with far-reaching effects. The organization's cyber operating environment consists of technically complicated structures and widely networked stakeholders, making the whole complex. It is impossible to fully predict its operation. There are also challenges in identifying different forms of cyber-attack and malware. The cyber operating environment is characterized by the speed of change, which requires fast reaction capability - agility, as well as preparation for situations that cannot be fully foreseen in terms of security measures. The examination of operational uncertainty can be based on the probability of occurrence of events (known or unknown) and the evaluation of its impact (known or unknown). The review leads to four possibilities regarding events, which are known known, known unknown, unknown known, and unknown unknown to understand and explain the nature of risk (Kim, 2017). The first three event cases can be covered by using risks assessment methods and processes, but totally unknown possibility cases need to be covered by a different tool. There is a need to increase the overall resilience of the organization's business operations.

Table 1: Simplified operational uncertainty model (adapted from Kim (2017))

	IMPACT	
OCCURRANCE	**Known, Knowns** Risks management process	**Unknown, Knowns** Risks management process
	Unknown, Known Risks management process	**Unknown, Unknown** Resilience enhance process

3. Cyber Threat Intelligence Process

Cyber Threat Intelligence (CTI) encompasses information derived from knowledge, skills, and experience, addressing both cyber and physical threats as well as the entities behind these threats. Its purpose is to aid in the prevention and mitigation of potential attacks and adverse events within the realm of cyberspace. Strategic cyber threat intelligence caters to top-level decision-makers, operational intelligence supports daily decision-making, and tactical threat intelligence targets units requiring real-time information. Within this framework, the cyber threat intelligence process involves system description, cyber threat analysis, vulnerability analysis, cyber-attack model analysis, and impact analysis.

Cyber threat intelligence is often broken down into three subcategories:

- Strategic (who/why) - Broader trends typically meant for a non-technical audience,
- Operational (how/where) - Technical details about specific attacks and campaigns,
- Tactical (what) - Outlines of the tactics, techniques, and procedures of threat actors for a more technical audience.

3.1 System of Systems Description

SoS environment is a collection of systems, each capable of independent operation, that interoperate together to achieve additional desired capabilities (Dahmann, 2015). By the SoS model, organizations may identify all its processes, users, and digital assets. In that sense Martin C. Libicki's structure for the cyber world uses a four-layer cyber world model: physical, syntactic, semantic, and cognitive. Using Libicki's structure and adding service as a fifth layer we have five-layer cyber world model: physical, syntactic, semantic, service, and cognitive (Libicki, 2007; Lehto & Neittaanmäki, 2018).

The physical layer contains the physical elements of communication and information network. The first requirement to build a cyberspace is the physical layer, which comprises all of the hardware required to send, receive, store, and interact with and through cyberspace.

The syntactic layer is formed of various system control and management programs and features which facilitate interaction between the devices connected to the network. This layer can be further broken down into sub-layers, such as the seven layers of the Open System Interconnection (OSI) Reference Model.

The semantic layer is the heart of the entire network. It contains the information and datasets in data warehouses, different large-scale systems, and computer terminals as well as different user-administered functions.

The service layer contains all the ICT-based services which the users use in the network.

The cognitive layer provides the decision makers an information-awareness environment: a world in which information is being interpreted and where one's contextual understanding of information is created including the user's cognitive and emotional awareness.

An organization’s cyber security operations require comprehensive awareness on the system level. The awareness of an organization and decision-makers can be seen as system-level awareness arrangement. Thus, the appropriate awareness supports cyber risk management and, more extensively, the evaluation of an organization’s whole cyber capability. It is possible to integrate an organization’s three decision-making levels into a five-layer cyber structure in order to have a comprehensive system view of that organization’s cyber security environment. It is a system-based approach to the topics and principles of an organization’s comprehensive cyber security. The combination of system views, decision-making levels and an organization’s cyber structure is described in Figure 1 (Pöyhönen & Lehto, 2020).

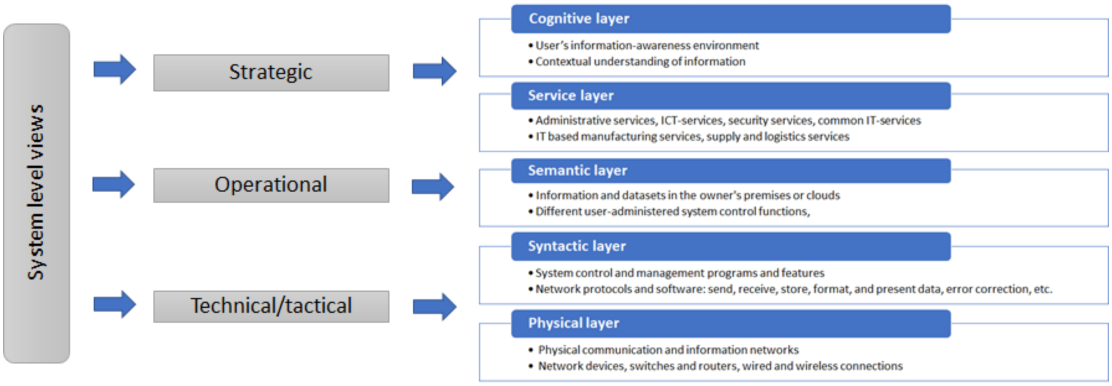
System level views
Strategic
Operational
Technical/tactical
Cognitive layer
• User’s information-awareness environment
• Contextual understanding of information
Service layer
• Administrative services, ICT-services, security services, common IT-services
• IT based manufacturing services, supply and logistics 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 1: System-level view on organizational cyber security in the five-layer cyber world model

3.2 Cyber Threat Analysis

A cyber-threat model compiles information related to potential cyber threats targeting various entities such as a system, enterprise, region, or a critical infrastructure sector. Achieving comprehensive cyber security necessitates a thorough analysis of a SoS against a spectrum of threat events. The analysis of SoS may depend on the creation and utilization of threat scenarios, visually representing potential threats and their resulting detrimental consequences (Bodeau and McCollum, 2018). Defining threats within the cyberspace realm presents challenges, primarily due to the elusive nature of attack origins, the intricate motives driving them, and the unpredictable unfolding of events. This dynamic nature makes addressing these threats an ongoing and intricate task (Lehto, 2013).

To tackle this challenge, a pragmatic threat taxonomy has been formulated, focusing on the motivations of attackers. The factors are: Cyber vandalism, Cyber-crime, Cyber espionage, Cyber terrorism, Cyber sabotage, and Cyber warfare. With typology such as these motives can be reduced to their very essence: Egoism, Money, Information, Destruction, Paralysis, and Power. (Kovanen et.al, 2021a)

Tier 1 Cyber Disruption: In the initial tier, we encounter cyber vandalism, which encompasses acts of cyber anarchy, hacking, and hacktivism.

Tier 2 Cybercrime: Moving up the hierarchy, cyber criminals aim to generate income through fraud or the sale of valuable information.

Tier 3 Cyber Espionage: At the third level, intelligence services engage in cyber espionage to gain economic, military, or political advantages for their entities.

Tier 4 Cyber Terrorism: In the fourth tier, cyber terrorism employs networks in attacks against critical infrastructure systems and their controls (Beggs, 2006).

Tier 5 Cyber Sabotage: At this level, cyber sabotage is an activity conducted by a state actor or state-sponsored group operating below the threshold of war or executing Military Operations Other Than War (MOOTW).

Tier 6 Cyber Warfare: The highest tier, cyber warfare lacks a universally accepted definition but is commonly used to describe state actors' operations in cyberspace. Cyber warfare is part of other military operations, including air, land, naval, and space.

3.3 Vulnerability Analysis

Vulnerability can be defined as an exploitable weakness or deficiencies in a system, device or its design that allow cyber attacker to execute cyber-attacks (Bertino et al., 2010). Vulnerabilities can be divided into those that exist in: People's actions, Processes in the organizations, and Technologies. A thorough vulnerability analysis should encompass all weaknesses or deficiencies present in the SoS environments within an organization.

People refer to the human resources available at the firm's disposal. The people are the ones who do the tasks described in the process. Most cyber security threats are due to employee errors. For example, a report by Kaspersky Lab indicated that employee errors accounted for 90 % of the data breaches (Borner, 2019).

Processes are crucial in defining how the organization's activities, roles and documentation are used to mitigate the risks to the organization's information.

Technology solutions protect against cyber risks that may arise from network vulnerabilities but technology itself contains vulnerabilities (hardware, HW and software, SW). So, technological vulnerabilities are security holes in a system.

3.4 Cyber-Attack Model Analysis

Cyber-attack models delineate the progression of an attack through distinct phases, offering a framework to conceptualize its various elements. However, it's crucial to recognize that the success of an attack doesn't necessarily hinge on completing all phases; rather, the attack's objective shapes its structure. Various cyber security actors have developed diverse cyber-attack models to comprehend the varied goals pursued by cyber attackers. These models are grounded in the targets and objectives of the attacks.

It's noteworthy that not all attacks follow a linear trajectory through all phases for success. In fact, many attacks iterate recursively through the phases, as observed in recent research (Lehto, 2022). These models have evolved based on the motives and objectives driving different cyber-attacks. Typically, cyber-attacks fall into four categories determined by their objectives and targets: Advanced Persistent Threat (APT) attacks, Cyber-Physical Attacks against Critical Infrastructure, Data breach attacks, and Military Cyberspace Operations.

The versatility of these models allows them to be applied to multiple types of attacks. Analysing different attack models within specific environments proves to be a valuable method for comprehensively understanding and describing the primary threats an organization faces, facilitating the assessment of potential impacts.

3.5 Impact Analysis

Widely used Lockheed Martin Cyber Kill Chain (https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html) offer a high abstraction level framework to understand cyber-attacks, and for example MITRE's ATT&CK (https://attack.mitre.org/) is a medium abstraction level model. ATT&CK offer a common behavior-focused adversary model which consists of the adversary's desired impacts can be listed according to ICT, ICS, and OT impacts of an organization. For example, ICT impacts are Data Destruction, Data Encrypted for Impact, etc., and ICS/OT impacts are Denial of Control, Loss of Availability, etc. (Kovanen et.al, 2021b, Table 4.). Those are the end point impacts that manifest after successful attack paths are completed and they are agnostic to the used techniques and technologies (Kovanen et.al, 2021b).

Behind an attack there are motivational factors and goals, capabilities and varying triggers depending on the attacker archetype. By identifying that information, it is possible to evaluate attack impacts against an organization. At the end all information can be collected in order to make general view from possible impacts against an organization. (Kovanen et.al, 2021a)

4. Cyber Risk Management Process

Cyber risk management is the process of identifying, analyzing, evaluating, and addressing cyber security threats to an organization's capital and earnings. These risks stem from a variety of sources including financial uncertainties, legal liabilities, technology issues, strategic management errors, accidents, and natural disasters.

The ISO 27000 family of standards provides recommendations for information security management systems (integrated elements of an organization to establish policies and objectives and processes to achieve those objectives), risk treatments and controls. (ISO/IEC 27000, 2018)

Risk categories can be defined as the classification of risks as per the business activities of the organization and provides a structured overview of the underlying and potential risks faced by them. Most used risk classifications include strategic, financial, operational, people, regulatory and finance. Figure 2 depicts the process of managing cyber risks utilizing information derived from the cyber threat intelligence process.

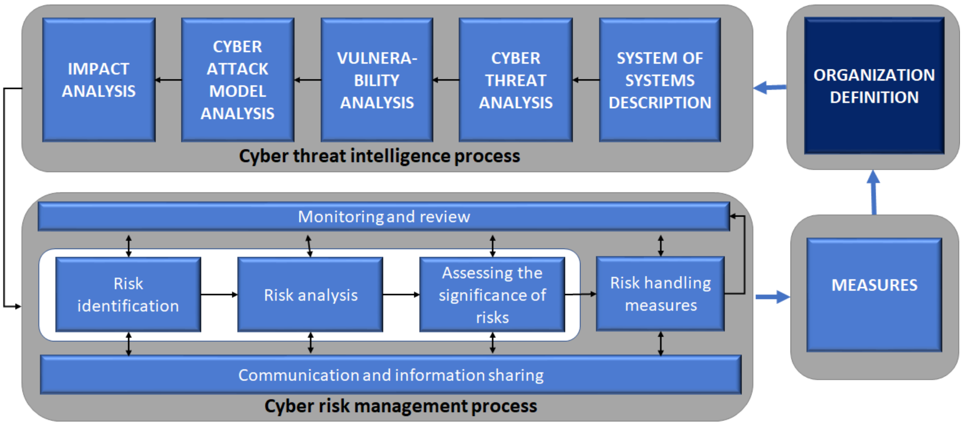
IMPACT ANALYSIS
CYBER ATTACK MODEL ANALYSIS
VULNERA-BILITY ANALYSIS
CYBER THREAT ANALYSIS
SYSTEM OF SYSTEMS DESCRIPTION
ORGANIZATION DEFINITION
Cyber threat intelligence process
Monitoring and review
Risk identification
Risk analysis
Assessing the significance of risks
Risk handling measures
MEASURES
Communication and information sharing
Cyber risk management process

Figure 2: Continuous development, cyber security enhancement processes

4.1 Risk Identification

The Cyber Threat Intelligence (CTI) process involves gathering information about threats that pertain to both cyber and physical domains, as well as the entities of these threats. Its primary goal is to support the risk assessment procedure to analyze and categorize the likelihoods of attacks and adverse events in the cyberspace domain for an organization.

In relation to risk identification, all discernible risks associated with the subject of the risk assessment need to be documented. The aim of risk identification is to recognize and detail all significant risks and opportunities, pinpoint sources of risks, delineate areas of impact, identify events (including changes in circumstances and their causes), and outline potential consequences. Risk identification should be conducted for each of the five layers of the cyber world.

4.2 Risk Analysis

There are diverse approaches to conducting risk analysis, wherein the assessment of the likelihood and impact is carried out on a risk-by-risk basis. This analysis serves as a foundation for making decisions regarding the identification and mitigation of risks. Estimates of both likelihood and impact in the analysis are often subjective, requiring multiple perspectives to construct a comprehensive understanding of the situation. The analytical process can be rooted in either quantitative (numerical) or qualitative (descriptive) methods, or a combination of both.

In the context of threat analysis and risk-level estimations for an organization's systems and sub-systems, the Delphi method is a notable approach. Used by cyber security experts within the organization, the Delphi method involves an iterative process aimed at enhancing consensus-building. Ultimately, the goal is to achieve a consensus among experts examining a particular case. The Delphi method is integral to quantitative analysis, contributing to the attainment of an optimally reliable expert consensus. According to Garson (2012), the Delphi method can be directed towards one of three objectives:

1. forecasting future events
2. achieving policy consensus on goals and objectives within organizations or groups
3. identifying diversity in and obtaining feedback from stakeholders in some policy outcome.

For risk analysis we have used probability tree principles, and it can be applied as well in general cases. The probability tree is described as using Defense probability P_D` against Attack probability P_A in the evaluation process. Cyberattacks (A) in organization´s processes are the same as the “Attack Identification” and located on all levels of the system level responsibilities (Strategy, Operational, Tactical/Technical). The P_A attack probability (P_{SOT}) to defend against attack probability P_D` (P_P, P_D, P_M, P_R) is related to the combination of cyber security capabilities (people, processes, and technologies), using “Protection” (P), “Detection” (D), “Countermeasure”

(M) and "Recovery" (R) activities according to NIST Framework for Improving Critical Infrastructure Cyber security (2018). The entire risk assessment process can be done by experienced cyber security professionals related to the case to be investigated. (Pöyhönen, et.al. 2022)

The probabilistic success of attacks, P(t), against the defense of system x can now be evaluated and calculated as follows, adapting the principle in "Threat Analysis of Cyber-Attacks with Attack Tree+" (Wang & Liu, 2014, mod.). $P_{Ax}(t) = P_A P_{D^{\cdot}} = (P_{SOT})(1 - P_P(t))(1 - p_D(t))(1 - p_M(t))(1 - p_R(t))$ (1)

Cyber security professionals employ the formula (1) principle for probability estimation. Subsequently, the OWASP Risk Rating Methodology is utilized to pinpoint security risks. This evaluation encompasses details about the involved threat agent, the planned attack, the associated vulnerability, and the potential impact of a successful exploit on system operations. (Pöyhönen, et.al. 2022)

The risk levels are categorized as LOW, MEDIUM, and HIGH, contingent upon the estimated severity of the attack impacts and the likelihood of harm post the evaluation of defense capabilities. The determination of the risk level relies on various elements within each factor, including the motive and capability of the attacker, the ease of identifying vulnerabilities, the compromise of CIA (Confidentiality, Integrity, Availability), and the resultant damages to the system. Each factor comprises a set of options, and each option is associated with a likelihood rating from 0 to 0.9. This rating scale is further divided into three segments: 0 to <0.3 corresponds to LOW, 0.3 to <0.6 equates to MEDIUM, and 0.6 to 0.9 signifies HIGH (OWASP, 2022).

4.3 Assessing the Significance of Risks

Risks are appropriate to prioritize according to business objectives. The aim of evaluating the importance of risks is to aid in decision-making regarding which risks should be tackled and their order of priority. The assessment may reveal the necessity to reevaluate certain risks or require additional analysis. Within the context of the significance assessment, it may be determined that certain identified risks will not be addressed.

4.4 Risk Handling Measures

In the risk handling process, risk-specific measures are decided. In the process organizations determine how to respond to the risks they face. In the risk handling process, risk-specific measures are decided. In this state of process organizations determine how to respond to the risks they have recognized. In the realm of risk management, organizations try to balance between risk acceptance and risk reduction efforts. Additionally, the practice of risk sharing, or transfer involves contractual arrangements with third parties, such as insurers, to assume some or all of the potential costs associated with a given risk, whether realized or not.

The risk handling plan is determined by the level of risk. It is essential to define the necessary handling measures and responsibilities for the most significant risks identified in the assessment and to ensure the progress and implementation of the agreed management measures.

4.5 Measures After Risk Assessment

The handling of the initial three scenarios regarding events, which are known known, known unknown and unknown known in the mentioned Table 1. necessitates the implementation of cyber and information security measures tailored to the organization. These measures should incorporate a fundamental security solution while considering potential risks. Continuously updated risk analysis plays a crucial role in supporting security measures. Unforeseen incidents, which cannot be anticipated, are addressed by the organization's contingency planning, ultimately enhancing operational resilience.

5. Resilience Development

The cyber operating environment of an organization is characterized by uncertainty, stemming from the likelihood of events occurring within intricate SoS structures. Cyber security resilience constitutes an integral component of preparedness and organizational continuity management. Cyber resilience is the ability of an organization to protect itself from, detect, respond to, and recover from cyber-attacks.

Unprecedented losses linked to events such as natural disasters and cyber-attacks have brought attention to novel strategies for reducing damage. While the prevailing analytical and governance framework of the past few decades centered on risk analysis, there has been a recent shift in rhetoric towards recognizing the importance of comprehending and crafting resilience (Linkov et al. 2013a). Linkov et al. (2013a) have cited the National

Academy of Sciences (NAS) report's characterization of resilience in the context of disasters (later: "Linkov model"). This model for strategic resilience planning combines the four essential stages of a resilience matrix framework—plan/prepare, absorb, recover, and adapt—with the four crucial domains encompassing physical, information, cognitive, and social aspects within a system of systems. Linkov et al. (2013b) extended the application of their model specifically to cyber systems, aiming to establish efficient metrics for assessing the resilience of such systems.

Disaster resilience exhibits elements of surprise, complexity, urgency, and the imperative for adaptation. In reaction to these challenges, military experts have put forth the concept of Network Centric Warfare (NCW). This doctrine emphasizes the establishment of shared situational awareness and decentralized decision-making through the dissemination of information across networks that operate in physical, information, cognitive, and social domains: (Linkov et al., 2013a)

- Physical: sensors, facilities, equipment, system states and capabilities
- Information: creation, manipulation, and storage of data
- Cognitive: understanding, mental models, preconceptions, biases, and values
- Social: interaction, collaboration and self-synchronization between individuals and entities

The development process of cyber security resilience plays a vital role in guaranteeing the continuity of organizational measures under various operational conditions. We have identified a proactive five-step process (refer to Figure 3) for strategizing and guiding resilient actions in the event of a significant cyber security threat to organizations.

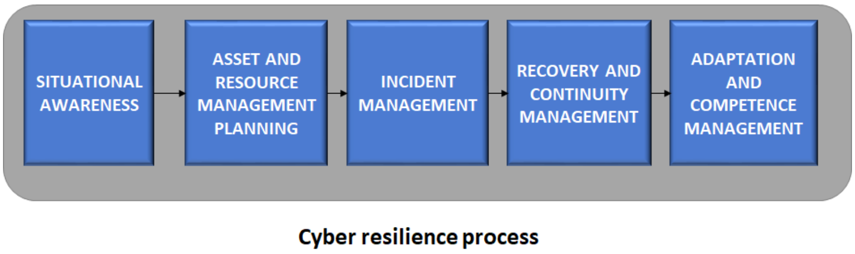
SITUATIONAL AWARENESS
ASSET AND RESOURCE MANAGEMENT PLANNING
INCIDENT MANAGEMENT
RECOVERY AND CONTINUITY MANAGEMENT
ADAPTATION AND COMPETENCE MANAGEMENT
Cyber resilience process

Figure 3: Cyber security resilience development process

5.1 Situational Awareness

Each organization needs information about its environment and its events, and its impact on their own activities. To get a holistic view of the organization's cyber security and resilience, situation awareness is needed. One solution to develop a company-specific understanding of situational awareness is using SWOT analysis (Pöyhönen et al., 2018). The term SWOT is an acronym of the words Strengths, Weaknesses, Opportunities and Threats. SWOT analysis is an important tool for analyzing an organization's performance and operating environment. Based on the SWOT analysis, the related needs of each organization can be planted to crucial domains encompassing physical, information, cognitive, and social aspects of resilience process within a system of systems according to Linkov's model phases; plan/prepare, absorb, recover, and adapt. The subsequent four chapters delineate these stages by providing an illustrative example in alignment with our previous paper titled "Application of Cyber Resilience Review to an Electricity Company"(Pöyhönen et al., 2018).

5.2 Asset and Resource Management Planning

Physical: In order to enhance technical solutions situational awareness of assets and effective segmentation of systems is crucial, and exploring alternative resources can provide valuable robust solutions.

Information: The organization should focus on the data of the classification and prioritization of critical systems and information of assessed potential business impacts and to implement thorough preparation for sensitive information and devised comprehensive communication plans to ensure a robust and proactive approach to risk management of data.

Cognitive: The effective development of situational awareness involves a comprehensive approach, encompassing the careful consideration of scenarios and models, and adept situational management. Ensure strategic resourcing for secure operations. Plans for training and benchmarking, supported by a robust feedback system to enhance the perception of situational awareness.

Social: The CI organization should focus on comprehensive communication plans to ensure a robust and proactive approach to inform necessary stakeholders. The naming of stakeholders' contact persons and specialized training for exceptional situations are crucial components in ensuring effective communication and preparedness within the organization.

5.3 Incident Management

Physical: The comprehensive approach to absorbs incident includes the recognition of disturbances, their scope, and impacts, ensuring the protection of sensitive information systems, deploying alternative resources, and implementing effective isolation measures to safeguard the critical system of systems.

Information: The thorough documentation of the incident data is instrumental in effectively informing all stakeholders about the progress of the case and analyze and storage its progress.

Cognitive: In the analysis of situational awareness, careful prioritization of available information is crucial, and the allocation of additional resources plays a pivotal role, while being ready to share sensitive information to stakeholders.

Social: Disseminating comprehensive updates to stakeholders and authorities, ensuring transparent communication, and providing detailed insights into the ongoing operations.

5.4 Recovery and Continuity Management

Physical: To ensure the smooth operation of recovery, it is necessary to focus on the maintenance of technical situational awareness of systems throughout the ramp-up phase, implementing rigorous testing protocols to guarantee the system's reliability.

Information: Careful documentation of the incident data and comprehensive information of the case recovery phases support its actions as well as ensuring trust and clarity of communication for continuity management.

Cognitive: The allocation of expertise is crucial for the efficient recovery process and collection of incident data and log information in order to enhance decision-making processes.

Social: Incident status information from CI organization updates stakeholders and authorities, ensuring transparent communication, and providing detailed knowledge shearing into the ongoing recovery ensuring trust, transparency, and clarity in communication.

5.5 Adaptation and Competence Management

Physical: After the incident, it became crucial to adapt to the new situation by implementing modifications and updates to techniques of systems.

Information: Part of the competence management development aggregation of incident documents, coupled with complementary improvements of data and information management processes, enhances the efficiency and effectiveness of organizational workflows.

Cognitive: Continuous improvement is achieved through a management and adaptation process that involves understanding log analysis and other information, conducting impact analysis, performing situation analysis, incorporating feedback analysis, and implementing timely system updates.

Social: The situation briefing for all parties on adaptation status, staff training programs, informing about development operations, and updating stakeholder information provides a comprehensive overview for the current organization updates measures and the networked partnership.

6. Discussion

In the realm of organizational cyber security management and continuity management, adopting a Systems of Systems (SoS) research approach facilitates the creation of a comprehensive cyber security framework. This approach entails identifying all processes, users, and digital assets within the organization. For instance, Directive (EU) 2016/1148 of the European Parliament and the Council was formulated to bolster cyber security capabilities across the European Union. Its aims encompassed mitigating threats to network and information systems, ensuring the provision of essential services in critical sectors, maintaining service continuity during incidents, and fortifying society's overall cyber security (EU, 2016). To fulfill these objectives, it is imperative to establish an overarching management system that encompasses risk management and continuity guidelines, thereby enabling continuous enhancement of business continuity practices. Consequently, this paper integrates risk assessment methodologies with resilience development models to offer organizations a comprehensive approach to continuity management.

7. Conclusion

Organizations in the realm of risk management aim to balance risk acceptance with insights from cyber threat intelligence. Decision-making is guided by risk avoidance principles, emphasizing elimination, reduction, and mitigation through cyber security and information security updates. Risk sharing involves contractual arrangements with third parties to assume potential costs. Incorporating resilience measures in planning benefits decision-making and preparedness, providing insights for security planning, and aiding learning and problem identification in unforeseen circumstances. The resilience development model supports operational continuity management at all decision-making levels of an organization. Maintaining awareness of cyber threats and employing a thorough risk management process together with resiliency measures allows organizations to strategically protect digital assets.

References

Beggs, C. (2006). Proposed Risk Minimization Measures for Cyber-Terrorism and SCADA Networks in Australia, Proceedings of the 5th European Conference on Information Warfare and Security, National Defence College, Helsinki, Finland, 1-2 June 2006

Bertino, E., Martino L.D., Paci F., and Squicciarini A.C. (2010). Web services threats, vulnerabilities, and countermeasures. In Security for Web Services and Service-Oriented Architectures, pp. 25–44. Springer.

Bodeau, D. J. and McCollum, C. D. (2018). System-of-systems threat model. The Homeland Security Systems Engineering and Development Institute (HSSEDI) MITRE: Bedford, MA, USA.

Borner, P. (2019). Cloud data breaches caused by human error, The Data Privacy Group blog, May 10 2019. https://thedataprivacygroup.com/blog/cloud-data-breaches-caused-by-human-error/ (Retrieved 1/2024)

Dahmann, J. S. (2015). Systems of Systems Characterization and Types, MITRE Corporation.

EU, (2016). Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union https://eur-lex.europa.eu/eli/dir/2016/1148/oj

ISO/IEC 27000. (2018). International Organization for Standardization. Information technology. Security techniques. Information security management systems. Overview and vocabulary. https://www.iso.org/standard/73906.html (Retrieved 2/2023)

Kim, S. D. (2017). Characterization of unknown unknowns using separation principles in case study on Deepwater Horizon oil spill. Journal of Risk Research, 2017 Vol. 20, No. 1, 151–168, http://dx.doi.org/10.1080/13669877.2014.983949 (Retrieved 1/2024)

Kovanen, T., Pöyhönen, J. and Lehto, M. (2021a). Cyber Threat Analysis in the Remote Pilotage System. Proceeding of the 20th European Conference on Cyber Warfare and Security ECCWS 2021, p. 221-229.

Kovanen, T., Pöyhönen, J. and Lehto, M. (2021b). ePilotage System of Systems' Cyber Threat Impact Evaluation. Proceedings of the 16th International Conference on Cyber Warfare and Security ICCWS 2021. p. 144-151.

Lehto, M. (2013). The Cyberspace threats and cyber security objectives in the Cyber Security Strategies. International Journal of Cyber Warfare and Terrorism, Vol. 3, Issue. 3, pages 1-18, 2013.

Lehto, M. and Neittaanmäki, P. (2018). The modern strategies in the cyber warfare. Cyber Security: Cyber power and technology. Berlin: Springer.

Lehto, M. (2022). APT cyber-attack modelling - building a general model. 17th International Conference on Cyber Warfare and Security, 17 - 18 March 2022, State University of New York at Albany, USA.

Libicki, M. C. (2007). Conquest in Cyberspace – National Security and Information Warfare, Cambridge University Press, New York 2007.

Linkov, I., Eisenberg, D., Bates, M., Chang, D., Convertino, M., Allen, J., Flynn, S. and Seager, T. (2013a). Measurable Resilience for Actionable Policy. Environmental Science & Technology. https://pubs.acs.org/doi/epdf/10.1021/es403443n (Retrieved 1/2024)

Linkov, I., Eisenberg, D., Plourde, K., Seager, T., Allen J. and Kott, A. (2013b). Resilience metrics for cyber systems. Environment Systems and Decisions, 33(4), pp. 471-476.

Lockheed Martin, LM. Cyber Kill Chain, https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (Retrieved 1/2024)

MITRE, ATT&CK https://attack.mitre.org/ (Retrieved 1/2024)

National Institute of Standards and Technology, NIST. (2018). Framework for Improving Critical Infrastructure Cyber security, April 16, 2018

OWASP Risk Rating Methodology, Available from: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology, (Retrieved January 2024)

Pöyhönen, J., Nuojua V., Lehto M. and Rajamäki J. (2018). Application of Cyber Resilience Review to an Electricity Company. ECCWS 2018: Proceedings of the 17th European Conference on Cyber Warfare and Security (pp. 380-389). Published by Academic Conferences and Publishing International Limited. Reading. UK.

Pöyhönen, J. and Lehto, M. (2020). Cyber security: Trust based architecture in the management of an organization‘s security. In Eze, Thaddeus; Speakman, Lee; Onwubiko, Cyril (Eds.) ECCWS 2020: Proceedings of the 19th European Conference on Cyber Warfare and Security (pp. 304-313).

Pöyhönen, J., Hummelholm, A. and Lehto, M. (2022). Cyber security risks assessment subjects in information flows. Proceedings of the 21st European Conference on Cyber Warfare and Security ECCWS2022, 2022, University of Chester, UK, pages 222-230.

Pöyhönen, J. and Lehto, M. (2022). Assessment of cyber security risks - Maritime automated piloting process. Proceedings of the 17th International Conference on Information Warfare and Security, 2022. pp 262-271.

Wang, P. & Liu, J. C. (2014). Threat analysis of cyber-attacks with attack tree+. Journal of Information Hiding and Multimedia Signal Processing, 5(4).