Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P626-cd

Modeling a cyber-resilience-for-manufacturing ecosystem through causal loop diagram

Saloua SAID

Systems engineering and decision support laboratory, Ibn Zohr University, ENSA, Agadir, Morocco. E-mail: Saloua.said.5@gmail.com

Hafida Bouloiz

Systems engineering and decision support laboratory, Ibn Zohr University, ENSA, Agadir, Morocco. E-mail: h.bouloiz@uiz.ac.ma

Maryam Gallab

MIS-LISTD Laboratory, Computer Science Department, Mines-Rabat School (ENSMR), Rabat, Morocco. E-mail: meryam09@gmail.com

From script kiddies to sophisticated and organized cybercriminals, cyber threats are constantly growing, adding new and further challenges. Therefore, overseeing and proactively responding to this severe and emergent cyber risk is of the utmost importance. This is called cyber resilience, which designates the ability to withstand and quickly recover from any cyber-related incident. Without this fundamental capability, a cybersecurity failure could inflict considerable damage on organizations and even drive them out of business. According to a recent IBM cyber security intelligence index survey, manufacturing is one of the most targeted industries for cyber-attacks. Manufacturing 5.0 is increasingly being adopted by companies as a transformation pillar to harness the potential of data and create value at scale. This includes connected factories, moving from insights and decision to operations and actions driven by analytics and artificial intelligence, scaling valuable use-cases and solutions and multiplying the impacts through a leverage effect, considering human resources as value creators, accelerators of innovation, and architects of change. These ambitions are accompanied by several cyber risks, such as system vulnerabilities, social engineering, malicious insiders, data loss, etc. In the present paper a cyber-resilience-for-manufacturing ecosystem will be introduced, and cause-effect relationships, identified within this ecosystem, will be illustrated using causal loop diagram in order to understand how an industrial site could be more resilient.

Keywords: resilience, cyber incidents, manufacturing, ecosystem, causal loop diagram, awareness, availability.

1. Introduction

Today's sociotechnical systems are constantly unearthing the latest trends and technologies to create the industry of the future: Industry 5.0. This most recent industrial revolution brings with it the promise of a more human-centric approach by establishing a proper balance between human values and the use of new technological advances. Furthermore, Industry 5.0 is focusing on resilience reinforcement rather than being aimed solely at improving profit and efficiency. In fact, during the COVID-19 outbreak, which swept across the world, plenty of lessons have been learned, especially the importance of developing resilience capabilities to surmount crises and overcome adversity successfully and rapidly. Sindhwani et al. (2022). This implies that Industry 5.0 appears to have considerable advantages in promoting sustainability and bringing about positive change. However, the emergence of digital technology in the context of industry 5.0 is creating a real and growing danger of cyber-attacks. Aside from the various forms of social engineering threats and hacking techniques, new attack vectors are increasingly expanding, such as crypto-jacking, botnets, data leakage, and cybercrimes driven by cloud computing. To address the different cyber security threats mentioned and provide better protection against

them, many measures are typically implemented and applied by sociotechnical systems. Blocking spam and malicious websites through the use of firewalls or proxy servers, using password managers to generate unique and hard-to-guess passwords, as well as opting for a multifactor authentication by adding further factors, such as fingerprint or face recognition, and above all providing security training for employees so that they can easily identify phishing emails might be a sound approach to avoid falling victim to phishing scams. Moreover, organizations can also avoid becoming infected by malware by applying security updates and patches, upgrading to the latest and more secure operating systems versions, installing firewalls and antimalware software, making frequent backups to guarantee a better availability of the system, and finally, education and training remain a fundamental necessity. Regarding crypto-jacking, considering whether the browser is vulnerable to this threat, installing Script-Blocking Browser Extensions, and using browsers with built-in ad blockers like Brave and Opera can help to overcome this concern. As for coping with botnets, DDoS (Distributed Denial of Service) attacks, and Internet of Things threats, several techniques may be employed. One can enumerate using multiple protected geographically separated data centers and diverse internet service providers, networks, and IoT (Internet of Things) devices safeguarding through, for example, blocking ports and network segmentation using routers and switchers. As regards the protection against cloud security threats, it is viewed as a shared responsibility across the sociotechnical system and the cloud service provider. Within this framework, the Cloud Security Alliance (CSA) has put at the disposal of organizations who wish to optimize their cloud experience and security guidance to help them to take the edge off risks relating to the uptake of cloud-computing technology. Encrypting data-at-rest and preventing access without permission could minimize the occurrence and impact of data breaches. Furthermore, it is essential to elaborate comprehensive and detailed cloud strategies, while thoroughly selecting cloud service providers that are characterized by the highest levels of security, monitoring, and response, and to ensure regular reviews of them. Shadow IT can be fought, in turn, by different means, notably IT Asset Inventory, IT processes promotion, security policies enhancement, and the use of control technologies, such as Security Information and Event Management Systems (SIEM), Network Access Control (NAC), and Cloud Access Security Broker (CASB). Preventive and remedial actions previously listed fall within the framework of cyber-security, which constitutes the key line of defense against online crime. This can be defined as a continuous improvement effort materialized by the implementation of proper requirements, controls, processes, and responses to protect digital assets including data, communication, software, applications, services, and equipment against the cyber-threats landscape. In addition to these measures designed to protect IT systems, business continuity should be ensured despite cyber-attacks. This can be achieved through cyber-resilience, which constitutes a concept that is gaining increased momentum, not only among academic researchers but also in sociotechnical systems. Björck et al. (2015). The ability to identify any breaches that affect the business operation, respond quickly and effectively by taking the appropriate measures to resist the destructive effect of the cyber incident and avoid the interruption of activity, recover within a short period, and learn from experiences of this kind to anticipate any future adverse events, constitute the main pillar of cyber resilience according to the definition of The National Institute of Standards and Technology (NIST). Hausken (2020). Cyber resilience is becoming a crucial element in manufacturing companies since this sector is regarded as being a popular, attractive, and high-value target for cybercriminals. The ransomware attacks encountered by Renault-Nissan in 2017, Norsk Hydro in 2019, and the cyber-attack on three major steel companies in Iran and Toyota's supply chain in 2022, provide a good example of the ever-growing cyber risk faced by manufacturing industries. Thanks to the improvement of human-machine interaction within the context of manufacturing 5.0, promising benefits will be demonstrated, notably the reduction of time losses, effort, and repetitive tasks for human workers. Adel (2022). Nevertheless, the increased connectivity driven

by the fifth industrial revolution may further increase cyber risk. For this reason, resilience is placed at the core of manufacturing 5.0. Romero et al. (2021). In order to foster this ability to remain operational in the face of adversity, numerous manufacturing companies are interested in the use of systematic problem-solving processes (SPSP), which form part of the design thinking approach. This process consists of several steps. Meister et al. (2018). The first and most critical one is problem clarification to contain the problem, ensure a clear common understanding and avoid a re-occurrence of the event. After the problem clarification, the issue should be described by analyzing the reasons of detection delay and occurrence. Various methods can be used for this purpose, such as 6M, 5 WHY'S, and Root Causes Tree Diagram. Then, an action plan should be drawn up and managed via PDCA (Plan, Do, Check, Act) methodologies. Finally, these countermeasures' efficiency must be constantly checked. This paper is intended to introduce a cyber-resilience-for-manufacturing ecosystem to determine the elements that can contribute to mitigating the cyber-risk in industrial sites.

2. Cyber-resilience-for-manufacturing ecosystem

Industrial activities run by large firms are usually highly automated manufacturing processes and thus are critically dependent on Information Systems. Qi et al. (2022). This generates a complex network of interrelated systems involving a vast variety of stakeholders. Each component of this network is constantly exposed to cyber threats and incidents, which places the cyber resilience at the heart of concerns since it allows to face situations that might cause critical impacts to the system and ensure the continuity of Information System operations, and the availability of the data. Smith (2023). In this section, the elements that compose the ecosystem of cyber-resilience for manufacturing will be introduced. Industrial sites constitute the first element. The equipment that carries the core processes of the plant (storage, weighting, fabrication, etc.) is hosted by Industrial Information Systems (IIS), such as Operator and engineering workstations, Maintenance laptops, PLCs (Programmable Logic Controllers), Industrial PCs (Packaging Component), HMIs (Human Machine Interface), AGVs (Automatic Guided Vehicles), Industrial application servers, and Utilities. Enterprise Information Systems (EIS) are used as well in industrial sites (Office workstations, Office application servers (e.g., mailing, Active Directory), Enterprise application servers). Taherdoost (2022). The mission to be achieved vis-à-vis of this element is availability: The operational functions of the plant must be ensured at any time whatever the circumstances. The second element is people, including human resources, customers, and suppliers. The qualities needed in this context are awareness and competence that can be achieved through training. The third element is cyber-attacks. This can be defined as an occurrence that actually or potentially jeopardizes the availability of the industrial site. This could be, among others, a data breach, a malware or ransomware infection, a sensitive data leak, a website defacement, an illegal intrusion on the information system (IS), an internal or external malicious act, a denial-of-service attack, etc. According to recent studies, 95% of cybersecurity breaches are caused by human error, hence the importance of training to improve people's awareness. By way of anticipation, potential cyber risks should be listed and analyzed on two levels, the probability of their occurrence (rare (e.g., approximately once every 10 years), occasional (e.g., once every 3 years), and probable (e.g., once a year)), and the severity of their potential consequences, which is assessed by evaluating the duration of production incapacity and the corresponding production volume loss (e.g., Low severity: less than 1 month production volume on site, Medium severity: from 1 to 3 months of production, High severity: more than 3 months of production). The fourth element is data, which can take different forms (transactional data, proprietary data…). To ensure sustainable data quality across the industrial site, data governance could be deployed. This is based on 4 pillars, which are data structures, data tools (advanced data management tools), organization (various levels of decision-making), and data policies (data quality, accessibility, external data acquisition…). Cyber incidents can affect data privacy (personal data, categories of individuals concerned). Cyber incidents can affect data

integrity and confidentiality (types and volumes of personal and non-personal data that could be altered and exposed, geographical perimeter of impact (outage, adverse media coverage, loss of market shares…)). The last element is finance. This englobes turnover that can be negatively impacted in case of cyber incidents, and recovery costs. Within this ecosystem, several cause-effect relationships can be detected. These links will be represented by a causal loop diagram (CLD).

3. Causal loop diagram

The diagram illustrated by figure 1 shows that providing training regarding cyber-resilience, measured by (i) target population rate, which defines the percentage of people covered by the training, (ii) training frequency (e.g., number of workshops per month), (iii) training follow-up (track progress and communicate frequently about changes and updates), contributes to raising the awareness about the evolving cyber-risk. This awareness is emphasized through alert and resistance rates, which characterize the capacity to rapidly notice, via direct observation or event correlation system analysis, and notify a potential incident. Training also helps to increase competence, which can be measured by efficiency rate (the ability to deal efficiently with unexpected cyber threats). With improved awareness and competence, human errors that constitute the main cause of cyber-attacks can be significantly decreased (error rate represents the number of cyber errors detected within a given period of time). In our context, a cyber incident can be defined as an occurrence that actually or potentially jeopardizes the availability of the information system (IS) in an industrial site or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. Cichonski (2019). A 3-level scale can be used to measure the frequency or the probability of occurrence of cyber risks for the industrial site (rare, occasional, probable). The analysis can be based on the history of accidents, nearly accidents or occurred production incapacity. Moreover, severity of the incident can be assessed by evaluating the duration of production incapacity and the corresponding production volume loss. A classification of severity with 3 levels (low, medium, high) can be used by the plant. The availability of the site can be measured through the use of two indicators, which are Recovery Point Objective (RPO) describing the period in which data must be restored after a disruption, and Recovery Time Objective (RTO) that is the period during which the system must recover. Said et al. (2019). It is worth mentioning that availability refers to staying operational and avoiding activity interruption, while recovery stands for full return to normalcy within the shortest delay (recovery time) and with the lowest level of damage possible (turnover loss, recovery costs, adverse media coverage, data loss…) and with lessons learnt.

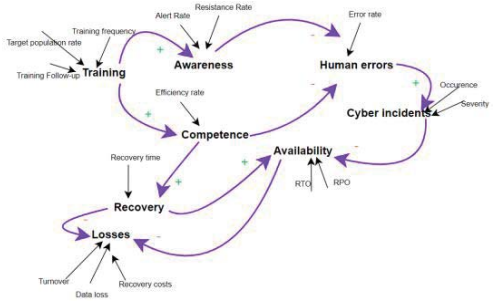

Fig. 1.CLD of cyber-resilience-for-manufacturing ecosystem

The feedback loops illustrated in Fig. 1 can be described as follows: A good level of training results in an increase in awareness and competence. These two strengths contribute to minimizing human errors and hence limiting the probability of serious cyber incidents. In this way, a satisfactory level of availability can be guaranteed. In the event of a cyber-attack, competence acquired through continuous training can be put in practice to accelerate recovery and therefore regain availability as rapidly as possible. The optimized recovery and

availability help to keep losses in turnover, data, time and costs to a minimum.

4. Conclusion

This paper is intended to discuss the main contributors to achieving cyber-resilience within an industrial context. This qualitative study is focusing on analyzing the causal links that lead to more resilient industrial systems and is aligned with industry 5.0 since it is putting people at the center of attention. In future research, interest will be paid to quantitative analysis. For this purpose, a stock-flow model will be elaborated and simulated by Insight Maker tool.

References

Adel, Amr. "Future of Industry 5.0 in Society: Human-Centric Solutions, Challenges and Prospective Research Areas." Journal of Cloud Computing 11, no. 1 (2022). https://doi.org/10.1186/s13677-022-00314-5.

Björck, Fredrik, Martin Henkel, Janis Stirna, and Jelena Zdravkovic. "Cyber Resilience – Fundamentals for a Definition." New Contributions in Information Systems and Technologies, 2015, 311–16. https://doi.org/10.1007/978-3-319-16486-1_31.

Cichonski, Jeff. "Cybersecurity Framework Manufacturing Profile Low Security Level Example Implementations Guide," 2019. https://doi.org/10.6028/nist.ir.8183a-1-draft.

Hausken, Kjell. "Cyber Resilience in Firms, Organizations and Societies." Internet of Things 11 (2020): 100204. https://doi.org/10.1016/j.iot.2020.100204.

Meister, Maximilian, Tobias Böing², Svenja Batz, and Joachim Metternich. "Problem-Solving Process Design in Production: Current Progress and Action Required." Procedia CIRP 78 (2018): 376–81. https://doi.org/10.1016/j.procir.2018.08.316.

Qi, Na, and Xun Zhang. "Optimization Design and Implementation of Shared Information Management System for Industrial Design Network Platform." Journal of Combinatorial Optimization 45, no. 1 (2022). https://doi.org/10.1007/s10878-022-00956-w.

Romero, David, and Johan Stahre. "Towards the Resilient Operator 5.0: The Future of Work in Smart Resilient Manufacturing Systems." Procedia CIRP 104 (2021): 1089–94. https://doi.org/10.1016/j.procir.2021.11.183.

Said, Saloua, Hafida Bouloiz, and Maryam Gallab. "Resilience Assessment of System Process through Fuzzy Logic: Case of COVID-19 Context." Advances in Science, Technology and Engineering Systems Journal 5, no. 5 (2020): 1247–60. https://doi.org/10.25046/aj0505150.

Sindhwani, Rahul, Shayan Afridi, Anil Kumar, Audrius Banaitis, Sunil Luthra, and Punj Lata Singh. "Can Industry 5.0 Revolutionize the Wave of Resilience and Social Value Creation? A Multi-Criteria Framework to Analyze Enablers." Technology in Society 68 (February 2022): 101887. https://doi.org/10.1016/j.techsoc.2022.101887.

Smith, Sidney. "Towards a Scientific Definition of Cyber Resilience." International Conference on Cyber Warfare and Security 18, no. 1 (2023): 379–86. https://doi.org/10.34190/iccws.18.1.960.

Taherdoost, Hamed. "An Overview of Trends in Information Systems: Emerging Technologies That Transform the Information Technology Industry." Cloud Computing and Data Science, 2022, 1–16. https://doi.org/10.37256/ccds.4120231653.