**The International Journal of Technology, Knowledge, and Society**
ISSN: 1832-3669 (Print), ISSN: 2835-0391 (Online)
Volume 20, Issue 1, 2024
https://doi.org/10.18848/1832-3669/CGP/v20i01/1-15

Original Research

# Industry 4.0 Introduction in Critical Infrastructure: Information Security Reasoning in Practice

Anton Holmström, Luleå University of Technology, Sweden
Johan Lugnet, Luleå University of Technology, Sweden
Åsa Ericson, Luleå University of Technology, Sweden

***Received:*** 02/17/2023; ***Accepted:*** 12/15/2023; ***Published:*** 02/09/2024

***Abstract:*** The article presents an empirical study of critical infrastructure service providers in consulting, energy, and mining. The study aims to investigate how such service providers perceive and explain information security and challenges in the context of an information technology-operational technology (IT-OT) interconnected environment, that is, Industry 4.0. The study is based on qualitative data from semi-structured interviews with informants holding three different types of positions at the organizations, that is, OT security advisor, business developer, and information security coordinator. The study indicatively concludes that role and responsibility significantly impact practitioners' reasoning and standpoints. Similarly, security focuses, or prioritization, differs between IT and OT. In line with the literature, the findings indicate that mindsets or mental models need further attention. The article, thus, suggests three research directions to develop insight for expanding information security practices to encompass human and organizational challenges based on behaviors, roles, norms, and attitudes.

***Keywords:*** *Operational Technology, Incident Management, Information Technology, Cybersecurity, Risk Management*

## Introduction

A fourth industrial revolution, or Industry 4.0, envisions radical changes in the industrial manufacturing sector, giving rise to new information security challenges. The sector's transformation will impact the essence of how people conduct their work and businesses (Schwab 2017). For an extended period, the manufacturing industry, acting as a forerunner for many other industries, has undergone a preceding third industrial revolution characterized by the implementation of computerized systems and automation. While the third revolution occurred in-house, Industry 4.0 interconnects not only in-house systems but also organizations and processes externally (Ustundag and Cevikcan 2018). Typically, cloud computing, system integration, industrial internet of things, big data, augmented reality, and other cyber-physical systems characterize the Industry 4.0 vision (Le Moigne 2021; Smart Service 2015). The concept of twin transition describes the importance of simultaneously progressing digitalization and the circular economy, that is, ecological, social, and economic sustainability (Ortega-Gras et al. 2021). Industry 4.0 technologies, notably, include the

capability to collect, store, share, and use data regarding products throughout their usage stages. For example, Thyssenkrupp, an elevator provider, applies this with 130,000 elevators worldwide, while Komatsu gathers spatial data on their machines (Le Moigne 2021). Having the capability to collect data and use it for circular processes and business models is essential for achieving sustainable development. The research field of product-service systems suggests three types of business models, that is, product-oriented, use-oriented, and result-oriented (Tukker 2004). The latter orientation is functional, that is, the customers pay per used unit or for performance rather than the products itself. The change toward providing functionality in the industry reflects an inevitable digitalization trend progressing from an internet-based business through an IoT-enabled (internet of things) to a cyber-physically intelligent one, thereby adding *smart* to businesses and cities (e.g., Zheng et al. 2019).

Industry 4.0 technologies, to some extent, are already introduced in critical infrastructure, which historically has been a service provider of functionality. Critical infrastructure is, for example, those organizations delivering vital functions for the national economy and civil society. The continuity of government, telecommunications, electricity, gas and oil storage and transportation, food and water supply, and emergency services are critical functions for both the economy and civil society (Moteff and Parfomak 2004). Security, safety, and protection are key concerns for critical infrastructure, but there are challenges concerning Industry 4.0 digitalization. Wisniewski et al. (2022, 82717) explain that it is important not to limit the perspective solely to technical issues; instead, security includes "many things, systems and processes." Their research revealed that the connection between critical infrastructure and Industry 4.0 technologies had gained limited attention. Furthermore, Wisniewski et al. (2022) concluded that both areas are highly significant but are separately approached by researchers and practitioners.

Research on critical infrastructure employs the term industrial control systems (ICS) or operational technology (OT). These kinds of technologies were originally, even before the third industrial revolution, designed for monitoring and controlling proprietary and closed infrastructures (Wu, Dai, and Wang 2020). Service providers in critical infrastructure seldom have the possibility to start over from a clean canvas but have to upgrade and replace elements in existing infrastructure. Industry 4.0 digitalization, which involves connecting OT to the internet, has occurred simultaneously with these upgrades. This implies that OT is partly designed without attention to net-based security and can be vulnerable to cyberattacks (Wu, Dai, and Wang 2020). As the name indicates, IT addresses the development, maintenance, processing, distribution, and use of information through computer systems, software, and networks (Hahn 2016; Lasi et al. 2014). IT has long been established within day-to-day business processes, with its embedded and connected features serving as key enablers of Industry 4.0 technologies (Lasi et al. 2014). One operational manager referred to IT in an informal conversation using the company jargon "*Office-IT*" and pointed to the direction of the offices for the administrative department. The described distinction inspired a study on

how representatives from critical infrastructure service providers reason about information security and risks in light of the IT-OT interconnected Industry 4.0 technologies. Thus, the purpose of this study was to investigate how critical infrastructure service providers perceive and explain information security and challenges in such a context.

The term information security is not straightforward and is often used interchangeably with cybersecurity (Von Solms and Van Niekerk 2013). Therefore, we include a problematization in the theoretical background section, which also briefly outlines a threat landscape. However, first, we explain the research design and the analysis of the empirical material. The article concludes with the presentation of the empirical results and conclusions.

## Research Design: Data Collection and Analysis

We gathered qualitative data through semi-structured interviews with key informants from three companies spanning the consulting, mining, and energy sectors. While recognizing that a larger sample could offer broader insights, the depth and detail obtained from these informants—holding roles such as security advisor, business developer, and information security coordinator—yield valuable perspectives closely aligned with our research objectives. The selection of informants was based on the topic of the study, that is, whether they should have a role in the information security work based on their job description. Furthermore, the selection aimed to include different responsibilities, all related to security work. The study comprises data from three semi-structured interviews that address insights into employees' experiences, aligning with the sample size (Miles and Huberman 1994).

The interviews lasted approximately one hour each and were voice-recorded after consent from the informants; see Table 1 for an overview.

Table 1: Summary of Interviewees

| *Position* | *Business* | *Employees* |
|---|---|---|
| OT security advisor | Consulting | 7,000+ |
| Business developer | Mining | 4,000+ |
| Information security coordinator | Energy | 100+ |

Additionally, gaining access to organizations for investigating information security is not straightforward. Informing externally about information security puts high demands on the organizational culture and transparency. When agreeing to participate in a study, organizations admit that information security is a topic of importance and in need of investigation, something that could be seen as a weakness by their consumers. Also, there is still a culture of silence when it comes to cyberattacks, concerning both sectors and states (Sander 2019). The companies and the informants are therefore kept anonymous. It should also be noted that the responsibilities connected to occupational roles differ in different countries. The respondents in this study came from the same country but from various organizations. Thus, as operational managers, the business developer and the technology

advisor are responsible for information security in their business departments. In contrast, the information security coordinator is responsible for leading and coordinating security measures in the organization. The coordinator is, thus, an expert accountable for policies and guidelines and for managing technical protection.

The interviews were conducted using an interview guide based on the topics of information security, organization, and procedures. Informants were also prompted to reflect on future challenges regarding their respective organizations. All informants were asked to share their understandings and thoughts about the topics included in the interview guide, but they could also add related issues from their own experiences, that is, semi-structured interviews (Patton 2002). The interviews were transcribed verbatim, that is, typing exact utterances; thus, hesitations, rephrasing, filler words, and so on, have been included in the material analyses. However, for readability, quotes have been used in a clear verbatim style, that is, with the removal of filler words, and so on, and quotes have been edited since they have been translated from another language to English. However, quotes have been kept as close to the original words and context as possible (Silverman 2000).

## Data Analysis

The analyses of the empirical material follow the collection of qualitative data; that is, the first analysis occurs when listening to the informants' reasoning. It is necessary to ask follow-up questions for clarification, that is, the interviewer interprets what has been said and asks if the understanding follows what the informant meant. Text analysis is then conducted during the reading of the transcripts, where categories emerge from patterns within the material (Mason 2017), that is, predefined categories were not imposed on the material. The transcripts are analyzed interpretively in light of the context for the data set, that is, the verbatim transcript, and then assessed concerning the informant's role.

## Information Security

Information security, originating from an IT point of view, addresses the protection of confidentiality, integrity, and availability (so-called CIA triad, e.g., Stallings et al. 2012). These perspectives cover security issues related to digitalization, focusing on data, information, and systems. This means that confidentiality protects sensitive information from unauthorized access or disclosure. For instance, utilizing access controls ensures that only authorized personnel can view patient information in healthcare organizations. Integrity concerns the preservation of the accuracy and completeness of the information. For example, to ensure that medical journals contain accurate information and can be trusted, availability describes how data, information, and systems are accessible by authorized users when they need it—for example, ensuring that a system or service is running smoothly with no interruptions and that users can access the information they need when they need it.

The CIA triad has been and is discussed regarding whether or not it needs to update its terminology (e.g., RealWorldCyberSecurity 2020). In our view, such discussions relate more to understanding information security as being detached from cybersecurity, a simplified view where information security is grounded in management and cybersecurity in technology. Von Solms and Von Solms (2004) emphasized that information and cybersecurity are jointly key elements embedded in a holistic view. In addition, Von Solms and Van Niekerk (2013), by referencing contemporary descriptions of cybersecurity, add that the concepts to some extent overlap since both are described in practice to include everything from policies, management, approaches, and training of personnel to infrastructure, systems, tools, and applications. They propose an additional concept for research, that is, information and communication technology security as the intersection between information security (information assets not stored or transmitted via IT) and cybersecurity (data or non-information vulnerabilities via IT).

However, given the encompassing digitalization of modern critical infrastructure, particularly the introduction of Industry 4.0, which is based on interconnectivity and embedded intelligent solutions, separating IT information assets from digital data assets becomes problematic for future practice. The data-information-knowledge-wisdom hierarchy (Ackoff 1989) visualizes the connection between data and information, especially given contemporary digitalized systems' capabilities, making both data (non-information) and information (contextualized data) assets crucial to protect. Although, as commonly applied in research and this study, distinctions help serve as a cognitive model to investigate complex relationships—such as the one between Industry 4.0 and the security practices for service providers of critical infrastructure functions—the term information security is used here to capture all types of security aspects (e.g., procedures, access, and protection of operations), data, and information assets. Nevertheless, as indicated in previous research (Wisniewski et al. 2022) and in our pre-studies, viewing IT and OT as standalone environments of operations in practice is a barrier to Industry 4.0 security (Jaatun et al. 2020).

The general term OT captures several different ICS, each examined from different perspectives, for example, Supervisory Control and Data Acquisition (SCADA) and Industrial Automation Systems. Knapp and Langill (2014) assert that OT includes all information and control system connected to the service provision operations. In critical infrastructure, the information security concerns for OT are manifold, for example:

- The safety of people and equipment is a critical concern, as malfunctions in the OT can result in severe consequences. For instance, incidents such as the ICS failure in Bellingham in 1999 caused an explosion from a gasoline leakage, leading to fatalities and injuries (Hahn 2016).
- Environmental failures in the OT can result in radiation or other toxic material being released into nature or the service processes (Knapp and Langill 2014).

- Supply chain dependencies, where errors in one link in the chain impact the end-user function; for example, the NotPetya attack targeted Ukrainian organizations, governmental agencies, hospitals, and financial institutions. Still, it also spread across the Ukrainian border to infect companies, including knocking out systems for the world's largest shipping company, Maersk (Greenberg 2018).

The threat landscape includes many different approaches and variants, often known to address IT environments. However, recent reports indicate that similar threats are targeting OT (Dragos 2022; ENISA 2022; Verizon 2023). Consequently, critical infrastructure systems become vulnerable to a wide range of threats, for example:

- Phishing and spear-phishing are based on social engineering and trick users into opening a malicious file or entering information on a fake website; the fraudulent goal is to set a point of entry into an organization (Bhardwaj et al. 2020).
- Malware is malicious software that disrupts or causes damage by infecting systems (Giles 2019).
- Ransomware is a specific type of malware that typically denies an organization access to its systems by holding data hostage if it does not pay (Liska and Gallo 2016).

## IT and OT Orientation

OT systems often depend on standards, protocols, and software that are relatively old, meaning that they are designed for isolated automation and not for interconnections between systems and networks. Consequently, OT has historically been designed without cyberattack detection or defense requirements in mind (Murray, Johnstone, and Valli 2017). The concept of an "air gap theory" explains the mental model that OT is isolated from IT. Thus, this air-gapped mindset is based on the idea that OT is not vulnerable to external cyberattacks due to its inaccessible proprietary characteristics. The air gap is one key barrier to introducing contemporary security models that converge IT and OT, as is needed in Industry 4.0 (Murray, Johnstone, and Valli 2017). The Stuxnet malware was an early eye-opener of how security challenges normally related to IT exploited the air gap to attack critical infrastructure, that is, maintenance aids on an infected USB flash drive (Hemsley and Fisher 2018; Knapp and Langill 2014).

The efforts to clarify IT and OT characteristics support understanding of two orientations, which also provide insights into their distinct impact on information security measures. First, the security focus differs from the CIA triad; for example, according to Zhu, Joseph, and Sastry (2011), IT's orientation toward confidentiality involves protecting sensitive data from unauthorized access and breaches, which is paramount in sectors like finance and healthcare where data privacy is a legal and ethical requirement. Conversely, OT prioritizes availability first, emphasizing the need for continuous operation and minimal downtime in industrial and manufacturing environments, where any interruption can lead to significant operational

disruptions or safety hazards (Prinsloo, Sinha, and von Solms 2019). Stouffer et al. (2015) exemplify these different focuses by stating that confidentiality and integrity are fundamental for IT, whereas human safety and operations protection are vital for OT. Furthermore, the differences between standard communication protocols in IT and the proprietary ones in OT are mentioned as important differences impacting updates or patches. IT systems can be updated automatically, while OT systems need to be closed for maintenance.

As a consequence, updates of OT systems cannot be done as frequently as those of IT systems and must be scheduled well in advance (Stouffer et al. 2015). The lifespan of the components in IT and OT differs radically. Laptops have a lifecycle of around three to five years, while OT components have a lifecycle of fifteen to twenty years or more (Stouffer et al. 2015). Murray, Johnstone, and Valli (2017) concluded that these different orientations and priorities between IT and OT pose a substantial challenge, leading to significant logical problems in information security, particularly for interconnected industrial systems and networks.

## Information Security Organization and Challenges

This study aims to compare the perspectives of IT and OT professionals in the context of information security. Using the CIA triad—encompassing confidentiality, integrity, and availability—as an analytic lens, we examine the priorities and challenges encountered by IT and OT professionals in critical infrastructure settings.

The roles of informants from service providers in critical infrastructure, namely, OT security advisor (advisor), business developer (developer), and information security coordinator (coordinator), contributed with different perspectives on the topics of the empirical study. In particular, the interpretation of information security varied between the advisor and the coordinator:

> Advisor: I do not consider OT as a part of information security. Security is easier in IT….You have more automation, and you dare to react to things automatically. In OT, you don't. Just due to the nature of OT, you need to be more reactive.
> Coordinator: A term that covers "the organizational security, guidelines, routines, and the technical security…."

The informants generally used descriptions of information security that aligned with their responsibilities. For instance, the developer highlighted assets and processes, the coordinator stressed risk management, and the advisor focused on responsibilities and shared definitions. Consequently, suggestions on how information security should be applied also reflected the point of view of the role. For example, the developer proposed iterations and systematic processes customized for the organization, the advisor recommended clarity in acceptable risk levels that the organization is willing to take, and the coordinator encouraged a top-down approach to controlling documents and routines.

Under the conditions that it is a team effort in an organization, the diverse reasoning collectively captures a broader perspective of information security, emphasizing the need to avoid approaching IT and OT separately (Wisniewski et al. 2022). However, the advisor has experienced problems with different roles that do not share the organizational or technical language, exemplifying the situation with a metaphor:

> Advisor: "It is like being a marriage advisor. First, you have to get these different groups to talk to each other and to understand what the other is saying."

The informants' reasoning on challenges related to information security highlighted the necessity to understand vulnerabilities related to the production processes and approach those in a goal-oriented way. The developer explained that if they come up with solutions for risks, they *imagine* there are "tend to be very wasteful of money and time." Instead, the informants suggested that the number of incidents would be a meaningful measure to evaluate if the information security is good enough, that is, following the logic that no incident equals sufficient security. However, after some thought, the coordinator added that this idea could only be true under the conditions of "having the ability to detect the incidents." On this topic, the advisor concluded, "There is always too much security until it is too little."

The reasoning from these service providers captures a difference between the formal and regulatory organization of critical infrastructure and the entrepreneurial and challenge-driven model of cybersecurity adversaries. The coordinator exemplified that organizations have guidelines and routines to follow, and a request has to be made to make changes in the systems. The developer clarified that awareness of an increased and changing threat landscape among upper management, one level down and on sites, exists and that this is because "someone has identified [phishing] emails…." The advisor explained that cybercriminals would quickly adapt to the organization's resistance: "the more you protect yourself, the more effort they put in." In the case of being under attack, the informants explained that they have routines and plans for how to react to a number of expected threats, but in an actual situation, they stressed that experience and instinct would matter. The organizations have established Security Operation Centers to detect and respond to incidents.

The informants generally reasoned in favor of structure, routines, and guidelines but also problematized the division of work, where communication between departments and within departments becomes too relationally complex.

> Advisor: "We are one department, but we have different systems for different business areas."

The coordinator described the division of work as a challenge in implementing security measures: "further down the organization they are not positive to information security." This expression can also indicate problems with a top-down approach, in which policies or

recommendations might not meet the requirements of practical usability at the intended level in the organization. The coordinator elaborated further on the topic of IT and OT security awareness:

> Coordinator: Those who work with the most vital systems prioritize information security. Absolutely. They understand that we need to have it like this. But, those who work in HR or administration in general…[searching for an appropriate word]…is not equally…[aware on a daily basis].

Besides highlighting the reasoning about IT and OT environments as different from each other, the explanation can be interpreted to align with the differences in prioritization of security focus (Murray, Johnstone, and Valli 2017; Stouffer et al. 2015; Zhu, Joseph, and Sastry 2011). On the one hand, the risks of loss of human life and inevitable damage to equipment and, in some cases, also nature give a more urgent feeling of security than a potential loss of business data and information, for example, observable equipment in production versus the intangible, non-visible data and information. On the other hand, from an OT point of view, the mindset of an air gap gives a false sense of security (Murray, Johnstone, and Valli 2017), perhaps missing the risks of external service personnel using maintenance aids (Hemsley and Fisher 2018; Knapp and Langill 2014), for example, cloud-based support.

When touching upon the future, the informants reflected on IT and OT convergence. The differences in lifecycles were discussed, especially the challenges to updating the sometimes *thirty-year-old* OT equipment with *cheap stuff* like sensors and how to manage patches or not in that environment. Further, they foresee *increased use of non-approved systems*, especially for easy access to service. Thus, the informants found interconnections and networks inevitable since they had already experienced the change.

> Developer: IT and OT are starting to merge; there is no question about it. By that, I mean that the technology used becomes collective and that systems, of course, merge and communicate with each other. This creates a lot of consequences for security. Some good, some bad. [The IT and OT environment] is then no longer so different, in the way they are different today, technology-wise.

> The advisor concluded that the future needs a holistic view to "put general security on the top of the agenda…not just something that removes risk, but something that creates opportunities."

## Concluding Reflective Discussion

The purpose of the study presented in this article was to investigate how critical infrastructure service providers perceive and explain information security and challenges in light of an IT-OT interconnected Industry 4.0 context. The study included empirical data from three

organizations and can, thus, conclude indicatively on these cases in relation to the literature. We embarked on Industry 4.0 as it was introduced to service providers of critical infrastructure. The informants' descriptions support the idea that interconnections, networks, and system integration between IT and OT are examples of such digitalization in critical infrastructure (Le Moigne 2021; Ustundag and Cevikcan 2018). Furthermore, the informants express the inevitability that their organizations will encounter such a future and the information security challenges it will bring.

We have used the term information security in its broadest sense, thus following the thought that information security and cybersecurity overlap (Von Solms and Van Niekerk 2013). The empirical data indicate that, from an OT perspective, information security generally relates to IT. At the same time, such a point of view will also impact future security measures in an OT environment due to the merging of the technologies. However, the informants do not mention cybersecurity as a more appropriate term for OT but rather point toward their prioritization of safety, that is, protecting humans and equipment from damage. This aligns with the suggested differences in security focus (Stouffer et al. 2015).

A difference in the security approaches mentioned is the IT automation of patches or updates, while OT equipment demands scheduled updates and maintenance stops. A challenge is, thus, the risk management of completely different types of equipment and business functions. The informants differentiate IT from OT, for example, with respect to the equipment's length of lifecycle, which raises a challenge to digital integration in old but well-functioning equipment (Stouffer et al. 2015). Also, the benefits of having plans, guidelines, and so on, have been explained by the informants. Still, when reflecting on the threat landscape, they indicate that, compared to cyber criminals, the formal procedures have limitations in managing new threats and changes in their operations. Another challenge for the future is thus to adapt new procedures while still safeguarding the formal ones, for example, managing the security connected to established and innovative technologies.

Finally, there is a challenge in approaching IT and OT information security jointly. As found in our study, the informants (naturally) see problems, challenges, and solutions from their role and their responsibility and do not have a language to support experience sharing. Thus, it prevents the desired learning from the two environments. The differences in culture between IT and OT departments are likewise indicated in a previous study (Murray, Johnstone, and Valli 2017), where the work of Hofstede (1998) supported the analysis showing that the organizational culture with respect to time horizons is entirely different.

An interpretation of the manifold descriptions that differentiate IT from OT, and vice versa, is that it might happen due to the manifestation in two very different environments, for example, machines operating at a site versus people working in an office, or a technical versus a social or organizational perspective. For example, IT departments typically focus on data integrity, confidentiality, and availability, often dealing with rapid change and software-centric solutions. On the other hand, OT prioritizes the safety and reliability of physical operations and

machinery. Changes in OT environments are often slower due to the need for stability and safety in physical processes. This results in different priorities and approaches to problem-solving, leading to a potential disconnect in understanding and collaboration. Our study indicates that there are traces of a culture not only based on differences in IT and OT environments but also in the sense of "we" versus "them," despite belonging to the same organization and being exposed to similar risks and threats about digitalization. The differences in priorities and approaches can foster a mentality where each group views the other as having different, sometimes conflicting, objectives. The separation between IT and OT can be viewed in light of a traditional diversion of office work and production; however, in other industries, digitalization has faded such differences by making the physical sites more similar. Wisniewski et al. (2022) have concluded that approaching IT and OT holistically is necessary for academia and practice. To achieve this, we might need to look beyond the obvious, that is, the fact that the environments traditionally are technically different and start to approach human attitudes and behavior seriously from an information security perspective.

Based on this concluding reflection, we suggest three future research directions that expand information security practice, addressing challenges related to behavior and organizations. First, an in-depth investigation of how different roles impact the practice of Industry 4.0 security in critical infrastructure seems valuable. This expansion can be achieved by diversifying the array of roles and sectors studied, thus addressing existing research gaps and providing a more holistic understanding of the security landscape. Future methodologies might include a combination of qualitative interviews and quantitative analyses across these varied sectors. From this direction, it would be interesting to better understand how different experiences and expertise can be applied to improve communication in risk management teams.

Second, a study where IT and OT are addressed with respect to a model for organizational learning is an interest for own further studies. From this perspective, analyses based on organizational learning theories could shed light on how, for example, reactive incident management could aggregate training tools for increasing entrepreneurial thinking in planning protection.

Third, investigate IT and OT from a norm-critical perspective. That is, finding out which norms and attitudes prevail in IT and OT, respectively—for instance, examining how the risk-averse culture in OT sectors such as oil and gas contrasts with the more agile IT culture in tech startups. From this direction, knowledge could be generated about how norms impact information security practices, thereby resulting in better insights into the air gap mindset. Understanding these cultural differences could pave the way for more integrated and effective security practices across both domains.

## Acknowledgment

The support from Interreg Aurora for the ISSUES project was gratefully acknowledged.

## AI Acknowledgment

The authors declare that generative AI or AI-assisted technologies were not used in any way to prepare, write, or complete essential authoring tasks in this manuscript.

## Informed Consent

The authors have obtained informed consent from all participants.

## Conflict of Interest

The authors declare that there is no conflict of interest.

## REFERENCES

Ackoff, Russell L. 1989. "From Data to Wisdom." *Journal of Applied Systems Analysis* 16 (1): 3–9.

Bhardwaj, Akashdeep, Varun Sapra, Aman Kumar, Naman Kumar, and S. Arthi. 2020. "Why Is Phishing Still Successful?" *Computer Fraud & Security* 2020 (9): 15–19. https://doi.org/10.1016/S1361-3723(20)30098-1.

Dragos. 2022. "2022 ICS/OT Cybersecurity Year in Review Report." https://www.dragos.com/year-in-review/.

ENISA. 2022. *ENISA Threat Landscape 2022: July 2021 to July 2022*. Luxembourg: Publications Office.

Giles, Martin. 2019. "Triton Is the World's Most Murderous Malware, and It's Spreading." *MIT Technology Review*, March 5, 2019. https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/.

Greenberg, Andy. 2018. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *WIRED*, August 22, 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Hahn, Adam. 2016. "Operational Technology and Information Technology in Industrial Control Systems." In *Cyber-Security of SCADA and Other Industrial Control Systems*, edited by Edward J. M. Colbert and Alexander Kott, 51–68. Advances in Information Security. Cham, Switzerland: Springer International Publishing.

Hemsley, Kevin, and Ronald Fisher. 2018. "A History of Cyber Incidents and Threats Involving Industrial Control Systems." In *Critical Infrastructure Protection XII: ICCIP 2018*, edited by Jason Staggs and Sujeet Shenoi, 215–242. IFIP Advances in Information and Communication Technology, vol. 542. Cham, Switzerland: Springer.

Hofstede, Geert. 1998. "Attitudes, Values and Organizational Culture: Disentangling the Concepts." *Organization Studies* 19 (3): 477–493. https://doi.org/10.1177/017084069801900305.

Jaatun, Martin Gilje, Lars Bodsberg, Tor Olav Grøtan, and Marie Elisabeth Gaup Moe. 2020. "An Empirical Study of CERT Capacity in the North Sea." Presented at the 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Dublin, June 15–19, 2020:1–8. https://doi.org/10.1109/cybersecurity49315.2020.9138865.

Knapp, Eric D., and Joel Thomas Langill. 2014. *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. Waltham, MA: Syngress.

Lasi, Heiner, Peter Fettke, Hans-Georg Kemper, Thomas Feld, and Michael Hoffmann. 2014. "Industry 4.0." *Business & Information Systems Engineering* 6 (4): 239–242. https://doi.org/10.1007/s12599-014-0334-4.

Le Moigne, Rémy. 2021. "The Power of Digital Technologies to Enable the Circular Economy." *Circulate* (blog), July 16, 2021. https://medium.com/circulatenews/the-power-of-digital-technologies-to-enable-the-circular-economy-5471d097ee7f.

Liska, Allan, and Timothy Gallo. 2016. *Ransomware: Defending against Digital Extortion*. Sebastopol, CA: O'Reilly Media.

Mason, Jennifer. 2017. *Qualitative Researching*. London: Sage.

Miles, Matthew B., and A. Michael Huberman. 1994. *Qualitative Data Analysis: An Expanded Sourcebook*, 2nd ed. Thousand Oaks, CA: Sage Publications, Inc.

Moteff, John, Paul Parfomak. 2004. "Critical Infrastructure and Key Assets: Definition and Identification." *Congressional Research Service*. https://sgp.fas.org/crs/RL32631.pdf.

Murray, Glenn, Michael N. Johnstone, and Craig Valli. 2017. "The Convergence of IT and OT in Critical Infrastructure." Presented at The Proceedings of 15th Australian Information Security Management Conference, edited by C. Valli; Edith Cowan University, Perth, Australia, December 5–6, 2017:149–155. https://doi.org/10.4225/75/5A84F7B595B4E.

Ortega-Gras, Juan-José, María-Victoria Bueno-Delgado, Gregorio Cañavate-Cruzado, and Josefina Garrido-Lova. 2021. "Twin Transition through the Implementation of Industry 4.0 Technologies: Desk-Research Analysis and Practical Use Cases in Europe." *Sustainability* 13 (24): 13601. https://doi.org/10.3390/su132413601.

Patton, Michael. 2002. *Qualitative Research and Evaluation Methods*. London: Sage.

Prinsloo, Jaco, Saurabh Sinha, and Basie von Solms. 2019. "A Review of Industry 4.0 Manufacturing Process Security Risks." *Applied Sciences* 9 (23): 5105. https://doi.org/10.3390/app9235105.

RealWorldCyberSecurity. 2020. "What Are the Fundamental Services Provided by Security? Hint: CIA Is Not the Answer." *Medium*, April 27, 2020. https://medium.com/@RealWorldCyberSecurity/what-are-the-fundamental-services-provided-by-security-hint-cia-is-not-the-answer-413d1a0355d.

Sander, Barrie. 2019. "The Sound of Silence: International Law and the Governance of Peacetime Cyber Operations." Presented at the 2019 11th International Conference on Cyber Conflict (CyCon), IEEE, Tallinn, May 28–31, 2019, vol. 900:1–21. https://doi.org/10.23919/CYCON.2019.8756882.

Schwab, Klaus. 2017. *The Fourth Industrial Revolution*. New York: Currency.

Silverman, David. 2000. "Analyzing Talk and Text." In *Handbook of Qualitative Research*, 2nd ed., edited by N. K. Denzin and Y. S. Lincoln, 821–834. Newbury Park, CA: Sage.

Smart Service. 2015. *Smart Service Welt—Recommendations for the Strategic Initiative Web-Based Services for Businesses*. Final Report.

Stallings, William, Lawrie Brown, Michael D. Bauer, and Arup Kumar Bhattacharjee. 2012. *Computer Security: Principles and Practice*. Upper Saddle River, NJ: Pearson Education.

Stouffer, Keith, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, and Adam Hahn. 2015. *Guide to Industrial Control Systems (ICS) Security*. NIST Special Publication 800-82:1–247. https://doi.org/10.6028/NIST.SP.800-82r2.

Tukker, Arnold. 2004. "Eight Types of Product–Service System: Eight Ways to Sustainability? Experiences from SusProNet." *Business Strategy and the Environment* 13 (4): 246–260. https://doi.org/10.1002/BSE.414.

Ustundag, Alp, and Emre Cevikcan. 2018. *Industry 4.0: Managing the Digital Transformation*. Springer Series in Advanced Manufacturing. Cham, Switzerland: Springer International Publishing.

Verizon. 2023. *2023 Data Breach Investigations Report*. https://www.verizon.com/business/resources/reports/dbir/.

Von Solms, Basie, and Rossouw Von Solms. 2004. "The 10 Deadly Sins of Information Security Management." *Computers & Security* 23 (5): 371–376. https://doi.org/10.1016/j.cose.2004.05.002.

Von Solms, Rossouw, and Johan Van Niekerk. 2013. "From Information Security to Cyber Security." *Computers & Security* 38:97–102. https://doi.org/10.1016/j.cose.2013.04.004.

Wisniewski, Michal, Bartlomiej Gladysz, Krzysztof Ejsmont, Andrzej Wodecki, and Tim Van Erp. 2022. "Industry 4.0 Solutions Impacts on Critical Infrastructure Safety and Protection—A Systematic Literature Review." *IEEE Access* 10:82716–82735. https://doi.org/10.1109/ACCESS.2022.3195337.

Wu, Yulei, Hong-Ning Dai, and Hao Wang. 2020. "Convergence of Blockchain and Edge Computing for Secure and Scalable IIoT Critical Infrastructures in Industry 4.0." *IEEE Internet of Things Journal* 8 (4): 2300–2317. https://doi.org/10.1109/JIOT.2020.3025916.

Zheng, Pai, Zuoxu Wang, Chun-Hsien Chen, and Li Pheng Khoo. 2019. "A Survey of Smart Product-Service Systems: Key Aspects, Challenges and Future Perspectives." *Advanced Engineering Informatics* 42:100973. https://doi.org/10.1016/j.aei.2019.100973.

Zhu, Bonnie, Anthony Joseph, and Shankar Sastry. 2011. "A Taxonomy of Cyber Attacks on SCADA Systems." Presented at the 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing: IEEE, Dalian, China, October 19–22, 2011:380–388. https://doi.org/10.1109/iThings/CPSCom.2011.34.

## ABOUT THE AUTHORS

**Anton Holmström**: PhD Student, Digital Services and Systems, Luleå University of Technology, Luleå, Sweden
Corresponding Author's Email: anton.holmstrom@ltu.se

**Johan Lugnet**: Associate Professor, Digital Services and Systems, Luleå University of Technology, Luleå, Sweden
Email: johan.lugnet@ltu.se

**Åsa Ericson**: Professor, Digital Services and Systems, Luleå University of Technology, Luleå, Sweden
Email: asa.ericson@ltu.se