|  |
| --- |
| **Prioritizing Security Awareness in the Fourth Industrial Revolution: Strategies and Considerations** |

**Dr. Ana Buhaljoti1, Prof.Asoc. Mirela Mersini2**

1 Faculty of Economics, University of Tirana, Albania

ana.buhaljoti@gmail.com

2 Faculty of Economics, University of Tirana, Albania

mirelamersini@yahoo.com

**ABSTRACT**

**Abstract**: Industry 4.0, which is the fourth industrial revolution, includes the integration of digitized physical objects and key partners into digital ecosystems and production processes to improve industrial processes. Unfortunately, these systems have increasingly become vulnerable to cyber-attacks, and significant security risks exist in the supply chain. As a result, security awareness has become crucial to improve behavior and reinforce good security practices. To identify an effective security awareness strategy, semi-structured interviews were held with security experts in the industrial sector. The study recognized the components of security awareness strategy, including knowledge, motivation, communication, training, and evaluation. The findings emphasize the significance of the industrial culture when implementing security awareness, while the most significant challenges are the rapidly increasing digital threats and the managerial shortage of time and resources.

**Keywords:** Information security, industry 4.0, digital transformation, awareness strategy, Albania

**Introduction**

The rapid acceleration of internet connectivity has led to increased automation for organizations, such as the Internet of Things (IoT) (Oscarson, 2019). The IoT has enabled the Industrial Internet of Things (IIoT), which improves industrial processes through interconnectivity and real-time control systems (Topping et al., 2021). This shift from traditional mechanical industrial methods to digitalization has been referred to as Industry 4.0 and led to new production and supply chain management methods (Pereira et al., 2017).

However, digitalization has intensified digital threats (Oscarson, 2019), and daily reported hacker attacks on supply chains (Zave & Rexford, 2021; Topping et al., 2021). As industries increasingly connect to external networks, hackers gain access to critical processes on the supply chain (Pereira et al., 2017).

Despite this threat, many organizations still do not prioritize security reinforcements and tend to focus on technical security solutions, even though humans are often the cause of security violations (Oscarson, 2019; Corallo et al., 2022; SANS, 2018;). Therefore, it is crucial to work on security awareness to protect industrial processes. This paper aims to identify the aspects of establishing an effective security awareness strategy applied to the industrial setting of Albania.

**Theoretical Framework**

In recent years, the threat landscape for cyber-attacks has become increasingly sophisticated, and businesses need to prioritize their information security measures. (IFSEC Global 2022) Organizations often rely solely on technical solutions to safeguard their systems, without considering the human factor in cybersecurity. Hackers frequently use social engineering tactics to exploit human weaknesses and gain unauthorized access to networks and sensitive information (SANS 2018). To address this challenge, it is crucial for businesses to implement security awareness programs that educate employees on cybersecurity best practices and raise awareness of the risks posed by cyber threats.

Security awareness can be defined as the process of promoting a culture of security within an organization and encouraging employees to adopt safe security behaviors (Ali Zani, Norman & Abdul Ghani 2020). The goal is to create a security-conscious workforce that understands the importance of information security and takes proactive steps to protect against cyber threats.

Effective security awareness programs may include training sessions, simulations of real-world cyber-attacks, regular communication and reminders of security policies and procedures, and incentives for good security practices (Légard 2020). By improving employee awareness of cybersecurity risks and promoting a culture of security within the organization, businesses can significantly reduce the risk of successful cyber-attacks. (Wilson & Hash 2003)

Research has shown that there is a need for increased security awareness and strategies for industry 4.0 to prevent security breaches that can cause financial losses. (Corallo et al. 2022, Pereira, Barreto & Amaral 2017) Industrial control system (ICS) are used for critical societal functions like electricity, water supply and transportation. (Knapp & Langill 2015)

Several studies have investigated how to build cybersecurity strategies, such as Legárd (2020), Ponsard & Grandclaudon (2020), Ryttare (2019), and Da viega (2018). However, standards for cybersecurity take time to be updated, and often do not provide advice on behavioral aspects of information security. Leaders’ role in ensuring good security awareness levels can affect the entire organization (Hwang, Wakefield, Sanghyun & Kim 2021).

Security awareness review has resulted in the steps of *knowledge, motivation, communication, learning/training, and evaluation* (Oscarson 2019; Legárd 2020).

Different groups within an organization may have different *knowledge* needs regarding cybersecurity. (Oscarson 2019). Besides knowledge, it is important to understand the *motivation* that affects people's behavior, to change their awareness. People are more likely to be engaged and committed to security when they understand not only how to act but also why. (Oscarson 2019). According to Kuppusamy et al., 2019 the most widely used motivation theory in information security behavior studies is the Protection Motivation Theory (PMT). PMT proposes that people's behavior is influenced by two main factors: threat appraisal and coping appraisal. (Kuppusamy et al., 2019)

Threat appraisal refers to individuals' perception of the severity of a potential threat. The more severe the perceived threat, the more motivated individuals are to protect themselves from it. Intrinsic and extrinsic rewards can also influence individuals' motivation to protect themselves.

Coping appraisal, on the other hand, refers to the evaluation of individuals' ability to manage and handle the threat. If individuals believe that the recommended behavior will effectively reduce the threat and they have the skills and resources to implement it, they are more likely to comply with security policies and procedures. (Kuppusamy et al., 2019)

Security policies are sometimes hidden or have very technical language (Oscarson 2019). Studies have shown that information security policies that are written in an easy and clear way are more effective in promoting compliance behavior among employees (Li et al., 2019; Legárd, 2020; Lundgren & McMakin, 2009; Oscarson, 2019). If policies are too technical or difficult to understand, employees may avoid security altogether, increasing the organization's vulnerability to cyber-attacks. A technical background may not always be sufficient to convey complex security concepts to employees who may have little or no technical expertise. As reported by SANS (2019), approximately 80% of security awareness professionals have a technical background but lack adequate communication skills.

According to Lee (2022), dialogic internal *communication* can encourage employees' safety behaviors in the workplace. This can be achieved by engaging employees in two-way conversations to identify and address their concerns. (Men & Yue (2019), Tao, Lee, Sun, Li & He 2022)

Providing practical exercises and real-life scenarios can also help employees understand the importance of security and how to act in a secure manner (Thomas 2014). Moreover, learning and training should not be a one-time event but rather an ongoing process to reinforce security awareness among employees and keep their knowledge up to date.

Oscarson (2019) emphasizes that *measuring* awareness activities is necessary to understand the impact of security awareness on employees' behavior. Measuring only knowledge may not provide an accurate representation of actual behavior, as highlighted by Fertig, Schütz, and Weber (2020). Therefore, organizations should develop customized metrics that align with their specific context and goals (Arabsorkhi & Ghaffari, 2018; Légard, 2020). Programs sometimes lack support from their operations and finance departments and the main reason why transformation fails is internal resistance (Reynolds 2020)

*Evaluating* security awareness programs is essential to understand their effectiveness, and customized metrics should be developed to align with organizational goals. (Legárd, 2020; Oscarson, 2019)

The literature review indicates a gab in security awareness strategy to increase security for industry 4.0.

**Research Method**

The use of interviews as a data collection technique allows for in-depth exploration of participants' perceptions and experiences (Myers, 2020). Semi-structured interviews allowed for a balance between a predetermined set of questions based on the theoretical framework (knowledge, motivation, communication, learning/training, and evaluation) and the ability to explore emerging themes or issues during the conversation.

Five experts were interviewed for their insights and experiences in both the information security fields. All experts were chosen based on their role as security responsible in the industry with knowledge and experience in the security building process.

The data analysis process involved transcribing the recorded interviews and conducting a thematic analysis of the data (Spencer et al., 2014). Thematic analysis is a flexible method that can be used in a range of research contexts and allows for the identification of patterns and themes in the data (Braun & Clarke, 2021). The use of a thematic analysis in this study allowed for the identification of common themes across the participants' responses, which were organized into the five categories of the theoretical framework.

**Results**

In relation to digital threats, participants mentioned the rapid pace of digitalization, while emphasizing the ransomware attacks and encryption viruses. Legislation and security standards often lag the knowledge of hackers and cybercriminals.

Expert 1: *“There seems to be a perpetual lag in legislation and security standards, and it appears that hackers and criminals are consistently ahead in terms of their knowledge and skills. It's unclear why this is the case, but it's a concerning issue that needs to be addressed.”*

The findings support previous studies that digitalization has increased the level of digital threats (Oscarson, 2019)

All of the participants highlighted the lack of security culture in industries.

Expert *5: “The industry is behind. Traditional companies that have been forced to enter digitalization to keep up with the market”.*

Expert *4 “We are behind in the security aspects”.*

Expert *2: “Industry workers are not out working with computer on a daily basis”*

These results confirm that industrial security is very problematic since security has not been a priority for industrial control systems evolvement.

All security experts mentioned that security is still not prioritized.

Expert 3 expressed that *“changing people's bad security habits is challenging, especially if they consider those habits effective way of working. De-effectivizing their way of working leads to resistance.”*

On the other hand, Expert 4 noted that the biggest challenge is the existing noise in the organization. *“It is not just the security department that is trying to communicate to employees, but also other departments such as HR, communication, economy, quality, and environment are competing for their attention.”*

The results confirm that organizations need to prioritize security reinforcements.

***Knowledge***

Concerning which knowledge needs to be taught to employees to become more security aware, all the informants agreed to work with knowledge in different levels. Four experts also mentioned sharing knowledge about security breaks. An example of these results are the following comments:

Expert 1 and 2 mentioned the importance of having a baseline level of security measures in place, but also emphasized that *“ there is a need for tailoring security efforts to the specific composition and level of knowledge of the staff group”.* They stated that the security measures presented must be relevant and practical for the group being addressed. Drawing a parallel to physical safety, Expert 2 likened this approach to the way fire safety measures are implemented and suggested that security awareness efforts can take inspiration from this approach.

Expert 5 “*we are not good at sharing our own mistakes”. “If we are going to get better in this I think that we need to be sector wise and share experiences and knowledge”.*

These results confirm what research is saying, that it is important for organizations to understand threats specific to a sector or organization.

***Motivation***

Regarding aspects to motivate the employees to become more security aware, three of the informants highlighted the importance of making inclusive and interactive activities.

*Expert 2: “I think that the most important motivation is comprehending the reason behind what we are doing”.*

*Expert 3: "If there is a collaboration or interaction, people are more likely to remember and engage."*

*Expert 4: To promote people's engagement is more effective.*

These results emphasize the importance of users recognizing the relevance of the subject to them.

***Communication***

When asked about who should lead the security awareness work, and what qualities are necessary for them to possess, four informants answered communication.

*Expert 1:* *In my opinion, effective communication is the key to success in this area.*

*Expert 4 “I think that it is good if the awareness work is led by a central security function*

*Expert 5“It has a lot to do with communication abilities and conveying a message”.*

According to three interviewees, “*it is essential to involve leaders in training activities”*. This confirms that leaders have a crucial role in promoting security awareness in organizations, as their behavior and decisions can affect the entire organization.

***Learning and training***

Regarding how to learn and train information security knowledge, security experts mentioned different types of activities.

Examples are the following comments:

*“Attending training courses, workshops or seminars*

*Discussing security topics with colleagues or peers*

*Participating in security competitions or hackathons*

*Sharing knowledge or experiences in communities*

*E - Learning”*

***Evaluation***

Concerning how to evaluate security awareness, few respondents mentioned techniques to evaluate knowledge or behavior.

The results confirm that measuring awareness is neglected.

Examples are the following comments:

*Expert 4: “The evaluation is a challenge and needs to be done among departments.”*

*Expert 5: “I believe that incorporating discussions and understanding of how people work, and whether they are engaged in these topics and groups, should be integrated into daily work.”*

The evaluation of security awareness should include measurements of knowledge and behavior, while only one respondent recommended assessing soft character traits.

**Discussion and Implications**

The research results have shown that one of the biggest digital threats for industries in Albania is the changing industrial processes and that the biggest security awareness challenge is the industrial culture.

The findings suggest that the rapid pace of digitalization poses a significant digital threat, while security measures are not keeping up with the same pace. It is crucial to involve leaders in the security awareness process, as they play a crucial role in influencing employees. However, some of the significant challenges faced by managers include a lack of time and resources, not seeing the value of security awareness, and psychological barriers. In terms of knowledge aspects, it is essential to teach information security knowledge at different levels and share it across organizational boundaries. Motivational aspects should also be considered, with interactive and context-specific activities being preferred. Experts suggested making learning and training activities interactive, enjoyable, and encouraging people to learn and share knowledge.

It is also important that managers assess culture changes and evaluate security awareness, knowledge and behavior of employees.

The findings can be applicable to security awareness efforts in other nations, as aligning security awareness strategies with the organization's culture has a significant impact.

**References**

Ali Zani Azma Alina, Norman Azah Anir & Abdul Ghani Norjihan (2020). Chapter 6 - A review of security awareness approaches: Towards achieving communal awareness. In Benson,Vladlena & Mcalaney, John. Cyber Influence and Cognitive Threats. *Academic Press*, Pages 97-127, https://doi.org/10.1016/B978-0-12-819204-7.00006-3.

Arabsorkhi A. & Ghaffari F. (2018). Security Metrics: Principles and Security Assessment Methods. *9th International Symposium on Telecommunications (IST)*, 2018, Pages 305-310, doi: 10.1109/ISTEL.2018.8661030.

Legárd , Ildikó (2020). Building an effective information security awareness program*. Central and Eastern European EDem and EGov Days 338 (July):189-200.* doi: 10.24989/ocg. 338.15.

Corallo Angelo, Lazoi Mariangela, Lezzi Marianna & Luperto Angela (2022)*.* Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. *Computers in Industry*, Volume 137. 103614, https://doi.org/10.1016/j.compind.2022.103614.

Fertig Tobias, Schütz Andreas E. & Weber Kristin (2020). Current issues with metrics for information security awareness*. Twenty-Eighth European Conference on Information Systems (ECIS2020) – A Virtual AIS Conference.*

Hwang Inho, Wakefield Robin Kim, Sanghyun & Kim Taeha (2021). Security Awareness: The First Step in Information Security Compliance Behavior. *Journal of Computer Information Systems,* 61:4, 345-356, doi: 10.1080/08874417.2019.1650676.

IFSEC Global (2022). A history of information security*.* Available at: https://www.ifsecglobal.com/cyber-security/a-history-of-information-security/

Knapp Eric D. & Langill Joel Thomas (2015a). Chapter 2 – About industrial networks*.* In Knapp, Eric D., Langill, Joel Thomas. *Industrial Network Security (Second Edition).* Syngress. <https://doi.org/10.1016/B978-0-12-420114-9.00007-1>.

Knapp Eric D. & Langill Joel Thomas (2015b). Chapter 3 - Industrial Cyber Security History and Trends*.* In Knapp, Eric D.,Langill, Joel Thomas. *Industrial Network Security (Second Edition).* Syngress. <https://doi.org/10.1016/B978-0-12-420114-9.00007-1>.

Knapp, Eric D. & Langill, Joel Thomas (2015c). Chapter 7 - Hacking Industrial Control Systems*.* In Knapp, Eric D.,Langill, Joel Thomas. *Industrial Network Security* (Second Edition), Syngress, Pages 171-207. https://doi.org/10.1016/B978-0-12-420114-9.00007-1.

Kuppusamy Puspadevi, Samy Ganthan Narayana, Maarop Nurazean, Magalingam Pritheega, Kamaruddin Norshaliza, Shanmugam Bharanidharan & Perumal Sundresan (2019). Systematic Literature Review of Information Security Compliance Behaviour Theories. Published under license by IOP Publishing Ltd. *Journal of Physics:* Conference Series, Volume 1551. *2nd International Conference on Recent Advancements in Science and Technology* . 28-30.

Pereira T, Barreto L & Amaral A. (2017). Network and information security challenges within Industry 4.0 paradigm. *Manufacturing Engineering Society International Conference, MESIC, 28-30 June*. *Elsevier, Procedia Manufacturing* 13, 1253–1260.10.1016/j.promfg.2017.09.047.

Ponsard Christophe & Grandclaudon Jeremy (2020). Guidelines and Tool Support for Building a Cybersecurity Awareness Program for SMEs. Conference paper, *Communications in Computer and Information Science book series* (CCIS, Volume 1221)

Ryttare (2019) Ryttare, Emma (2019). Change Management: A Key in Achieving Successful Cyber Security-A Multiple Case Study of Organizations in Sweden*.* Luleå university of technology.

Da Veiga, Adéle (2018). An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture*.* Article in *Information and Computer Security,* doi: 10.1108/ICS-08-2017-0056.

Oscarson, P. (2019). Information Security Fundamentals. *WISE*.

Li Ling, He Wu, Xu Li, Ash Ivan, Anwar Mohd & Yuan Xiaohong (2019). Investigating the impact of cybersecurity policy awareness on employees’ cybersecurity behavior. *International Journal of Information Management* 45. 13–24. <https://doi.org/10.1016/j.ijinfomgt.2018.10.017>.

Lundgren Regina E. & McMakin Andrea H. (2009). *Risk communication: a handbook for communicating environmental, safety, and health risks.* 4th ed. Hoboken, N.J.: Wiley.

Men Linjuan Rita & Yue Cen April (2019). Creating a positive emotional culture: Effect of internal communication and impact on employee supportive behaviors. *Public Relations Review,* Volume 45. Issue 3,101764,ISSN 0363-8111, <https://doi.org/10.1016/j.pubrev.2019.03.001>.

Tao Weiting, Lee Yeunjae, Sun Ruoyu, Li Jo-Yun & He Mu (2022). Enhancing Employee Engagement via Leaders’ Motivational Language in times of crisis: Perspectives from the COVID-19 outbreak. *Public Relations Review*, Volume 48. Issue 1,102133,ISSN 0363-8111. <https://doi.org/10.1016/j.pubrev.2021.102133>.

Myers, Michael D. (2020). *Qualitative research in business & management*. Third edition London: SAGE Publications Ltd.

SANS (2018). Security report for executives*.* Available at: https://www.sans.org/securityawareness-

training/resources/reports/?msc=main-nav.

SANS (2019). 2019 Security Awareness Report. Available at: https://www.sans.org/securityawareness-

training/resources/reports/?msc=main-nav.

Spencer Liz, Ritchie Jane, Ormston Rachel, O’connor William & Barnard Matt (2014). Analysis: Principles and processes. In Ritchie Jane, Lewis Jane, McNaughton Nicholls Carol & Ormston Rachel (red.) *Qualitative research practice: a guide for social science students and researchers*. Second edition Los Angeles: SAGE.

Topping Colin, Dwyer Andrew, Michalec Ola, Craggs Barnaby & Rashid Awais (2021). Beware suppliers bearing gifts!: Analyzing coverage of supply chain cyber security in critical national infrastructure sectorial and cross- sectorial frameworks. *Computers & Security*, Volume 108. 102324. <https://doi.org/10.1016/j.cose.2021.102324>.

Thomas Valerie (2014a). Chapter 7 - Social Engineering*.* In Gardner Bill, Thomas, Valerie. *Building an Information Security Awareness Program*. Syngress, Pages 45-63. <https://doi.org/10.1016/B978-0-12-419967-5.00007-7>.

Traballesi Alberto & Bologna Sandro (2020). Iot in the context of Critical Infrastructures. *AIIC (Associazione Italiana esperti Infrastrutture Critiche)*. ISBN: 979-12-200-6977-9.

Wilson Mark & Hash Joan (2003). Building an Information Technology Security Awareness and Training Program. NIST (2003). NIST Special Publication 800-50. Available at: https://csrc.nist.gov/publications/detail/sp/800-50/final.

Zave Pamela & Rexford Jennifer (2021). Patterns and Interactions in Network Security. Princeton University*. ACM Computing Surveys,* Volume 53. Issue 6. Article No.: 118, Pages 1–37. https://doi.org/10.1145/3417988 .