*SPS2022*
*A.H.C. Ng et al. (Eds.)*

*doi:10.3233/ATDE220140*

# Improving Cybersecurity Awareness Among SMEs in the Manufacturing Industry

Kevin JOHANSSON[a], Tim PAULSSON[a], Erik BERGSTRÖM[a,1], Ulf SEIGERROTH[a]
[a] *Department of Computer Science and Informatics, School of Engineering, Jönköping University*

**Abstract.** Small and medium-sized (SME) manufacturing enterprises have been described as a sector that traditionally has not been data-intensive, with low spending on IT and cybersecurity and employees with low cybersecurity awareness. SMEs have also been described as agile and under pressure to adopt new technology and embrace digitalization to gain a competitive advantage. Entering this data-intensive world also comes with new risks, making them extra vulnerable. Not much attention has been directed at how SMEs in the manufacturing sector are working with improving employees' cybersecurity awareness. Especially not where cybersecurity training programs are in focus. To investigate these aspects, we opted for a set of five SMEs in the manufacturing industry where it was possible to perform in-depth semi-structured interviews with chief information security officers' (CISO) and employees. The results show several interesting results, for example, regarding the view on contextualization of training material and the relevance of microlearning. The study also presents several practical implications, including recommendations for improving cybersecurity training measures for SMEs in the manufacturing sector.

**Keywords.** Cybersecurity awareness, cybersecurity practices, countermeasures, training

## 1. Introduction

In this paper, we explore how small and medium-sized enterprises (SME) in the manufacturing industry are working on improving cybersecurity awareness, which is a fundamental aspect of creating resilient production in a connected world.

Manufacturing has in the last decades started to undergo a digitalization process and is now aiming at Industry 5.0. The common theme of transformation of the manufacturing sector is digitalization, connectivity, and automation which has led to an increased dependency on technologies such as the Internet of Things (IoT), cloud computing, big data and artificial intelligence, new generation robotics, and blockchain [1]. In relation to exploiting these technologies, we also see the need for business operations to become *"data-driven."* A consequence of this is that some traditional manufacturing businesses are transforming into tech companies [2]. One example of this is the automotive industry that invests in electrification, autonomous vehicles, and

[1] Corresponding Author, Erik Bergström; E-mail: erik.bergstrom@ju.se.

connectivity [2]. Another example is additive manufacturing (AM), which gives manufacturers more flexibility through technology [3].

With the ongoing digital transformation comes both opportunities and challenges, and companies need to handle challenges at the same time as they are exploiting opportunities. A challenge that has received much attention is cybersecurity to prevent unintentional and intentional security incidents. Unfortunately, firms have promoted digitalization investments and, to some extent, ignored cybersecurity investments, and we see daily attacks on the manufacturing industry [4].

A recent study carried out by Franke and Wernberg [4] in collaboration with the Association of Swedish Engineering Industries showed that the implementation of cybersecurity measures is still in its infancy in Swedish manufacturing industries. Their study also revealed deficiencies in organizational and social cybersecurity measures as technological countermeasures were favored. This is critical since, in an industrial setting, the employees would be the easiest point of entry to exploit and get into a company's system and network [5].

This work aims to investigate how SMEs in the manufacturing industry are dealing with cybersecurity awareness, and therefore we have formulated the following research question.

RQ: *How can cybersecurity awareness be improved among SMEs in the manufacturing industry?*

## 2. Background

Connecting IoT devices to the Internet and becoming data-driven or data-intensive has brought fantastic opportunities to the manufacturing industry. But at the same time, it has also come at the cost of security-related issues. In many cases, the development of technological solutions such as firewalls, anti-phishing software, and authentication mechanisms to keep hackers out is handled in a reactive and *"must-do"* manner. Still, we know that they do not guarantee a secure environment for information and that hackers prefer to target humans rather than computers [6].

Humans have for a long time been known to be a weak link – if not the weakest link – from a security perspective. We click on links and attachments, make mistakes entering information, share our username and password, despite knowing that we shouldn´t. To manage the human aspects of cybersecurity, organizations utilize a combination of technology and administrative countermeasures, such as directives and information security policies (ISP) [6, 7]. An ISP is often seen as an essential starting point used by most organizations as it outlines the security-related rules and requirements [7].

### *2.1. Cybersecurity in manufacturing*

More connectivity and reliance on data to run manufacturing operations have drastically increased the need for improved cybersecurity. All types of organizations struggle to make their employees more aware of potential cybercrimes and improve their cybersecurity awareness [8]. However, employees in manufacturing have been described as lacking specialist talent, having low awareness, only possessing basic cybersecurity competence [1], and might be unfamiliar with cybersecurity concepts [9]. In a study investigating employees' ISP awareness and compliance, the manufacturing industry scored lowest of the investigated industries [10]. This is not especially surprising as the manufacturing industry traditionally has been described as a non-data-intensive industry, and therefore less focus has been directed to cybersecurity [10].

Digitalization has opened up many new attack vectors for actors with malicious intentions. Moving work procedures from companies to the cloud has made many company-specific countermeasures ineffective [1]. The number of entry points for user access has multiplied by the introduction of IoT devices [1]. More IoT devices and increased connectivity has led to increased vulnerabilities [11]. The IoT devices and sensors can be used to add data-driven capabilities to existing equipment and gather data about the manufacturing process and human behavior, helping to add *"smart"* to industries and their processes. The increased connectivity has also led to new attack vectors in control systems such as SCADA (Supervisory Control And Data Acquisition) that were originally designed to work in closed networks [11].

Phishing, i.e., where a fraudulent email is sent to someone intended to trick the receiver into revealing sensitive information or deploying malicious software, is another example of how digitalization has created a new attack vector. Phishing attacks have been around for decades and are considered one of the primary attack vectors [12] and a type of attack that is increasing [13, 14]. It is difficult to protect against phishing attacks as it attacks humans [15]. It might be specifically problematic in the manufacturing sector since the attack is directed towards a workforce with a low degree of cybersecurity maturity [9] and where technology will not prevent this kind of attack.

Also, new types of manufacturing, such as AM, bring new and unique vulnerabilities [3]. AM has helped to reduce the time for prototyping and, at the same time, help the production of complex parts [16]. However, the flexibility that comes with AM has given attackers new possible attack vectors [16]. Several researchers have raised concerns regarding the security aspects of AM. For example, attacks on AM could lead to compromised components in critical systems, where even human lives could be endangered [17] or the loss of intellectual property [18].

### *2.2. Cybersecurity awareness and compliance*

A critical brick in the cybersecurity wall is the ISP. Unfortunately, it is not enough to just have an ISP because the employees also need to comply with it. Compliance is central in organizations, and ISP compliance has proven to be an effective and efficient approach to mitigate the risk of security breaches [6]. Employees' cybersecurity awareness is seen as crucial in mitigating risks associated with their behavior [6], and studies such as Li, Zhang et al. [19] and Webb, Ahmad et al. [20] have shown that organizations oversee to focus on the employees' compliance fail to succeed in their efforts.

In this work, we use cybersecurity awareness synonymously to the term information security awareness, which can be defined as *"an employee's general knowledge about information security and his cognizance of the ISP of his organization."* [7, p. 532] The first part that describes general knowledge targets an employee's overall knowledge and understanding of potential information security issues and their ramifications. The second part targets knowledge and understanding of the requirements prescribed in the ISP and the aims of those requirements [7].

There are several different models (e.g. [7, 21, 22]) with different levels of detail outlining the central concepts in cybersecurity awareness and their interdependencies. Common for these models is that cybersecurity awareness increases with education and training and improved compliance to the ISP as an effect. This is hardly surprising as the first step to compliance is to be aware as it is impossible to comply with something unknown or not understood. Education and training improve employees' knowledge about cybersecurity, affecting attitudes positively towards cybersecurity compliance [6, 23, 24].

Besides education and training, several other factors, such as the industry type and the organization's size, play a role in an employee's intention to comply with the ISP [7]. Smaller-sized organizations (SMEs) generally have less emphasis on ISP compliance [7]. Reasons for this could include that SMEs are big adopters of digital technologies to stay competitive and because they might believe their insignificant size makes them not worth being attacked [25]. As previously mentioned, employees in the manufacturing industry have lower cybersecurity awareness than other industries [10], and employees are characterized by having only basic cybersecurity competencies such as password storage and phishing emails [1]. The lack of cybersecurity awareness and compliance might be critical pieces in the puzzle on why the manufacturing industry is exposed to many security breaches [26].

Companies generally use three types of control to achieve compliance: coercive, remunerative, and normative [27]. With coercive controls, threats and punishments (i.e., the *"stick"* in carrot-and-stick) are used to achieve compliance. With remunerative controls, incentives such as bonuses or promotion (i.e., the *"carrot"*) are used in exchange for compliance. When normative controls are used, the focus is on moral reasoning, and the values behind compliance are emphasized [27]. The most effective controls are widely discussed, and studies have shown inconsistent findings [28], and there are many calls for more research on achieving compliance [28, 29].

Finally, it is also essential to mention what motivates employees to comply with the ISP. Research has shown that two types of motivation are put forward, extrinsic and intrinsic [30]. Extrinsic motivation could be carrots and sticks, such as sanctions, rewards, and social pressure [31]. Intrinsic motivation, such as the perceived effectiveness and self-efficacy to perform security tasks and the perceived ownership of an information system, affect employees' actions. Intrinsic motivation has been pointed out as an area that needs more empirical research [30, 32].

### *2.3. Cybersecurity training programs*

The value of cybersecurity training and education cannot be emphasized enough. For many types of attacks such as phishing, the best countermeasure to mitigate or prevent is cybersecurity training and education [9, 33]. In this work, we focus on cybersecurity training and not cybersecurity education. The reason is that education has been described as more in-depth, targeting cybersecurity professionals using more theoretical delivery methods such as seminars, classroom discussions, and research [34]. On the other hand, training has been described as equipping employees with knowledge specific to their roles and responsibilities using more practical delivery methods such as seminars and workshops [34]. For training to be effective, it needs to be designed in a way that the employees can relate to it [8] and so that it supports the business context of the organization [35] and uses a variety of delivery methods [8]. Abawajy [36] describes six types of delivery methods, conventional (for example, leaflets, posters, and newsletters), instructor-led (for example, workshops, lectures, and presentations), online (for example, email, blogging, and screensavers), game-based, video-based, and simulation-based. A similar division of delivery methods is presented by Al-Daeef, Basir et al. [37].

There is evidence that online and game-based delivery methods are picking up pace. For example, microlearning has become increasingly popular. Microlearning can be described as a learning approach that delivers compact and focused information about a specific idea [38]. In cybersecurity, it can be small web-based educational nuggets about a particular topic, e.g., a small phishing module aimed at increasing employee awareness. Many aspects of microlearning are still unknown, but it is clear that it is a cost-effective and fast training approach that can cover many organizational needs [39]. There are also some challenges related to microlearning. For example, it might not be suitable for all subject matters, relies heavily on contextualization, adaptation [40], and might be limited to achieve deep learning [39]. However, the knowledge about the effects of using microlearning in companies is scarce, and most literature in the field can be found in managerial magazines rather than academic papers [39].

From a general cybersecurity training perspective, the training programs have not been as effective as intended. Research points out that training programs are not empirically grounded [37, 41] and that there is a need for further research in the area [42].

## 3. Method

This work focuses on how manufacturing organizations are working with improving cybersecurity awareness and how the employees perceive it. Such focus suggests a qualitative interpretative approach and an explorative case study [43]. Yin [43] differentiates various kinds of case studies: explanatory, exploratory, and descriptive. The case studies are to be considered exploratory, as they are used to explore cybersecurity awareness and compliance.

In the domain of cybersecurity awareness, much of the knowledge comes from survey research, especially when the manufacturing industry is in focus. To gain an understanding of user perceptions in the manufacturing sector, sampling based on a few respondents possessing expertise in the chosen area was performed [44, 45]. Here, a saturation of the selected topic, where patterns in the answers occur, were sought after [46], not statistical generalizations. Therefore, semi-structured interviews were selected as a data collection method to be able to collect more in-depth data. The interviews were prepared following advice on preparing interviews from Bryman and Bell [47] and Oates [48]. The interviews were based on a series of open-ended questions to avoid imposing perceptions on the interviewees' answers, recording, and transcription.

In cybersecurity, it is well-known that it is challenging to collect empirical data [49, 50], and in this study, the data collection had to be specific to fulfill the aim. To capture the dynamics between CISO and employees, several requirements were set. The data collection had to be performed in (1) a manufacturing company, (2) the company had to be an SME following the European Commission's recommendation (max 250 employees) [51], (3) the company had to have a manager/CISO responsible for the cybersecurity, (4) the company had to provide access to the CISO and two employees, and (5) it had to be willing to discuss their cybersecurity awareness. More than 40 companies were contacted via email during the spring of 2021. Five companies fulfilling all the requirements were selected after discussions via email and/or telephone. From these five companies, we interviewed the CISO and two employees in all except one where only the CISO and one employee were available, in total 14 interviews. All interviews were performed via the video conferencing software Zoom.

All the collected data were transcribed and checked by two authors (99 pages) and then imported to the analysis tool NVivo for coding according to Strauss and Corbin [52].

## 4. Results

A common denominator among all the investigated organizations was the reactive approach to improving cybersecurity awareness. Several organizations described that increased phishing activity led the IT department to send out notifications when it was recognized that the organization was targeted and that the employees should be on extra alert. This was exemplified by one of the case organizations that became victims of a targeted phishing attack that led to an outage that lasted several days. After this incident, the employees were subjected to various, repeated information related to cybersecurity. The rest of this section is presented from the view of CISOs and employees.

### *4.1. Chief Information Security Officers*

All the chief information security managers (CISOs) had higher education, but they lacked formal education in information security. Four organizations had an ISP, while the fifth organization had an IT policy and an email policy filling the ISP gap. The CISOs all understood the importance of having an ISP, but at the same time, they didn't use the ISP as a natural part of their day-to-day operations. All of the organizations used the policies to inform employees what is allowed and what is not. CISO1 called the ISP a *"symbol document"* that was *"important to have* […] *but a challenge to convey."*

Several of the CISOs tried to encourage the employees to forward suspected phishing emails to them for inspection. This can be exemplified by CISO1 that explained that he did not use the carrot-and-stick approach at all but instead tried to strengthen the employees as individuals by encouraging them to do the right thing. For instance, when they forwarded emails that were suspected to be phishing emails. However, when asked about the consequences, CISO1 explained that *"everybody who has worked here for a long time knows what happens, everything shuts down. Nobody wants to be hung out. You hear them* [the employees] *talking to each other about that time someone clicked on a link and that you do not want to be that person."*

CISO3 tried to stimulate intrinsic motivation by emphasizing softer values, that they were a small company, that everyone is fighting for everyone to feel at home, that they are like a family, and that they together have to protect the company and the brand. CISO4 similarly used the advantage of being an SME by emphasizing that they were not a big company. The employees were encouraged to talk to each other and develop their social relations (get to know each other) to decrease the risk for phishing and encourage them to double-check the sender if possible.

All the CISOs worked with several delivery methods as part of their cybersecurity training programs. They had all used instructor-led methods as part of their program, and traditional instructor-led presentations were the preferred delivery method. Presentations were seen as an easy and comfortable delivery method that can go out to most staff with mandatory participation on short notice. They believed presentations were beneficial if they themselves delivered them. The reason was that they could make the presentations contextualized and adapted to their specific needs. Several had tried to engage consultancy firms for presentations, but they were generally disappointed. For example, CISO5 believed the training from a consultant to not be appreciated by the employees.

CISO1 summarized it as the *“quality was not good, even though it was a decent supplier. It was not sufficiently concise and a little too superficial.”*

Four companies used variants of microlearning, either with or without a simulation-based module that could be used to send phishing emails to employees simulating an attack. The microlearning software also had quizzes to check knowledge levels on a topic and a management interface to monitor employee progress and other stats. Several aspects were perceived as positive, the functionality and flexibility in running the software were mentioned. There was a possibility to schedule modules at specific points in time or use it self-paced. They also felt that it was possible to make the modules contextualized, but that it was hard and took a lot of time, and sometimes the software was not flexible enough. CISO2 had added own images and tried to adapt the content to their specific situation. Still, both he and the employees felt that some parts were off-topic. CISO2 even wondered about the validity of some of the content in the training modules.

The CISOs’ recognized an increased awareness among the employees through the use of microlearning and that it facilitated follow-up on training progress compared to other types of self-paced training. At the same time, CISO1 emphasized that microlearning is not a silver bullet, and even though his management wanted to roll out more microlearning, CISO1 felt that he had to slow down the pace. CISO1 wanted to be able to find a suitable concept and implementation for delivering the microlearning, and that it needs to contain the right things, with the correct language, to fit their context and culture, *“otherwise it will be quite pointless, it will have no efficiency.”*

The language and terminology challenges were extensively discussed, which also relates to making the delivery of the material contextualized. All had different levels of bad experiences related to these issues. The fundamental problem for the SME cases in this study was that most of the microlearning material is in English, which is an issue shared with other delivery formats that are readily available on the Internet. The general perception was that to be effective for all, the education must be in the local language (in this case, Swedish), but to what extent it had to be contextualized was difficult to answer. The general view was that it was enough to add local examples if existing. CISO2 had a good experience using key employees as examples. The company had most of the contact information on the web, and in combination with Sweden’s quite relaxed privacy laws, very much personal information is available online. A combination of such data was used to create a scenario to show weaknesses and how attackers can work, and how they, even as private citizens, can pose a risk to the company.

### *4.2. Employees*

The employees all lacked formal education in cybersecurity and had different backgrounds regarding higher education. It was a fragmented picture regarding the perceived usefulness of the ISP among the employees. The ISP was deemed *“fuzzy”* (Employee6), *“never seen it”* (Employee8), *“a less ambiguous would have been preferred”* (Employee5), and *“it is not related to my job”* (Employee1).

One of the employees had clicked on a suspected simulated phishing email and expected to get some reprisals (stick) from the CISO but got no response at all. This led the employee to question the CISOs compliance work and wonder if the CISO classified the click as done-on-purpose or if the organization lacked security countermeasures to detect phishing attacks. All interviews with the employees touched on the subject of what happens if you click on a phishing email, and they all felt that they would have been exposed to the organization and that they would have been made as an example. For example, Employee7 said: *"Oh no! I would have been declared an idiot. I think the worst thing is for yourself, that you felt so terribly stupid and gullible [...] I do not even want to think about it."*

The employees shared the CICOs perception that training delivered by consultancy firms was unsatisfactory because of insufficient contextualization to local requirements. The employees also believed the instructor-led presentations, regardless of the presenter, were too long, and they recommended around 15-20 minutes to stay focused on the topic. Furthermore, they could be more contextualized, even if they were delivered by a local such as the CISO. Employee2 exemplified it by highlighting that the CISO was off-topic from the perspective of many field employees in a recent presentation. The presentation was more suitable for office staff, while field workers would instead prefer to use their smartphones instead of organized in-house lectures in front of a computer. Workshops or different types of interactive meetings where discussions could take place were examples of instructor-led training that were perceived positively by the employees. The interactivity in the delivery was the main reason for the positive attitude.

Microlearning was received positively by all the employees that had experience from it. Several, however, saw microlearning as a type of *"alarm clock"* (Employee1) constituted by a module with a small, focused, and contained piece of information. Employee2 described the training modules as *"very thin"* but appreciated them as a recurring reminder to think about cybersecurity. The length of a module was also discussed, and the employees would prefer it very brief, a couple of minutes, *"something you can do quickly when you have a break"* (Employee6), was perceived as reasonable. Quizzes that immediately followed a module or came later were also appreciated because they forced them to focus on the content.

Adapting the training material to the local context was perceived as key for the employees, but they also acknowledged that this could be challenging. Even in their relatively small organizations, they had employees with very varying work tasks and backgrounds. Employee8 described microlearning as questionable from an age perspective and that this type of education should focus more on those who are a little older since they aren´t raised in the same way where usage of digital devices is a natural way of living.

## 5. Discussion

The ISP or similar was considered essential for the CISOs. Still, the importance was downplayed. On the other hand, most employees felt that it was too ambiguous or not related to them. This mismatch affects employee compliance [7]. For the same reason, the delivery methods must be contextualized. We see that the ISP also needs to be contextualized to provide a useful frame of reference for the organization and its employees. Literature mentions that one way of increasing their knowledge about the ISP is to encourage knowledge-sharing [6]. This study indicates that interactive instructor-led workshops could be a suitable delivery method to achieve that.

There was no relationship between the CISOs view on encouraging talking about incidents and the employees' perspective on this. This suggests that the carrot-and-stick approach is not very significant, but intrinsic motivation is. To stimulate intrinsic motivation, cultivating a social context and a type of family bond between the employees and the organization could be crucial, especially for SMEs. This is in line with Cheng, Li et al. [53], which revealed that employee compliance was greater among those with a stronger bond to their organization.

An essential aspect of selecting a variety in the delivery methods is that the CISOs might assume that the employees are more homogenous than they actually are. Here it can be exemplified by a CISO that believed all employees to be reachable via email, while some employees used only shared email addresses. To reach all employees in a language they can understand and using a delivery method they prefer might be a utopia. However, this study suggests that it is highly likely that increased contextualization and a mixed-use in the delivery methods should be opted for. Shorter modules, such as microlearning, were appreciated among all the interviewees, especially the CISOs, as they could track progress in a better way. At the same time, the employees also feel that microlearning was beneficial for improving awareness, but unlike the CISOs, they thought it works best as an alarm clock, which is in line with Beste [39]. The use of shorter modules also makes it possible to motivate a more frequent use of cybersecurity training, which is mentioned as a key factor in the literature. One also must acknowledge that the employees perceived cybersecurity as necessary, but so were other things in their organizations. Finding the right amount of cybersecurity training is difficult, especially since too much work on cybersecurity demands or training can lead to cybersecurity fatigue [54].

The CISOs understood the importance of contextualizing and making the content more domain-specific, partly because of bad experiences with external instructor-led training which was poorly received in their organizations. The CISOs had also identified the need to adapt the material based on groups or individuals in their organization. These insights partly came from using the management interface in the microlearning products where individual performance is tracked. Similar thoughts have been put forward by Menard and Shropshire [55]. They describe the one-size-fits-all, cost-containment strategy where a single, static course delivered to everyone is an approach with questionable effectiveness. In addition, it is essential to understand that both skill and time are general challenges the CISOs face in updating and contextualizing the training modules.

## 6. Conclusions

The result of this study nuances how cybersecurity training could be implemented to improve cybersecurity awareness. This is done by presenting a set of recommendations for the manufacturing sector. These recommendations can help balance spending on cybersecurity-related countermeasures to harvest the potential of the ongoing digitalization of the manufacturing industry. The recommendations are as follows:

- Use delivery methods that focus on short nuggets of information (modules that are small, focused, and contained). For example, microlearning was a delivery method that both CISOs and employees favored. Another favored example was traditional newsletters that can deliver short cybersecurity-related information about a specific topic of importance.
- Use contextualized information and examples as much as possible. The employees do not perceive the delivered material as contextualized as the CISOs do. Managers need to be more perceptive to context and adapt the

training material to the employees or even to different categories of employees or even individuals.

- Remember that microlearning is not a silver bullet and a mix of delivery methods is preferable. Despite being perceived as positive from the perspective of both employees and CISOs, deep learning is questioned, and long-term effects are unknown. To use recurring instructor-led workshops could be one piece of the puzzle.
- Repeat critical topics regularly. One way is to plan structured activities throughout the year with a mixture of delivery methods to avoid fatigue. That also helps prevent the traditional reactive approach where anti-phishing reminders are sent just after a targeted phishing attack is a fact (fait accompli).
- At the same time, try not to hoist the security flag too often. Cybersecurity fatigue is a challenge to respect.
- Use the ISP. It is a challenge to get the ISP to be a document that in a natural way governs the day-to-day behavior in an organization. Using a simpler language could make the ISP more useful. Another aspect is to relate constituents of the ISP to microlearning modules.
- Use intrinsic motivation by emphasizing softer values. It is easy to end up with the carrot-and-stick in cybersecurity, but viewing the SME as a family is one successful example of facilitating ISP compliance.

Cybersecurity in manufacturing has attracted much attention from researchers, primarily on more technical aspects, such as vulnerabilities in protocols, architectures, and platforms. We encourage future studies to use other approaches to study cybersecurity awareness in the manufacturing sector, such as ethnographic studies, to acquire more in-depth insights. Also, there are many possibilities for future studies on microlearning and similar approaches. Many facets of microlearning need investigation, for example, to highlight best practices and contextualization so that both employees and CISOs share the same perception and to measure the effect of using microlearning.

## References

[1] Culot G, Fattori F, Podrecca M, Sartor M. Addressing Industry 4.0 Cybersecurity Challenges. IEEE Engineering Management Review. 2019;47(3):79-86.

[2] Llopis-Albert C, Rubio F, Valero F. Impact of digital transformation on the automotive industry. Technol Forecast Soc Change. 2021;162:120343-. Epub 2020/10/08. PubMed PMID: 33052150.

[3] Sturm LD, Williams CB, Camelio JA, White J, Parker R. Cyber-physical vulnerabilities in additive manufacturing systems: A case study attack on the .STL file with human subjects. Journal of Manufacturing Systems. 2017;44:154-64.

[4] Franke U, Wernberg J, editors. A survey of cyber security in the Swedish manufacturing industry. 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA); 2020 15-19 June 2020.

[5] Howarth F. The role of human error in successful security attacks. Security intelligence. 2014;2.

[6] Sohrabi Safa N, Von Solms R, Furnell S. Information security policy compliance model in organizations. Computers & Security. 2016;56:70-82.

[7] Bulgurcu B, Cavusoglu H, Benbasat I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. Mis Q. 2010;34(3):523-48.

[8] Bada M, Nurse JRC. Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). Information & Computer Security. 2019;27(3):393-410.

[9] Ani UD, He H, Tiwari A. Human factor security: evaluating the cybersecurity capacity of the industrial workforce. Journal of Systems and Information Technology. 2019;21(1):2-35.

[10] Chua HN, Wong SF, Low YC, Chang Y. Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations. Telematics and Informatics. 2018;35(6):1770-80.

[11] Malik VR, Gobinath K, Khadsare S, Lakra A, Akulwar SV, editors. Security Challenges in Industry 4.0 SCADA Systems – A Digital Forensic Prospective. 2021 International Conference on Artificial Intelligence and Computer Science Technology (ICAICST); 2021 29-30 June 2021.

[12] Alabdan R. Phishing attacks survey: types, vectors, and technical approaches. Future Internet. 2020;12(10):168.

[13] Manoharan S, Katuk N, Hassan S, Ahmad R. To click or not to click the link: the factors influencing internet banking users' intention in responding to phishing emails. Information & Computer Security. 2021;ahead-of-print(ahead-of-print).

[14] Lallie HS, Shepherd LA, Nurse JRC, Erola A, Epiphaniou G, Maple C, et al. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & Security. 2021;105:102248.

[15] Zhang Z, He W, Li W, Abdous MH. Cybersecurity awareness training programs: a cost–benefit analysis framework. Industrial Management & Data Systems. 2021;121(3):613-36.

[16] Venkata RY, Brown N, Ting D, Kavi K. Offensive and Defensive Perspectives in Additive Manufacturing Security. ICSEA 2020. 2020:85.

[17] Yampolskiy M, Schutzle L, Vaidya U, Yasinsac A, editors. Security Challenges of Additive Manufacturing with Metals and Alloys2015; Cham: Springer International Publishing.

[18] Bradshaw S, Bowyer A, Haufe P. The intellectual property implications of low-cost 3D printing. ScriptEd. 2010;7:5.

[19] Li H, Zhang J, Sarathy R. Understanding compliance with internet use policy from the perspective of rational choice theory. Decision Support Systems. 2010;48(4):635-45.

[20] Webb J, Ahmad A, Maynard SB, Shanks G. A situation awareness model for information security risk management. Computers & Security. 2014;44:1-15.

[21] Bauer S, Bernroider EWN. From Information Security Awareness to Reasoned Compliant Action: Analyzing Information Security Policy Compliance in a Large Banking Organization. SIGMIS Database. 2017;48(3):44–68.

[22] Murire OT, Flowerday S, Strydom K, Fourie CJS. Narrative review: Social media use by employees and the risk to institutional and personal information security compliance in South Africa. 2021. 2021;17(1). Epub 2021-01-20.

[23] Albrechtsen E, Hovden J. Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. Computers & Security. 2010;29(4):432-45.

[24] Parsons K, McCormac A, Butavicius M, Pattinson M, Jerram C. Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security. 2014;42:165-76.

[25] Ponsard C, Grandclaudon J, Bal S, editors. Survey and Lessons Learned on Raising SME Awareness about Cybersecurity2019.

[26] Rose DM. Employee adoption of information security measures in the manufacturing sector using extended TAM under a quantitative study [Ph.D.]. Ann Arbor: Capella University; 2015.

[27] Chen Y, Ramamurthy K, Wen K-W. Organizations' Information Security Policy Compliance: Stick or Carrot Approach? Journal of Management Information Systems. 2012;29(3):157-88.

[28] Liu C, Liang H, Wang N, Xue Y. Ensuring employees' information security policy compliance by carrot and stick: the moderating roles of organizational commitment and gender. Information Technology & People. 2021;ahead-of-print(ahead-of-print).

[29] Merhi MI, Ahluwalia P. Examining the impact of deterrence factors and norms on resistance to Information Systems Security. Computers in Human Behavior. 2019;92:37-46.

[30] Herath T, Rao HR. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems. 2009;47(2):154-65.

[31] Talib YYA. Intrinsic motivation and information systems security policy compliance in organizations: Virginia Commonwealth University; 2015.

[32] Padayachee K. Taxonomy of compliant information security behavior. Computers & Security. 2012;31(5):673-80.

[33] Jansson K, von Solms R. Phishing for phishing awareness. Behaviour & Information Technology. 2013;32(6):584-93.

[34] Amankwa E, Loock M, Kritzinger E, editors. A conceptual analysis of information security education, information security training and information security awareness definitions. The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014); 2014 8-10 Dec. 2014.

[35] Santos-Olmo A, Sánchez LE, Caballero I, Camacho S, Fernandez-Medina E. The importance of the security culture in SMEs as regards the correct management of the security of their assets. Future Internet. 2016;8(3):30.

[36] Abawajy J. User preference of cyber security awareness delivery methods. Behaviour & Information Technology. 2014;33(3):237-48.

[37] Al-Daeef MM, Basir N, Saudi MM. Security awareness training: A review. Lecture Notes in Engineering and Computer Science. 2017.

[38] Maddox T. Microlearning and the Brain. Microlearning is effective for hard skills but detrimental when it comes to people and emotional skills. 2018.

[39] Beste T. Knowledge Transfer in a Project-Based Organization Through Microlearning on Cost-Efficiency. The Journal of Applied Behavioral Science. 2021:00218863211033096.

[40] Ann-Christin Karlén G, Ejemyr E, Thunell E. Implementing Nano-Learning in the Law Firm. Legal Information Management. 2019;19(4):241-6. PubMed PMID: 2348796257.

[41] Alshaikh M, Maynard SB, Ahmad A, Chang S, editors. An Exploratory Study of Current Information Security Training and Awareness Practices in Organizations. Proceedings of the 51st Hawaii International Conference on System Sciences; 2018.

[42] Kävrestad J, Nohlberg M, editors. ContextBased MicroTraining: A Framework for Information Security Training2020; Cham: Springer International Publishing.

[43] Yin R. Case Study Research : Design and Methods. Third ed: Sage Publications; 2003.

[44] Kvale S. InterViews: An Introduction to Qualitative Research Interviewing. Thousand Oaks, CA.: SAGE Publications; 1996.

[45] Patton MQ. Qualitative Research & Evaluation Methods: Integrating Theory and Practice. Thousand Oaks, CA.: SAGE Publications Inc.; 2014.

[46] Mason J. Qualitative Researching. Second ed. London: SAGE Publications; 2002.

[47] Bryman A, Bell E. Business Research Methods. 3rd ed: Oxford University Press, USA; 2011.

[48] Oates BJ. Researching Information Systems and Computing. London: SAGE Publications Inc.; 2006.

[49] Baskerville R, Rowe F, Wolff F-C. Integration of Information Systems and Cybersecurity Countermeasures: An Exposure to Risk Perspective. SIGMIS Database. 2018;49(1):33-52.

[50] Kotulic AG, Clark JG. Why there aren't more information security research studies. Information and Management. 2004;41(5):597-607.

[51] European Commission. Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises. OJ L 124 of 2052003. 2003:0036-41.

[52] Strauss A, Corbin J. Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory. Thousand Oaks: Sage Publications, Inc.; 1998.

[53] Cheng L, Li Y, Li W, Holm E, Zhai Q. Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. Computers & Security. 2013;39:447-59.

[54] Reeves A, Delfabbro P, Calic D. Encouraging Employee Engagement With Cybersecurity: How to Tackle Cyber Fatigue. SAGE Open. 2021;11(1):21582440211000049.

[55] Menard P, Shropshire J. Training Wheels: A New Approach to Teaching Mobile Device Security. KSU Proceedings on Cybersecurity Education, Research and Practice2016.