Security Culture in Industrial Control Systems Organisations: A literature review

Stefanos Evripidou[1(✉)], Uchenna D Ani[2], Jeremy D McK. Watson[3], Stephen Hailes[4]

[1]Centre for Doctoral Training in Cybersecurity, University College London, London, UK

[2]School of Computing and Mathematics, Keele University, Keele, UK

[3]Department of Science Technology Engineering and Public Policy, University College London, London, UK

[4]Department of Computer Science, University College London, London, UK

[✉]stefanos.evripidou.16@ucl.ac.uk

Abstract. Industrial control systems (ICS) are a key element of a country's critical infrastructure, which includes industries like energy, water, and transport. In recent years, an increased convergence of operational and information technology has been taking place in these systems, increasing their cyber risks, and making security a necessity. People are often described as one of the biggest security risks in ICS, and historic attacks have demonstrated their role in facilitating or deterring them. One approach to enhance the security of organisations using ICS is the development of a security culture aiming to positively influence employees' security perceptions, knowledge, and ultimately, behaviours. Accordingly, this work aims to review the security culture literature in organisations which use ICS and the factors that affect it, to provide a summary of the field. We conclude that the factors which affect security culture in ICS organisations are in line with the factors discussed in the general literature, such as security policies and management support. Additional factors related to ICS, such as safety culture, are also highlighted. Gaps are identified, with the limited research coverage being the most prominent. As such, proposals for future research are offered, including the need to conduct research with employees whose roles are not security related.

Keywords: Industrial Control Systems • ICS • Cybersecurity • Security Culture • Critical Infrastructure • Human Factors • Operational Technologies • OT

1 Introduction

Industrial Control Systems (ICS) are systems that manage, monitor, and control industrial processes [1]. Among those, ICS are used to operate critical infrastructure (CI) in sectors like energy, water, and transport, and are essential for a country's security, economy, and safety [2]. A convergence between information technology (IT) and operational technology (OT) has been increasingly taking place in ICS, further widening their attack surface [3]. Given the potential catastrophic impact of a cyber-attack which could include injury and loss of life or property, there is an increasing need to secure these systems.

Typically, three core interacting elements can be found in an ICS environment: people, processes, and technology. As such, to effectively control the vulnerabilities and threats in ICS, all three elements must be incorporated into holistic security solutions [3]. Additionally, from a socio-technical perspective, successful system performance is achieved by the 'joint optimization' of both the social and technical elements of a system [4]. Technology-based security solutions [5], as well as security processes (e.g., security assessment [6], risk management [7]), have been extensively researched for ICS. In contrast, the 'human factor' in ICS security has been relatively under-researched.

Some studies have shown that people pose a significant security risk in ICS. Namely, respondents in the 2019 SANS OT/ICS Cybersecurity survey [8] ranked people as the greatest risk to a control system compromise (62,3%), followed by technology (21.8%) and processes (14%). According to Kaspersky [9], social engineering is the most widely used method to gain initial access to these systems. Miller et al. [10], having extensively reviewed past ICS attacks, similarly state that attackers have relied on social engineering techniques such as spear-phishing to obtain access to ICS, especially in the last decade.

Some of the attacks where the human factor played a significant role include Stuxnet, believed to have been delivered to the Natanz nuclear facilities by removable media [10]. Additionally, the 2015-16 attacks on Ukrainian power stations, which resulted in widespread power outages, were initiated via spear-phishing

Original publication: https://doi.org/10.1007/978-3-031-12172-2_11

[10]. More recently, intruders attempted to remotely change the levels of lye in the supply of a water treatment facility in Florida. Fortunately, an operator detected and reversed this action [11]. While technical safeguards were in place to prevent damage even if the change was undetected by an operator, this incident highlights the importance of users in enhancing ICS security.

One approach that aims to reduce the human factor risk and improve an organisation's security is the cultivation of an organisational security culture. Developing and strengthening a security culture aims to increase security awareness, as well as influence the security attitudes and behaviours of employees [12]. As such, academics [10], security agencies [13], and governmental bodies [14] have called for the development of an enhanced security culture in organisations using ICS.

Currently, few works have investigated security culture in such organisations, with most research conducted in the IT domain. However, organisations using ICS differ from IT organisations. For example, they have a wider diversity of user roles compared to 'end-users' in IT systems, including operators, technicians, and engineers [15]. Moreover, while research in security culture has been influenced by the safety culture literature [16], safety culture is not as prominent in IT organisations, and the two cultures have rarely been studied together. Organisations using ICS, however, have developed a strong safety culture over the years due to the nature of their physical operations. Accordingly, they foster an environment where both cultures co-exist. Employees' safety perceptions, or processes to ensure safety, might also enhance or obstruct the security culture in ICS.

Thus, this work aims to provide an overview of the literature, answering the following research questions:

1) What is the scope and level of maturity of the security culture research in ICS environments?
2) Which constituents of security culture have been examined in an ICS context?
3) Which factors affect the security culture of organisations using ICS and how do they align with the factors described in the general security culture literature?

Providing clear answers to the above research questions can help industrial organisations to identify and understand relevant factors and attributes that can help improve their organisational security culture. In turn, an enhanced security culture can improve the security and resilience levels of their business and operational environments.

The remainder of this work is presented as follows; Section 2 provides an overview of the literature on security culture, followed by the methodology in Section 3. Accordingly, the selected works are presented in Section 4 and a discussion of the findings, research gaps, and potential future research is provided in Section 5. Finally, Section 6 provides the conclusion.

2 Background on Security Culture

Security culture research has been heavily influenced by the organisational and safety culture literature. It aims to examine how organisational procedures can affect employees' security perceptions and behaviours and to propose better ways to manage security [17]. Defining security culture has been an ongoing process with a variety of definitions presented in the literature [18], leading some academics to describe it as an ill-defined problem [19]. However, despite the multitude of definitions, the majority assert that security culture is constituted by cognitive-related attributes such as the knowledge, attitudes, perceptions, values, beliefs, and behaviours of employees. Accordingly, this work defines the security culture of organisations using ICS as 'the collective perceptions, attitudes, beliefs, and knowledge of users, and subsequently how they are manifested in their security behaviours in an ICS context'.

The constituent elements of an organisation's security culture can be influenced by a variety of factors, internal or external to an organisation, and several reviews have collated these factors [16], [20]. In their systematic review, Uchendu et al. [21], have identified 19 factors, including rewards and sanctions. Da Veiga et al. [18], having integrated academic and industrial perspectives, proposed a model with 25 factors, including trust between employees and change management. Another internal factor is the provision of education, training, and awareness (ETA) programmes to employees [16]. Employees' security perceptions can also be affected by the actions of their co-workers or managers [22]. Oftentimes, security tasks may conflict with every-day tasks, which also negatively affects employees' attitudes towards security [23].

Original publication: https://doi.org/10.1007/978-3-031-12172-2_11

External factors include national culture, i.e., the different security values and beliefs of each nation [21]. Additionally, security legislation and regulation, such as the General Data Protection Regulation (GDPR) and the changes it has introduced, such as mandatory reporting along with substantial fines, can also affect an organisation's security culture [18].

Calls have been made for these factors to be standardised to enable practitioners and researchers to work with common models and to allow research findings to be generalisable [24]. However, given that each organisation is different in terms of size, function, and regulations among others, this seems infeasible, as the candidate factors are potentially limitless. Moreover, these factors affect each organisation differently. For example, research into small and medium sized enterprises (SMEs) has validated some of the factors in the extant literature [21]. However, tools or frameworks developed for larger organisations can be unusable by SMEs due to their complexity. Additionally, resources are much more limited in SMEs, making change initiatives harder to implement. Consequentially, different, custom-built approaches may be needed to influence their security culture [21].

The way these factors affect organisations differently motivates our research in ICS. As already stated, ICS organisations have many differences compared to IT organisations where most security culture research has taken place. These range from the lifecycle and heterogeneity of their system components [3] to the variety of operating roles [15]. As such, research is needed to identify the most impactful factors and how they affect ICS security culture, to efficiently enhance it.

3 Methodology

A narrative literature review was conducted, with Scopus and Web of Science being the main research indexes used. This is due to their reputation for maintaining high-impact and quality research and the relevancy of their results as they encompass works from popular scientific databases such as IEEE, ACM, Springer etc. This minimises the chances of missing out relevant works.

As a starting point, the following query was used: ('security culture' AND ('industrial control systems' OR 'critical infrastructure' OR ICS)), returning 17 distinct results. Accordingly, three modifications were made on the base query to increase the number of results. The following keywords were added to the second part of the query: water, energy, oil, gas, transport, and nuclear, representing different industrial sectors that operate ICS. Additionally, another search was conducted with 'security culture' broken down into two keywords (security AND culture). Finally, to broaden the scope and capture studies related to the attributes making up security culture, such as knowledge or attitudes, the first part of the base query was reformulated to ('human factors' AND security). In total, 407 results were identified. Accordingly, titles and abstracts were scanned, and works were excluded based on the following criteria:

a) Works before 2010 were excluded, as the issues around security culture in ICS organisations were not common and were not considered by research prior to this time. For example, security could signify security of supply, without incorporating cybersecurity.
b) If the study had vaguely used the term critical infrastructure without making any distinction between ICS or other OT systems and IT systems, or critical infrastructure referred to sectors like finance who do not typically use ICS.
c) If security culture or any of the constituents of security culture (i.e., perceptions, attitudes, knowledge etc.) were not the focus, or examined in detail as part of the study.

As such, 9 works were selected. Supplementary searches were also conducted through Google Scholar, as well as by looking into other publications by the identified authors. Finally, selected works were also backwards and forwards reference searched [25]. This step produced another 3 works. Overall, works which were judged to sufficiently touch upon security culture, or at least one aspect of it such as employees' security perceptions, were selected. In total, 12 works were included to be reviewed. Figure 1 details the literature selection process.

Original publication: https://doi.org/10.1007/978-3-031-12172-2_11

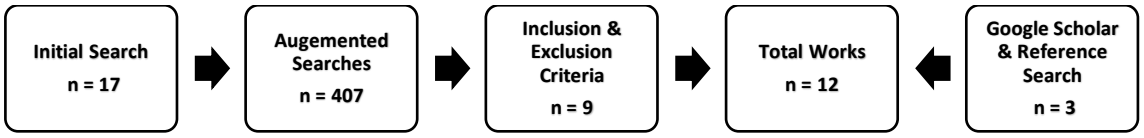

Fig 1. Literature Selection Process

The factors that affect security culture as identified by the reviews in section 2 were aggregated and synthesised to develop a collection of themes to analyse the selected works [16], [18], [20], [21]. Namely, different terms that referred to the same underlying factor, such as leadership involvement or top management support, were grouped under a common theme. The most prominent factors with respect to their frequency were selected. These factors were security training, security awareness, communication, management and leadership, and security policies and procedures. While no factors were outright excluded, some factors such as change management and national culture were not identified in the literature.

4 Results

Regarding the constituent elements of security culture, personnel security perceptions have been the focus of some works. Namely, Frey et al. [15], analysed six historical ICS incidents to understand the factors that affect ICS security, concluding that operators' perception errors, such as those about their system's boundaries, had played a significant role in them. However, it was emphasised that latent design conditions like the lack of fail-safe mechanisms had fundamentally affected these perceptions, challenging the idea that humans are the weakest link in a system's security.

Small scale surveys were also used to capture employees' security perceptions and beliefs. Green et al. [26], examined how employees in an ICS organisation prioritise each dimension of the confidentiality, integrity, availability (CIA) triad, to obtain insights into how security perspectives were formed in the organisation. Their results demonstrated discrepancies across both ICS levels and operational roles (operators and support/maintenance). For example, operators were prioritising availability and/or integrity before confidentiality which was not the case for support/maintenance staff, indicating the effect that ICS level and role can have in the formation and prioritisation of security perceptions. As such, to prevent fragmented approaches to security, the need for effective and coherent messaging from an organisation to its employees was highlighted.

Madnick et al. [27], presented a methodology to measure employees' perceptions on eight security constructs, including security culture. Participants came from two renewable energy companies, and similar perception discrepancies between different stakeholders were highlighted. OT personnel had the biggest gaps between their perceived assessment and the ideal level of importance across all constructs, with policy and procedures having the biggest difference compared to personnel from other functional areas, such as IT.

In an analysis of 25 interviews with ICS personnel having security-related roles, including control engineers, managers, and IT staff, Zanutto et al. concluded that security is a grey area, shaped by the multitude of demands of its stakeholders [28]. Oftentimes, organisations prescribed a top-down approach to security, which was not always compatible with everyday practices. Moreover, security was seen as a concern to be handled by a specific team rather than a problem to be tackled by every employee, with the authors highlighting that this perception was maintained by the lack of organisational commitment towards the management and communication of security. Besides, security practices did not always align with employees' practices and expected workload, creating tensions, as they necessitated a change in their habits. Generally, the many obstacles arising from organisational divisions, and the lack of guidance security personnel faced, have led the authors to describe them as "shadow warriors".

Reflecting the cyber-physical nature of ICS, employees' different roles and functional areas translated to different operational priorities. Discussing these, OT engineers in the water sector would refer to the safety, reliability, and availability (SRA) triad as being representative of their systems' priorities [29]. Contrastingly, interviewees working in IT were more concerned about the security and accuracy of their data. These differences in ICS security perceptions were highlighted in a variety of practices like patch

Original publication: https://doi.org/10.1007/978-3-031-12172-2_11

management, access privileges, and backups, indicating how differing priorities arising from each role also affect personnel's security perceptions.

Shapira et al. [30], reported on the findings of an active workshop which elicited cybersecurity perspectives from stakeholders in the Israeli water sector. The lack of both professional security knowledge and organisational awareness of cybersecurity risks were identified as the sector's two biggest gaps. Consequently, comprehensive security policies, together with education, awareness and training campaigns were recommended to solve the lack of awareness. Skotnes [31], also revealed similar practices while studying ICS owners and suppliers in the Norwegian electric power supply industry to understand the division of cybersecurity responsibilities between them. ICS owners appeared to have limited awareness of cybersecurity threats and relied heavily on their suppliers and their technical solutions for improving their systems' security, which resulted in a weakly focused organisational security culture.

A couple studies have proposed more holistic and validated approaches to measure aspects of security culture. Ani et al. [1], presented a methodology to assess the cybersecurity capabilities of workers in ICS, measured with respect to their knowledge and skills. Recognising that many studies had focused on the perceptions and behaviours of individuals, the authors state that knowledge and skills underpin and influence the two former attributes. Accordingly, their survey consisted of scenario-based questions tailored to ICS environments in areas like patch management and removable media protection, demonstrating the effectiveness of their approach in assessing individual employee cybersecurity capabilities.

Nævestad et al. [32], evaluated the information security culture of a Norwegian critical infrastructure organisation. The GAIN scale, originally developed to measure safety culture was used, supplemented with security knowledge and attitude questions. This allowed for comparisons to be made between organisational departments concerning topics such as reporting culture. Additionally, security culture was found to be the most significant predictor of security behaviour. A follow-up study was conducted with the same organisation two years later, comparing the security culture before and after the organisation's attempts to enhance it [33]. The results suggest that security culture had improved, which was attributed to the measures taken by the organisation's management. Unfortunately, these measures were not discussed in depth, but stronger password practices and improved security consultations between each department's supervisor and their team were highlighted.

Safety culture and its relationship to security culture was also discussed in a few works. Piggin and Boyes [34], in their 2015 article, stated that security culture was not yet on the same level as safety culture. Moreover, security was still not viewed as business as usual in most ICS. On the other hand, safety was given top priority with recurrent lesson sharing and the disobedience of safety guidance was not tolerated, especially in high hazard environments. This organisational lack of commitment towards security could also influence employees' perceptions. While physical security and safety risks could easily be appreciated due to their tangible impacts, this was not the case for cybersecurity risks.

More recently, Dewey et al. [35] conducted four case studies with UK nuclear organisations on the status and challenges of security culture. In one of their case studies, the authors reported that staff were more aware of issues concerning safety than security. Moreover, the security team was viewed as an obstacle by employees, as they were seen to be limiting business development. From their viewpoint, the security team reported that they had to compete for employees' time and attention with issues related to safety. However, the organisations studied had taken a variety of measures to improve their security culture. These ranged from awareness campaigns and training, to appointing a security culture manager. Moreover, security assessment procedures were put in place, enabling the benchmarking of security culture and comparisons over time.

5 Discussion

The number of reviewed works indicate that research in security culture, and more generally human factor security in ICS, is limited. However, research in ICS security culture is emerging, as most of the reviewed articles were published from 2017 onwards. This can be partly attributed to the fact that cybersecurity concerns are relatively recent in ICS. Moreover, the wider cybersecurity literature had for years not given

Original publication: https://doi.org/10.1007/978-3-031-12172-2_11

strong attention to human-factor security, compared to technical security solutions. A similar trend can be observed for ICS, where technical research appears to be outnumbering people-centric security research.

Regarding their scope, some works were quite narrow such as [26] where employees' perceptions of the confidentiality, integrity, and availability (CIA) attributes were specifically explored, or were pilot studies [27]. One work had relied on the authors' knowledge as practitioners to discuss security culture in ICS, without providing any empirical evidence, thus raising concerns about its external validity [34]. Moreover, while the ability of the employee security evaluations methodology in identifying variations in the capabilities of industrial personnel was demonstrated [1], participants did not originate from a single organisation. Applying similar evaluation methodologies in partnership with a particular organisation could lead to more significant results, such as highlighting differences between organisational departments [36], or gaps in their security culture [37]. However, it should be noted that collaboration with industrial partners was limited. Only two works had an industry co-author, but none were industry-led. Similar trends have been described in prior research, where no industry-led works were identified in a systematic review of the state of cybersecurity research in the water sector [38]. Security is a multi-disciplinary field, which increasingly requires collaboration between academia and industry. Additionally, partnership with industrial organisations can lead to richer insights and improve the validity of research findings.

As for application areas, studies have been conducted in various critical infrastructure sectors, including water, energy, transport and nuclear. Among those, the cases studies conducted in nuclear organisations indicate that despite the challenges, these organisations appear to be making good efforts to establish and maintain a strong security culture. Overall, the nuclear sector appears to be more mature with respect to security culture compared to other critical infrastructure sectors. This is unsurprising, given that the International Atomic Energy Agency (IAEA) released a security culture implementation guide more than a decade ago [39], and a self-assessment security culture guide in 2017 [40], whereas other industrial sectors lack similar guidelines.

Overall, a few works have presented methodologies to evaluate specific constituents of security culture, including security perceptions, knowledge and skills, and attitudes. Different perceptions were highlighted between functional areas such as IT and OT, as well as between OT roles, which could translate into different security practices and introduce security blind spots and vulnerabilities. Indeed, OT operators' perception errors regarding the observability and controllability of their systems were shown to be detrimental in past ICS attacks. Nevertheless, there is still room for research when it comes to incorporating these constituent attributes into more holistic evaluation approaches and systems viewpoints, as well as research with additional organisations using ICS to increase the validity of existing findings.

Regarding the factors that impact the security culture of organisations using ICS, the lack of awareness and subsequently of security initiatives from the top management was often highlighted. Skotnes [33], asserted that due to their limited security awareness and involvement, ICS owners were placing too much trust on their suppliers, who could only provide security assurances for their products but not entire systems. Green et al. [26], also emphasised the importance of coherent messaging from an organisation's management, to address potential risks arising from varied security perceptions between roles or departments. However, the top management's involvement may not always prove beneficial. For example, excessively strict policies and procedures set from the top of the organisation can prove unpopular with staff as they often exert constraints on operational practices. This can put security personnel at an uneasy position, as they must act as enforcers by trying to negotiate the uptake of security with operational staff [28]. Some studies recommended proper framing of security in terms of risk management and business losses to persuade the buy-in for security initiatives from senior management [28], [35].

Insufficient employee training, and the lack of security awareness and knowledge also emerged as key factors influencing security culture. It was observed that important security information such as the threat landscape or previous ICS attacks were not disseminated across organisations and were not reaching OT personnel, leading to flawed security perceptions. This was part of a general trend where organisation-wide security training and awareness initiatives were found to be insufficient [28]. Another study also highlighted that OT personnel had the biggest gaps on policy as well as security awareness, reaffirming the inadequacy of organisational security guidance [27].

Original publication: https://doi.org/10.1007/978-3-031-12172-2_11

Latent design conditions can also affect operators' security perceptions and lead to security incidents [15]. For example, weaknesses in an intrusion detection system may lead an operator to form inaccurate assumptions about the observability of their system and induce a false sense of security. Broadly, technical and other factors related to a system's design have not been studied in the context of ICS security culture as much as people-centric factors such as security training or policy. This generally extends to the wider security culture literature, where technology aspects and their influence on security culture have had limited attention [41]. However, the unique operational nature of ICS, where patching is harder to implement, or passwords frequently need to be shared [29], often contrasts general security practices. As such, security staff should recognize and resolve such issues, as insisting on unworkable security practices can negatively influence the attitudes of OT personnel towards security.

Security culture research has been heavily influenced by safety culture, and safety culture approaches to study security culture were utilised [22], [32]. As such, it was expected that more works would have investigated security along with, or in relation to safety perceptions in ICS environments. However, only three works had explicitly acknowledged the existence of a safety culture in ICS and only one had provided evidence on the state of the two cultures, with the authors of [35] positing that security culture was still not on the level of safety culture in their study organisations. Nevertheless, the factors that affect security and safety culture are quite similar. As such, there is potential value into research that aims to establish how the challenges and achievements of establishing a safety culture can be incorporated to enhance security culture.

Nonetheless, constructive security practices that strengthened security culture also emerged in the literature. The importance of factors such as communication, which should be two-way and active between all levels was stressed [35]. Training programs, which should be varied and interactive to stimulate participants were also highlighted as a good practice, along with establishing procedures for the continuous assessment of security culture. One study clearly asserted that the improvements in security culture in the study organisation could be attributed to the initiatives taken by the top management, such as improved training and additional middle management support [35].

Generally, the works reviewed highlighted that operational personnel's practices and everyday tasks would often clash with security requirements. This can be partially attributed to their differing operational priorities such as the safety, availability, and functionality of their systems [28]. One example was the dissatisfaction OT engineers expressed with requests for stricter access permissions and log-in auditing as these security measures would add to their routine workload. The human-factors security literature has proposed that employees have a compliance threshold, which once exceeded, results in non-compliance towards security [23]. Alternatively, employees may result in 'shadow security' practices to resolve these tensions [42]. Improving the security attitudes and perceptions of operational personnel is then paramount to ensure that employees behave securely.

While the reviewed studies had considered various ICS stakeholders, OT employees were generally underrepresented. For example, two works had focused on personnel with security roles [28], [29] and one had focused on system owners and suppliers [31]. However, no study has examined the perspectives of employees whose main roles and responsibilities do not revolve around security, such as operators or maintenance staff. As such, a gap currently exists in the literature that needs to be addressed, to better understand how to improve security from the OT viewpoint. Further research with operational personnel is warranted, to investigate their attitudes and perceptions towards the security of their systems.

Overall, a range of high-level factors that affect the security culture of ICS organisations across the span of critical infrastructure sectors were identified, as shown in Figure 2. These include the top management and their role in promoting security throughout the organisation, and middle management, which as the employees' reporting line should also be involved in security. Additionally, security policies and the need to minimise their conflict with every-day working practices was highlighted. The need for security communication between departments, the security team and employees, as well as efficient security messaging from the top to the whole organisation was also discussed. Security awareness and training were also found to be lacking on all levels of the organisation, from the senior management to OT operators, leading to inadequate knowledge. Finally, two factors more closely linked to ICS environments which have not been the focus of the wider security culture literature were identified; latent design conditions and their

Original publication: https://doi.org/10.1007/978-3-031-12172-2_11

effect on operators' perceptions, and safety culture and how its prevalence in ICS organisations can affect security perceptions and attitudes.

However, the degree to which each of these factors can affect security culture is still not clearly understood. Factors which were identified in the wider literature, such as rewards and sanctions, have not been examined in ICS contexts. As such, further research is needed with organisations that use ICS to examine the state of their security culture along with their current practices. Additionally, it is crucial for organisations to identify the most important factors that influence security culture, to develop appropriate measures towards enhancing it, and ultimately improve their security. Our ongoing research is focused on these objectives, by collaborating with industrial practitioners in ICS organisations through surveys and one-to-one interviews.

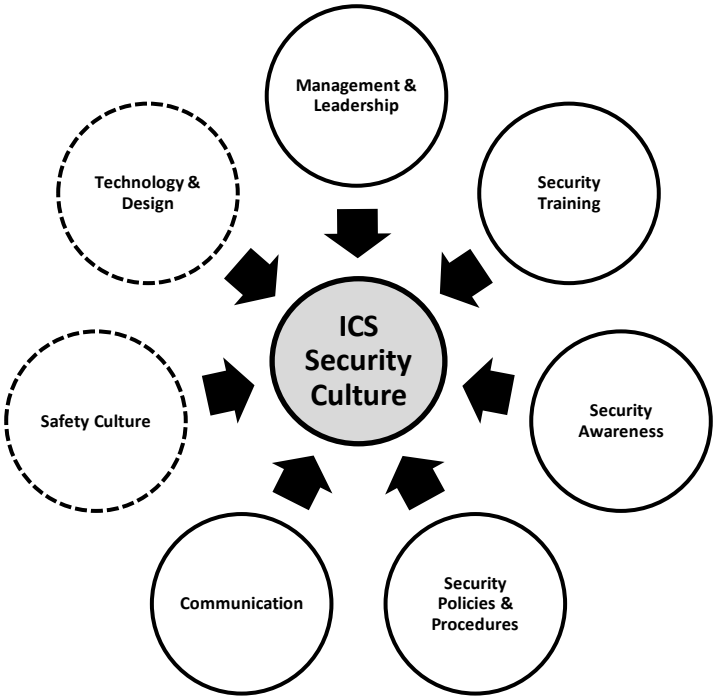

Fig. 2. Factors that affect security culture in organisations using ICS

6 Conclusion

This work has reviewed the literature on the security culture of organisations using ICS, with a focus on two areas: the constituent elements of security culture such as attitudes and beliefs, and the factors that affect it. Studies have examined the various attributes that make up security culture, indicating differences in perceptions and attitudes between roles and departments, which partially stem from employees' different operational priorities. It was also demonstrated that the factors that affect security culture in the broader security culture literature also apply to ICS organisations and their security culture. These include management and their leadership, training and awareness, and security communication among others. Two additional factors, closely related to ICS, have also been identified: safety culture and technology and system design.

Overall, the literature is limited but emerging. However, there is a clear lack of research with operational personnel whose roles are not security-related, with most works having focused on employees with security roles. Additional research with operational personnel would enable a better understanding of their views on security and how it affects their work. Finally, there is a lack of research looking into safety culture and its relationship with security culture. Potential future research could examine how safety culture was cultivated and maintained in organisations using ICS, and how these lessons can be used to enhance their security culture.

Original publication: https://doi.org/10.1007/978-3-031-12172-2_11

Nevertheless, ICS organisations should take steps to improve their security, with security culture being one such socio-technical approach. Treating personnel as the 'weakest-link' or confining them to unworkable policies has been demonstrated to be a bad approach. As such, future research should aim to propose better ways to positively influence personnel's security attitudes and perceptions along with making organisational security procedures workable to employees, thus fostering a strong and beneficial security culture in organisations using ICS.

References

[1] * U. D. Ani, H. He, and A. Tiwari, 'Human factor security: evaluating the cybersecurity capacity of the industrial workforce', *J of Systems and Info Tech*, vol. 21, no. 1, pp. 2–35, Mar. 2019, doi: 10.1108/JSIT-02-2018-0028.

[2] 'Critical Infrastructure Sectors | CISA'. https://www.cisa.gov/critical-infrastructure-sectors (accessed Nov. 27, 2021).

[3] U. P. D. Ani, H. (Mary) He, and A. Tiwari, 'Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective', *Journal of Cyber Security Technology*, vol. 1, no. 1, pp. 32–74, Jan. 2017, doi: 10.1080/23742917.2016.1252211.

[4] G. H. Walker, N. A. Stanton, P. M. Salmon, and D. P. Jenkins, 'A review of sociotechnical systems theory: a classic concept for new command and control paradigms', *Theoretical Issues in Ergonomics Science*, vol. 9, no. 6, pp. 479–499, Nov. 2008, doi: 10.1080/14639220701635470.

[5] J. Suaboot *et al.*, 'A Taxonomy of Supervised Learning for IDSs in SCADA Environments', *ACM Comput. Surv.*, vol. 53, no. 2, p. 40:1-40:37, Apr. 2020, doi: 10.1145/3379499.

[6] Q. S. Qassim, N. Jamil, M. Daud, A. Patel, and N. Ja'affar, 'A review of security assessment methodologies in industrial control systems', *ICS*, vol. 27, no. 1, pp. 47–61, Mar. 2019, doi: 10.1108/ICS-04-2018-0048.

[7] Y. Cherdantseva *et al.*, 'A review of cyber security risk assessment methods for SCADA systems', *Computers & Security*, vol. 56, pp. 1–27, Feb. 2016, doi: 10.1016/j.cose.2015.09.009.

[8] 'SANS 2019 State of OT/ICS Cybersecurity Survey | SANS Institute'. https://www.sans.org/white-papers/38995/ (accessed Jul. 23, 2021).

[9] 'APT attacks on industrial organizations in H1 2021 | Kaspersky ICS CERT', *Kaspersky ICS CERT | Kaspersky Industrial Control Systems Cyber Emergency Response Team*, Oct. 26, 2021. https://ics-cert.kaspersky.com/reports/2021/10/26/apt-attacks-on-industrial-organizations-in-h1-2021/ (accessed Nov. 27, 2021).

[10] T. Miller, A. Staves, S. Maesschalck, M. Sturdee, and B. Green, 'Looking back to look forward: Lessons learnt from cyber-attacks on Industrial Control Systems', *International Journal of Critical Infrastructure Protection*, vol. 35, p. 100464, Dec. 2021, doi: 10.1016/j.ijcip.2021.100464.

[11] 'Florida Hack Exposes Danger to Water Systems | The Pew Charitable Trusts'. https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2021/03/10/florida-hack-exposes-danger-to-water-systems (accessed Aug. 02, 2021).

[12] ENISA, 'Cyber Security Culture in organisations'. https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations (accessed May 31, 2021).

[13] NCSC, 'A positive security culture'. https://www.ncsc.gov.uk/collection/you-shape-security/a-positive-security-culture (accessed Nov. 27, 2021).

[14] DCMS, 'Water Sector Cyber Security Strategy', p. 12.

[15] * S. Frey, A. Rashid, A. Zanutto, J. Busby, and K. Follis, 'On the Role of Latent Design Conditions in Cyber-Physical Systems Security', in *2016 IEEE/ACM 2nd International Workshop on Software*

Original publication: https://doi.org/10.1007/978-3-031-12172-2_11

Engineering for Smart Cyber-Physical Systems (SEsCPS), May 2016, pp. 43–46. doi: 10.1109/SEsCPS.2016.015.

[16] K. Reegård, C. Blackett, and V. Katta, *The Concept of Cybersecurity Culture*. 2019. doi: 10.3850/978-981-11-2724-3_0761-cd.

[17] A. B. Ruighaver, S. B. Maynard, and S. Chang, 'Organisational security culture: Extending the end-user perspective', *Computers & Security*, vol. 26, no. 1, pp. 56–62, Feb. 2007, doi: 10.1016/j.cose.2006.10.008.

[18] A. da Veiga, L. V. Astakhova, A. Botha, and M. Herselman, 'Defining organisational information security culture—Perspectives from academia and industry', *Computers & Security*, vol. 92, p. 101713, May 2020, doi: 10.1016/j.cose.2020.101713.

[19] N. Gcaza and R. Solms, *Cybersecurity Culture: An Ill-Defined Problem*. 2017, p. 109. doi: 10.1007/978-3-319-58553-6_9.

[20] H. W. Glaspie and W. Karwowski, 'Human Factors in Information Security Culture: A Literature Review', in *Advances in Human Factors in Cybersecurity*, Cham, 2018, pp. 269–280. doi: 10.1007/978-3-319-60585-2_25.

[21] B. Uchendu, J. R. C. Nurse, M. Bada, and S. Furnell, 'Developing a cyber security culture: Current practices and future needs', *Computers & Security*, vol. 109, p. 102387, Oct. 2021, doi: 10.1016/j.cose.2021.102387.

[22] M. Chan, I. Woon, and A. Kankanhalli, 'Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior', *Journal of Information Privacy and Security*, vol. 1, no. 3, pp. 18–41, Jul. 2005, doi: 10.1080/15536548.2005.10855772.

[23] A. Beautement, A. Sasse, and M. Wonham, 'The compliance budget: managing security behaviour in organisations', Jan. 2008, doi: 10.1145/1595676.1595684.

[24] A. Nasir, R. A. Arshah, M. R. A. Hamid, and S. Fahmy, 'An analysis on the dimensions of information security culture concept: A review', *Journal of Information Security and Applications*, vol. 44, pp. 12–22, Feb. 2019, doi: 10.1016/j.jisa.2018.11.003.

[25] Y. Levy and T. J. Ellis, 'A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research', *InformingSciJ*, vol. 9, pp. 181–212, 2006, doi: 10.28945/479.

[26] * B. Green, D. Prince, U. Roedig, J. Busby, and D. Hutchison, 'Socio-Technical Security Analysis of Industrial Control Systems (ICS)', presented at the 2nd International Symposium for ICS & SCADA Cyber Security Research 2014, Sep. 2014. doi: 10.14236/ewic/ics-csr2014.2.

[27] * S. Madnick *et al.*, 'Measuring Stakeholders' Perceptions of Cybersecurity for Renewable Energy Systems', in *Data Analytics for Renewable Energy Integration*, Cham, 2017, pp. 67–77. doi: 10.1007/978-3-319-50947-1_7.

[28] * A. Zanutto, B. Shreeve, K. Follis, J. Busby, and A. Rashid, 'The Shadow Warriors: In the no man's land between industrial control systems and enterprise IT systems', p. 6.

[29] * O. Michalec, S. Milyaeva, and A. Rashid, 'Reconfiguring governance: How cyber security regulations are reconfiguring water governance', *Regulation & Governance*, vol. n/a, no. n/a, doi: 10.1111/rego.12423.

[30] * N. Shapira, O. Ayalon, A. Ostfeld, Y. Farber, and M. Housh, 'Cybersecurity in Water Sector: Stakeholders Perspective', *J. Water Resour. Plann. Manage.*, vol. 147, no. 8, p. (ASCE)WR.1943-5452.0001400, 05021008, Aug. 2021, doi: 10.1061/(ASCE)WR.1943-5452.0001400.

[31] * R. Skotnes, 'Division of Cyber Safety and Security Responsibilities Between Control System Owners and Suppliers', in *Critical Infrastructure Protection X*, Cham, 2016, pp. 131–146. doi: 10.1007/978-3-319-48737-3_8.

Original publication: https://doi.org/10.1007/978-3-031-12172-2_11

[32] * T. O. Nævestad, S. F. Meyer, and J. H. Honerud, 'Organizational information security culture in critical infrastructure: Developing and testing a scale and its relationships to other measures of information security', in *Safety and Reliability – Safe Societies in a Changing World*, CRC Press, 2018.

[33] * T. O. Nævestad, J. H. Honerud, and S. F. Meyer, 'How can we explain improvements in organizational information security culture in an organization providing critical infrastructure?', in *Safety and Reliability – Safe Societies in a Changing World*, CRC Press, 2018.

[34] * R. S. H. Piggin and H. A. Boyes, 'Safety and security — A story of interdependence', in *10th IET System Safety and Cyber-Security Conference 2015*, Oct. 2015, pp. 1–6. doi: 10.1049/cp.2015.0292.

[35] * K. Dewey, G. Foster, C. Hobbs, and D. D. Salisbury, 'Nuclear Security Culture in Practice', p. 46.

[36] A. Beautement, I. Becker, S. Parkin, K. Krol, and A. Sasse, 'Productive Security: A Scalable Methodology for Analysing Employee Security Behaviours', 2016, pp. 253–270. [Online]. Available: https://www.usenix.org/conference/soups2016/technical-sessions/presentation/beautement

[37] A. Da Veiga, 'Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study', *Information & Computer Security*, vol. 24, no. 2, pp. 139–151, Jan. 2016, doi: 10.1108/ICS-12-2015-0048.

[38] N. Tuptuk, P. Hazell, J. Watson, and S. Hailes, 'A Systematic Review of the State of Cyber-Security in Water Systems', *Water*, vol. 13, no. 1, Art. no. 1, Jan. 2021, doi: 10.3390/w13010081.

[39] IAEA, 'Nuclear Security Culture', 2008. https://www.iaea.org/publications/7977/nuclear-security-culture (accessed Nov. 27, 2021).

[40] IAEA, 'Self-assessment of Nuclear Security Culture in Facilities and Activities', 2017. https://www.iaea.org/publications/10983/self-assessment-of-nuclear-security-culture-in-facilities-and-activities (accessed Nov. 27, 2021).

[41] C. M. Ocloo, A. da Veiga, and J. Kroeze, 'A Conceptual Information Security Culture Framework for Higher Learning Institutions', in *Human Aspects of Information Security and Assurance*, Cham, 2021, pp. 63–80. doi: 10.1007/978-3-030-81111-2_6.

[42] I. Kirlappos, S. Parkin, and A. Sasse, 'Learning from "Shadow Security:" Why Understanding Non-Compliant Behaviors Provides the Basis for Effective Security', Feb. 2014. doi: 10.14722/usec.2014.23007.

Original publication: https://doi.org/10.1007/978-3-031-12172-2_11