Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P297-cd

Drawing on the Success of Developing a Safety Culture to Improve the Security Culture in Companies That Use Operational Technology

Stefanos Evripidou
Centre for Doctoral Training in Cybersecurity, UCL, UK. E-mail: stefanos.evripidou.16@ucl.ac.uk

Uchenna D Ani
School of Computing and Mathematics, Keele University, UK. E-mail: u.d.ani@keele.ac.uk

Stephen Hailes
Department of Computer Science, UCL, UK. E-mail: s.hailes@ucl.ac.uk

Jeremy D McK. Watson
Department of Science Technology Engineering and Public Policy, UCL, UK. E-mail: jeremy.watson@ucl.ac.uk

Companies using operational technology (OT), including critical infrastructure ones, are increasingly becoming more digitalized. This digitalization, however, has led to an extended attack surface, making cybersecurity a necessity. One approach to enhance a company's security is the development of a security culture, similar to what has already been done with safety culture in these companies. While the two cultures share many commonalities, there has been limited research into their relationship. As such, we have conducted a critical analysis of the safety and security culture literatures, as well as 35 interviews with OT security professionals on the topic of security culture development. Our findings demonstrate that both cultures share almost entirely overlapping enabling factors, such as top management leadership and involvement. Accordingly, the successful development of safety culture informs security practitioners' views on practices such as establishing security management systems and security communications. However, a few obstacles prevent security culture from reaching the level of safety culture, including differences in how safety and security risks are perceived. As security culture is still in its early maturity stages, future research could investigate ways to integrate both cultures in operational environments, as well as examine how safety and security risks are perceived by OT employees.

Keywords: Security, Safety, Cybersecurity, Security Culture, Safety Culture, Organizational Culture, Operational Technology, OT, Critical Infrastructure, Industrial Control Systems

1. Introduction

An organizational culture typically consists of the perceptions, attitudes, and behaviors of employees, along with organizational structures such as management systems (Guldenmund 2000). Interventions in a company's culture can affect its performance, as culture is the bridge between the management's interests and organizational behavior (Wiegmann et al. 2004). Culture can be broken down to sub-parts, such as a safety and a security culture, allowing managers to effectively direct their efforts and resources at a smaller subset of organizational practices (Wiegmann et al. 2004).

Companies using Operational Technology (OT) such as Industrial Control Systems (ICS) and Supervisory Control and Automation Systems (SCADA), are often responsible for operating a nation's critical infrastructure, like those in the water, energy, and transport sectors. Accordingly, they have concentrated on developing a safety culture over the past decades. As a term, safety culture was first cited as a main contributing factor to the Chernobyl nuclear disaster in 1986 (International Nuclear Safety Advisory Group 1991). The introduction of safety regulation and the creation of governmental agencies was another driver for the creation of safety culture in companies that operate OT (Hofmann, Burke, and Zohar 2017).

The concept of security culture started gaining prominence in the early 2000s (Schlienger and Teufel 2002; United Nations General Assembly 2003) with the uptake of information technology systems and increased internet connectivity. Companies using OT have been increasingly digitalizing over the past decade (i.e., IT/OT convergence, Industry 4.0), which has led to cybersecurity becoming a prominent concern given the extended attack surface (Evripidou et al. 2022). Accordingly, these companies are currently at the early stages of developing their security culture. Just like safety culture, high-profile incidents (e.g. Stuxnet) along with regulation (e.g., Network and Information Systems - NIS NCSC 2019) were instrumental in enabling the OT cybersecurity transformation.

Both cultures are influenced by the organizational culture literature, sharing many similarities. However, given the limited number of years OT security has been at the forefront in these companies, its maturity is still not at the levels of safety culture (Dewey et al. 2021). Given the interdependencies between safety and security, there have been calls for more research into their relationship, and the potential of integrating the two cultures (Reegård, Blackett, and Katta 2019; Ylönen et al. 2021). This work has explored the relationship between the two cultures in OT contexts, identifying practical insights from safety culture on how security culture can be developed. This was achieved by a scoping literature review of the two research fields, along with an analysis of interview data of 35 OT security practitioners, with the following research questions guiding this research:

1. What is the theoretical relationship between the safety and security cultures, e.g., influential theories, factors that enable culture?

2. How does the existing safety culture influence OT security practitioners?

2. Background

Research in OT security culture is an emerging area, with most works being published in the last decade (Evripidou et al. 2022). Various organizational factors that obstruct the development of a security culture have been demonstrated in the literature. Namely, a variety of external stakeholders must be involved in OT cybersecurity, including original equipment manufacturers (OEMs) and regulatory authorities, complicating communications and knowledge sharing (Wallis and Johnson 2020). The lack of internal professional knowledge and organizational awareness in OT companies also impedes the development of a security culture (Shapira et al. 2021). The NIS has been instrumental in targeting this lack of knowledge by fostering collaborations both inside OT companies, as well as intra-organizational ones (Michalec, Milyaeva, and Rashid 2021).

Research has also compared the two cultures, recognizing the prominence of safety culture over security in nuclear organizations (Piggin and Boyes 2015). This was also acknowledged by Dewey et al. (2021) in their case studies of four UK nuclear organizations, where safety was generally better understood by personnel than security. Nevertheless, it was recognized that the two cultures share many commonalities, which could be exploited by security teams.

3. Methodology

3.1. *Literature review*

A scoping literature review was undertaken for this work (Grant and Booth 2009). As the safety culture literature is of a considerable size, works from influential authors and pivotal moments in the field's history were included. Moreover, a substantial percentage of primary sources used in this work are existing reviews of the field. A similar selection approach was followed for the security culture literature, with a focus on examining the theories that influenced early research in this area. Additionally, various literature reviews have been published in the past five years, which have been incorporated into the analysis.

3.1. *Interviews*

35 semi-structured interviews on the topic of security culture development were conducted, with professionals with OT security related roles in the UK. The participant pool consists of

professionals working in OT companies, including Chief Information Security Officers (CISOs) and OT managers, as well as external stakeholders, such as consultants, security service providers, and regulators. As most OT sectors share similar challenges when it comes to security, participants came from water, energy, oil and gas, transport, and maritime companies. Interviews were conducted between July 2022 to March 2023 through Microsoft Teams. The NVivo 12 software was used to analyze the resulting transcripts. Finally, thematic analysis, a widely-used method to analyze, identify, and subsequently interpret themes in qualitative data, was used (Braun and Clarke 2006).

4. Results

4.1. *Safety and security culture review*

As occupational safety research's focus shifted from individual human factors to organizational aspects in the late 20th century, safety climate and culture research started becoming prominent (Hofmann, Burke, and Zohar 2017). Safety climate is a snapshot of employees' safety perceptions, whereas culture supersedes climate, and includes other factors such as management systems and behaviors (Guldenmund 2000). According to Le Coze (2019), the safety culture literature can be split into two waves, with one starting from the mid-1980s and the second one from the mid-2000s. The first wave brought many debates on the nature of safety culture under two approaches: the functionalist (i.e., culture can be managed) and interpretivist (i.e., culture as a social construct to be studied). Developing a culture of safety has followed the technology wave (e.g., engineering solutions, equipment) and the process wave (e.g., risk assessments, certifications) in these companies (Hudson 2007).

Since the mid-2000s, the safety culture research has been diverging into four different streams (Le Coze 2019). The first stream consists of more critical views, such as Hopkins' (2018), who has called for an abandonment of the safety culture term. The second stream of research is focused on safety culture as an object of solely scientific interest, whereas the third stream recognizes safety culture's importance to practice, but nevertheless calls for a better understanding to make it relevant to industry. Finally, functional approaches towards developing methods and tools, like maturity scales, make up the fourth stream (Goncalves Filho and Waterson 2018). Starting from Zohar's (1980) work, research has demonstrated the links between employee safety climate and culture and safety performance (Kalteh et al. 2019). A meta-analysis by Beus et al. (2010) demonstrated that injuries and safety climate were related, with injuries being more predictive of a company's safety climate than the other way around.

Some of the most influential culture theories in the safety literature come from Schein (1985), Reason (1998) and Cooper (2016). Schein's interpretive view consists of three increasingly more observable levels. These are the hidden, basic assumptions a company is built on, followed by the level of espoused personnel values, and the level of visible artifacts where objects like a company's safety policies exist. Reason's research on latent conditions, i.e., design decisions that lead to enduring organizational weaknesses, directs companies to investigate structural issues rather than being preoccupied with individual errors by fostering five subcultures: namely, informed, reporting, just, learning, and flexible cultures. Cooper's functional approach is based on a business process model with safety culture being the end-product of a transformation process, and includes three aspects: psychological (e.g., perceptions), behavioral, and situational (e.g., what an organization has, such as policies).

Throughout the field's history, a variety of factors have been proposed that enable a safety culture. Nevertheless, reviews agree on the most common ones (Choudhry, Fang, and Mohamed 2007; Lane 2002; Wiegmann et al. 2004; Bisbey et al. 2021; Guldenmund 2000). Firstly, top-management

leadership and involvement are considered crucial. Likewise, managers at each level need to be involved in the planning of safety as well as day-to-day safety operations. The components of a company's safety management system are also considered as important enablers of a culture. Policies and procedures are one such aspect, as they establish a correct way of working and are used to audit behaviors and processes. Workforce development, including education and certification, training, and more broadly safety awareness raising efforts, are another aspect of this. The communication of safety, from safety briefings to published material, is also an enabling factor.

One of the earliest mentions of security culture was in a hospital setting in 1998, where the need for top management leadership and commitment was stressed (Gaunt 1998). In the early 2000s security culture started becoming popular, being part of the third wave of information security, following the technology and management ones (von Solms 2000). Security policies were a frequently researched enabling factor in early literature. To be accepted by the staff and achieve the desired behaviors, policies should be aligned to the company's organizational culture, and be clear and appropriate for the task (Gaunt 2000). Accordingly, awareness programs are key vehicles to drive compliance, and subsequently a security culture (von Solms and von Solms 2004). Finally, communications at all levels, both vertically (e.g., management to employees) and horizontally (e.g., between co-workers) are another essential culture enabler (Reegård, Blackett, and Katta 2019).

Schein's model was employed by some early works (Schlienger and Teufel 2002; R. von Solms and von Solms 2004), with Schlienger and Teufel (2002) recognizing the similarities between safety and security cultures. The field has been growing since then, with studies looking at the relationship between culture's enabling factors, and security behaviors and their antecedents like knowledge. Namely, employees who had read the security policy were found to score higher in their assessment of their company's security culture and security knowledge (Da Veiga 2016). Moreover, the links between the top and direct management practices and compliant behavior have also been demonstrated (Chan, Woon, and Kankanhalli 2005). Overall, according to recent reviews of the field (Reegård, Blackett, and Katta 2019; Glaspie and Karwowski 2018; Uchendu et al. 2021), the most commonly studied enabling factors of security culture are the top management's leadership and involvement, policies and procedures, education and training, and communications.

4.2. *Interview analysis*

The prominence of safety culture in OT companies was reflected in participants' responses, with safety being described as the *"number one value"* and *"top priority"*. The development of safety culture has been ongoing for the past few decades, while most companies had started their cybersecurity journey around NIS's introduction in 2018, with participants describing security culture as *"still a baby"* and *"embryonic"*. The role of the board in driving this change was often highlighted. Boards are increasingly buying-in on cybersecurity, with cybersecurity becoming part of annual statements, risk appetite reports, and CEO calls. The recognition and involvement from the top have provided security practitioners with the leverage to influence other departments, and initiate security changes throughout their companies. This responsibility is driven down to managers, who in turn instill that culture to their teams. One participant compared these efforts to established safety practices:

"It's incumbent on me to call somebody out and not accept [examples of using the handrail (safety) and locking the screen when leaving the desk (security)]. *These are all things that have come to us from safety culture, and I think there are huge parallels that we can use to try and develop security culture." – P25, OT manager*

Safety culture inspires security practitioners' efforts to develop their company's security culture, with security often *"piggybacking"* on safety culture. For example, an OT security manager has been collaborating with the safety team to distribute OT cybersecurity communications, given the safety team's OT knowledge and ability of delivering that message in functions like engineering and operations. Generally, linking the effects of a cybersecurity attack on the safety and availability of OT systems helps grab the attention of OT personnel, and convince them of the value of cybersecurity. Overall, the belief that following a similar route to safety culture will strengthen the security culture was widely shared by participants, who used terms like *"embedding"*, *"ingrained"*, and *"structure"*, referring to how safety culture was made prominent in their companies.

"Once you've embedded [security] *into the business and you run it very similar to how you run your health and safety program that's where it becomes the norm. It sits alongside health and safety, and training happens on a regular basis, processes are reviewed, we're audited against those processes and people are held accountable for outcomes from nonconformance to those processes." – P31, Security consultant*

A few shared challenges that OT companies face on security culture reaching higher levels of maturity compared to safety culture were identified. Firstly, safety risks are more easily understood than security ones. Examples involving the use of ladders or mugs would often be used to show how unsafe actions and their effects are easily recognized. On the contrary, making the connection between an action in cyberspace, such as clicking a phishing link, and its effects on the company's security is not as easy. In turn, this makes the intervening and reporting of insecure behavior far less likely.

"I think the biggest difference will be that anybody would intervene in an unsafe environment… If you see somebody up the ladder, hanging on with one leg and balancing a bucket and things, most people would probably … stop and intervene or say something. If you walked past somebody who hadn't locked their screen on their laptop most people… wouldn't intervene." – P7, CISO

The second challenge is that security functions are often perceived as blockers. As such, security practitioners are actively trying to build better relationships with other functions to effectively embed security as business-as-usual. A frequent example provided was the introduction of security at the initial stages of new projects, rather than security becoming a last-minute consideration which results into overtime and overbudget projects and frustrated personnel.

"If you were building a pipeline, you would never need to say… 'You will need to make sure that nobody gets hurt while building it'. It's absolutely given … and it still needs to be designed in, but nobody would argue. It's just one of those things that you do, is how we work around here, and that's what we're trying to get to with security." – P8, CISO

Overall, participants reflected on whether security culture could reach the maturity levels of safety culture, with most responses being optimistic. In theory, with enough time and active effort security could reach the cultural levels of safety, as they share the same enabling factors. However, some participants recognized that security culture should not aspire to be as prominent given that safety is the number one priority of OT companies.

5. Discussion

Overall, security culture still lags behind safety culture in academic output, as well as industrial maturity in companies that use OT. Academically, both fields are inspired by the organizational culture literature, with Schein's model being prominent, especially in security (Reegård, Blackett, and Katta 2019). Both cultures are enabled by the same factors: top management's leadership, the management's involvement, the components of a company's management system such as policies, procedures, training, and communications. While bottom-up approaches to culture exist, most OT companies

are at lower maturity levels, where security culture must be driven from the top-down to effectively get company-wide traction for it. Additionally, most research in security culture is theoretical, followed by quantitative approaches based on these theoretical frameworks (Uchendu et al. 2021). As such, there is ample room for applied research, like Le Coze's (2019) third stream, to increase its relevance to industry. Safety culture's progress should inspire security culture researchers, with the consideration of alternative culture models aside from Schein's, and real-world research aiming to improve the understanding of security culture in practice, being two examples.

In practice, both cultures were initiated by high-profile incidents and the ushering of regulation. Our analysis demonstrates that security practitioners look up to the success of safety culture to appropriately model their approach to security. This includes various aspects, such as obtaining the top management's buy-in, and setting up proper governance structures. For OT environments more specifically, the impact of security on OT systems and their safety is often used to drive the security message. Nevertheless, while safety culture provides a useful roadmap, some challenges on the development of security culture exist. These are the differences in safety and security risk understanding which leads to a lack of intervention and reporting, and the belief that security is a blocker which hinders it from becoming business as usual. While the latter challenge will gradually improve as cybersecurity becomes more prominent in OT companies and as regulatory pressures increase, the understanding of security risks by employees is still an open question.

Finally, our data do not show a great deal of integration between the safety and security cultures in these companies. This is understandable given the infancy of cybersecurity, with security practitioners still integrating security into business structures before any potential efforts are made to integrate the two cultures. Accordingly, calls for integration may not yet apply to most OT companies except those where security is already an established value, along others such as safety and reliability. Integrating security and safety at a cultural level might also not provide value to the entirety of a company. Functions at the enterprise part of the business (e.g., HR, marketing) need to be more focused on security than safety and might not appreciate additional safety initiatives. As such, integrating these two cultures might be optimally done in OT environments, rather than the entirety of a company using OT. As security culture becomes more mature, future research can investigate whether the two cultures can be integrated and if so, the optimal organizational level for this integration to take place.

6. Conclusion

This work has investigated the relationship between security and safety cultures in companies that use OT, via a scoping review and an analysis of interview data from 35 OT security professionals. Academically, the two cultures share many commonalities, such as fundamental theories and enabling factors. These commonalities were also recognized by security practitioners, who often try to model their approach in similar ways to safety culture. This includes management approaches, such as governance structures and risk assessments, and the use of shared communication channels. Nevertheless, the biggest challenge towards developing a security culture compared to safety culture is the understanding of security risks by personnel. As such, future research could explore how safety and security risks are perceived in OT companies, to propose ways to effectively change employees' security risk perceptions.

Bibliography

Beus, Jeremy, Stephanie Payne, Mindy Bergman, and Jr Arthur Winfred. 2010. 'Safety Climate and Injuries: An Examination of Theoretical and Empirical Relationships'. *The Journal of Applied Psychology* 95 (July): 713–27. https://doi.org/10.1037/a0019164.

Bisbey, Tiffany M., Molly P. Kilcullen, Eric J. Thomas, Madelene J. Ottosen, KuoJen Tsao, and Eduardo Salas. 2021. 'Safety Culture: An Integration of Existing Models and a Framework for Understanding Its

Development'. *Human Factors* 63 (1): 88–110. https://doi.org/10.1177/0018720819868878.

Braun, Virginia, and Victoria Clarke. 2006. 'Using Thematic Analysis in Psychology'. *Qualitative Research in Psychology* 3 (2): 77–101. https://doi.org/10.1191/1478088706qp063oa.

Chan, Mark, Irene Woon, and Atreyi Kankanhalli. 2005. 'Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior'. *Journal of Information Privacy and Security* 1 (3): 18–41. https://doi.org/10.1080/15536548.2005.10855772.

Choudhry, Rafiq M., Dongping Fang, and Sherif Mohamed. 2007. 'The Nature of Safety Culture: A Survey of the State-of-the-Art'. *Safety Science* 45 (10): 993–1012. https://doi.org/10.1016/j.ssci.2006.09.003.

Cooper, Dom. 2016. 'Navigating the Safety Culture Construct: A Review of the Evidence'.

Da Veiga, Adéle. 2016. '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* 24 (2): 139–51. https://doi.org/10.1108/ICS-12-2015-0048.

Dewey, Karl, George Foster, Christopher Hobbs, and Dr Daniel Salisbury. 2021. 'Nuclear Security Culture in Practice', 46.

Evripidou, Stefanos, Uchenna D. Ani, Jeremy D McK. Watson, and Stephen Hailes. 2022. 'Security Culture in Industrial Control Systems Organisations: A Literature Review'. In *Human Aspects of Information Security and Assurance*, 133–46. IFIP Advances in Information and Communication Technology. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-12172-2_11.

Gaunt, Nicholas. 2000. 'Practical Approaches to Creating a Security Culture'. *International Journal of Medical Informatics* 60 (2): 151–57. https://doi.org/10.1016/S1386-5056(00)00115-5.

Gaunt, Nick. 1998. 'Installing an Appropriate Information Security Policy'. *International Journal of Medical Informatics* 49 (1): 131–34. https://doi.org/10.1016/S1386-5056(98)00022-7.

Glaspie, Henry W., and Waldemar Karwowski. 2018. 'Human Factors in Information Security Culture: A Literature Review'. In *Advances in Human Factors in Cybersecurity*, 269–80. Advances in Intelligent Systems and Computing. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-60585-2_25.

Goncalves Filho, Anastacio Pinto, and Patrick Waterson. 2018. 'Maturity Models and Safety Culture: A Critical Review'. *Safety Science* 105 (June): 192–211. https://doi.org/10.1016/j.ssci.2018.02.017.

Grant, Maria J., and Andrew Booth. 2009. 'A Typology of Reviews: An Analysis of 14 Review Types and Associated Methodologies'. *Health Information & Libraries Journal* 26 (2): 91–108. https://doi.org/10.1111/j.1471-1842.2009.00848.x.

Guldenmund, F. W. 2000. 'The Nature of Safety Culture: A Review of Theory and Research'. *Safety Science* 34 (1): 215–57. https://doi.org/10.1016/S0925-7535(00)00014-X.

Hofmann, David A., Michael J. Burke, and Dov Zohar. 2017. '100 Years of Occupational Safety Research: From Basic Protections and Work Analysis to a Multilevel View of Workplace Safety and Risk'. *Journal of Applied Psychology* 102: 375–88. https://doi.org/10.1037/apl0000114.

Hopkins, Andrew. 2018. 'The Use and Abuse of "Culture"'. In *Safety Cultures, Safety Models: Taking Stock and Moving Forward*, 35–45. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-95129-4_4.

Hudson, Patrick. 2007. 'Implementing a Safety Culture in a Major Multi-National'. *Safety Science*, Safety Culture and Behavioral Change at the Workplace: A selection of papers from the 23rd NeTWork Workshop, 2004, 45 (6): 697–722. https://doi.org/10.1016/j.ssci.2007.04.005.

International Nuclear Safety Advisory Group. 1991. 'Safety Culture'.

Kalteh, Haji Omid, Seyyed Bagher Mortazavi, Eesa Mohammadi, and Mahmood Salesi. 2019. 'The Relationship between Safety Culture and Safety Climate and Safety Performance: A Systematic Review'. *International Journal of Occupational Safety*

and Ergonomics, May. https://www.tandfonline.com/doi/full/10.1080/10803548.2018.1556976.

Lane, Broad. 2002. 'Safety Culture: A Review of the Literature', 40.

Le Coze, Jean Christophe. 2019. 'How Safety Culture Can Make Us Think'. *Safety Science* 118 (October): 221–29. https://doi.org/10.1016/j.ssci.2019.05.026.

Michalec, Ola, Sveta Milyaeva, and Awais Rashid. 2021. 'Reconfiguring Governance: How Cyber Security Regulations Are Reconfiguring Water Governance'. *Regulation & Governance* n/a (n/a). https://doi.org/10.1111/rego.12423.

NCSC. 2019. 'NIS Introduction'. 2019. https://www.ncsc.gov.uk/collection/caf/nis-introduction.

Piggin, R. S. H., and H. A. Boyes. 2015. 'Safety and Security — A Story of Interdependence'. In *10th IET System Safety and Cyber-Security Conference 2015*, 1–6. https://doi.org/10.1049/cp.2015.0292.

Reason, James. 1998. 'Achieving a Safe Culture: Theory and Practice'. *Work & Stress* 12 (3): 293–306. https://doi.org/10.1080/02678379808256868.

Reegård, Kine, Claire Blackett, and Vikash Katta. 2019. *The Concept of Cybersecurity Culture*. https://doi.org/10.3850/978-981-11-2724-3_0761-cd.

Schein, Edgar H. 1985. 'Organizational Culture and Leadership', 458.

Schlienger, Thomas, and Stephanie Teufel. 2002. *Information Security Culture: The Socio-Cultural Dimension in Information Security Management*.

Shapira, Naama, Ofira Ayalon, Avi Ostfeld, Yair Farber, and Mashor Housh. 2021. 'Cybersecurity in Water Sector: Stakeholders Perspective'. *Journal of Water Resources Planning and Management* 147 (8): (ASCE)WR.1943-5452.0001400, 05021008. https://doi.org/10.1061/(ASCE)WR.1943-5452.0001400.

Solms, Basie von. 2000. 'Information Security — The Third Wave?' *Computers & Security* 19 (7): 615–20. https://doi.org/10.1016/S0167-4048(00)07021-8.

Solms, Rossouw von, and Basie von Solms. 2004. 'From Policies to Culture'. *Computers & Security* 23 (4): 275–79. https://doi.org/10.1016/j.cose.2004.01.013.

Uchendu, Betsy, Jason R. C. Nurse, Maria Bada, and Steven Furnell. 2021. 'Developing a Cyber Security Culture: Current Practices and Future Needs'. *Computers & Security* 109 (October): 102387. https://doi.org/10.1016/j.cose.2021.102387.

United Nations General Assembly. 2003. 'Creation of a Global Culture of Cybersecurity'. 2003. https://digitallibrary.un.org/record/482184.

Wallis, Tania, and Chris Johnson. 2020. *Implementing the NIS Directive, Driving Cybersecurity Improvements for Essential Services*. https://doi.org/10.1109/CyberSA49311.2020.9139641.

Wiegmann, Douglas A., Hui Zhang, Terry L. von Thaden, Gunjan Sharma, and Alyssa Mitchell Gibbons. 2004. 'Safety Culture: An Integrative Review'. *The International Journal of Aviation Psychology* 14 (2): 117–34. https://doi.org/10.1207/s15327108ijap1402_1.

Ylönen, Marja, Minna Nissilä, Jouko Heikkilä, and Nadezhda Gotcheva. 2021. *Integrated Management of Safety and Security Synergies in Seveso Plants (SAFЄRA 4STER)*. VTT Technology. FI: VTT Technical Research Centre of Finland. https://doi.org/10.32040/2242-122X.2021.T386.

Zohar, Dov. 1980. 'Safety Climate in Industrial Organizations: Theoretical and Applied Implications'. *The Journal of Applied Psychology* 65 (March): 96–102. https://doi.org/10.1037/0021-9010.65.1.96.