Learning from Safety Culture to Optimise Cybersecurity Culture

Claire Blackett

Risk Pilot AB, Sweden. E-mail: claire.blackett@riskpilot.se

As the cybersecurity threat landscape continues to evolve, there is a growing awareness within the industry that protection against threats depends on more than complex technology infrastructure and tools. Human error is still considered to be the cause of most cybersecurity breaches, but humans may also be the key to building a successful cybersecurity defence. Over time, it has become evident that the most common approaches to address cybersecurity e.g., awareness training and simulated phishing attacks, will not be sufficient by themselves. Successful implementation of cybersecurity measures requires both a human-centred approach and the adoption of a cybersecurity culture mindset within the organisation. Safety-critical industries have undergone a similar challenge over the past almost 40 years, when the Chernobyl nuclear accident revealed that systemic organisational issues created the conditions for human error to occur. In the wake of this and other large-scale industrial accidents, safety-critical organisations identified the need for cultural change to fully embed safe behaviours and practices so that future accidents may be avoided. Safety culture has continued to evolve in the years since, and there are several lessons learned for organisations attempting to implement a cybersecurity culture today. This paper explores the many parallels between safety culture and cybersecurity culture and considers how organisations could learn from the implementation of safety culture to support adoption of a sustainable, human-centred cybersecurity culture.

Keywords: Cybersecurity, Cybersecurity culture, safety culture, human factors, nuclear.

1. Introduction

As the cybersecurity threat landscape continues to evolve, the industry maintains its focus on the development of technical solutions (hardware and software) to maintain security and avoid breaches (Baltuttis et al., 2024). People are still considered to be the weakest link (Ebert et al., 2023), with claims that anywhere between 74% (Nixu, 2023) to 95% (Widdowson, 2022) of cybersecurity breaches are caused by *human error*. Many organisations still believe that raising awareness alone is enough to manage human error and avoid future breaches (Dornheim and Zarnekow, 2023).

However, there has been a growing understanding that the successful implementation of cybersecurity measures that are sustainable over time requires a human-centred approach, that focuses on the human as part of the solution, rather than as a liability. Attention has turned towards the development of a cybersecurity culture within organisations to ensure that the desired behaviours are accepted, understood and achievable within an organisation (Sutton and Tompson, pg.4). The recognition of the need for a cultural change mirrors a radical shift that occurred in the safety-critical industries towards the concept of safety culture in the wake of the several large disasters such as the Chernobyl nuclear accident in 1986.

2. Evolution of the Safety Culture Concept

The concept of safety culture was first introduced in a report by the International Atomic Energy Agency (IAEA) after the Chernobyl accident, when technical, organisational and cultural factors were identified as root causes of the accident, and not just human error (IAEA, 1991). At that time, many safety-critical sectors were operating in what has since been called a *blame culture* (Reason, 1997), whereby incidents were blamed almost exclusively on human error, and remediation took the form of punishment such as demotion, dismissal, or even legal action.

Technical, organisational, or other systemic issues were rarely identified or addressed, meaning that underlying problems persisted, resulting in recurrence of the same types of accidents over and over again, even though the individuals initially blamed for the accident may have been reassigned elsewhere or even fired.

In 1990, James Reason introduced the concept of the *Swiss Cheese Model* (Fig.1) to

Proceedings of the 35th European Safety and Reliability and the 33th Society for Risk Analysis Europe Conference
Edited by Eirik Bjorheim Abrahamsen, Terje Aven, Frederic Bouder, Roger Flage & Marja Ylönen

ISBN: 981-973-0000-00-0 :: doi: 10.3850/981-973-0000-00-0 esrel2022-paper

explain how latent failures in systems can create the conditions for human error to occur.

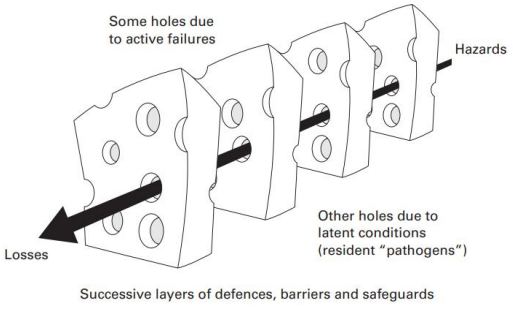

Fig. 1. The "Swiss Cheese" model of accident causation (Reason et al., 2001).

The model illustrates how systems are comprised of multiple layers, which can be physical, technical and/or administrative defences, barriers and safeguards. Most of the time, if a hazard penetrates a vulnerability in one barrier, it will be stopped by subsequent barriers, resulting in a *near miss* rather than an accident. But occasionally, vulnerabilities in the layers coincide meaning that a hazard can penetrate all of the layers, resulting in an accident. Since humans often represent the final defence in most systems, when an accident does occur it can seem obvious to blame it on the human at the sharp end. However, it is the vulnerabilities in the layers throughout the system that created the conditions for that human error to occur. Blaming the event on the human will not fix the weaknesses in the other layers, and so the conditions remain for similar accidents to happen again in the future.

Reason's work played a significant role in helping to advance safety-critical industries beyond blame culture, and towards system-based safety thinking. Subsequent work by Reason and others extended this thinking to develop the concept of a *just culture*, in which organisations seek to understand the systemic causes of accidents, and focus on organisational learning and improvement, rather than trying to find a person to blame for an accident.

2.1. *A Changing View of Cybersecurity*

While human error is still often cited as the leading cause of cybersecurity incidents, deeper investigation of most incidents often reveals systemic failures at multiple levels meaning, in many cases, that it was inevitable that such an incident would occur, regardless of the individual person at the sharp end.

For example, the Colonial Pipeline ransomware attack in 2021 initially attributed the cause of the failure to human error. This was a significant cybersecurity incident that affected critical infrastructure in the USA, disrupting fuel supplies across the entire east cost of the country. A ransomware group of hackers gained access to Colonial Pipeline's information technology (IT) systems through an exposed password for a VPN account of one of the employees (Kerner, 2022). The hackers had obtained the password for this account via a separate data breach. Initially the incident was blamed on human error – the employee had likely used the same password in a different location – but further investigation revealed a number of systemic and organisational weaknesses, including a lack of basic cybersecurity policies such as multifactor authentication (MFA), inadequate segmentation between critical system networks, inadequate implementation of best practices for cybersecurity such as regular updates and installing patches, insufficient incident response planning, and lack of employee training.

2.2. *Mirroring the Shift to Safety Culture*

The realisation that cybersecurity breaches are not caused solely by human error has led to a change of mindset amongst many cybersecurity professionals that mirrors the mindset change that started happening within safety-critical industries in the late 1980's. Furthermore, the cybersecurity industry has not only started to move beyond a blame culture but is now actively seeking to implement a *cybersecurity culture*, acknowledging the need to extend responsibility and ownership for cybersecurity throughout the organisation.

Despite this evolution of mindset, it appears that many organisations still struggle to understand what is required to implement a cultural change, that can be sustained over years. This is unsurprising, considering that, for many organisations, cybersecurity has historically been seen as the sole responsibility of the IT department. IT professionals have been responsible for buying and setting up computers and networks, as well as overseeing the security aspects of the organisations' IT infrastructure, such as setting up firewalls, installing anti-virus

software on computers, etc. (Baltuttis et al., 2024) and, more recently, ensuring adequate cybersecurity awareness within organisations.

Since cybersecurity is commonly seen as the responsibility of IT professionals, it is often addressed from a primarily technical perspective, i.e., involving the development of sophisticated and complex IT infrastructures and technologies used to detect and combat attacks. When it comes to addressing the human factor, this often takes the form of cybersecurity awareness training and occasional simulated phishing attacks and/or reminders to change passwords, but little else. Despite the advancements made over the years in technical solutions, and the addition of awareness training for employees, cybersecurity attacks continue to breach organisational defences. A human-centered approach is needed if a cybersecurity culture is to be truly embedded in an organisation, and safety culture can offer lessons learned on how to do this.

3. Understanding Cultural Change

Experience tells us that safety culture cannot be achieved through the implementation of a single policy or training program – there is no silver bullet that can transform an unsafe organisation into a safe one. Equally, there will be no one-size-fits-all solution to the implementation of a cybersecurity culture within an organisation.

3.1. *A Model of Organisational Culture*

To implement cultural change in an organisation, it is important to first understand how that culture is formed. Organisational culture is often conceptualised as having three levels or layers. These are: (i) tacit assumptions, which are beliefs about reality and human nature; (ii) espoused values, which refer to social principles, philosophies, goals, and standards; and (iii) artefacts, which are the visible, tangible, and audible results of activities grounded in the espoused values and assumptions. Artefacts can also be understood as the measurable behaviours that people exhibit.

In the cybersecurity cultural model (Reegård et al., 2019; Fig.2), a fourth layer is often added to the concept called "knowledge", which influences the assumptions, values, and behaviours (ibid). Knowledge is considered implicit in the three layers of the original organisational model, but it is explicitly mentioned in the cybersecurity culture model because "in an information security culture, the requisite knowledge cannot be assumed to be present" (Van Niekerk and Von Solms, 2010).

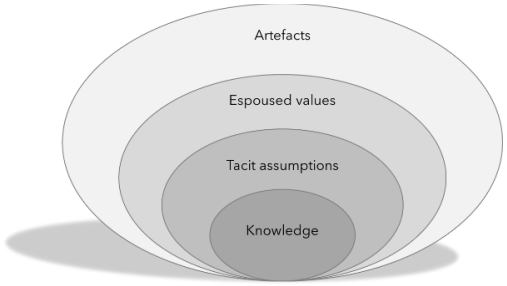

Fig. 2. The cybersecurity cultural model (adapted from Reegård et al, 2019).

When one examines how cybersecurity has typically been addressed within organisations, it appears that many efforts are targeted primarily at the knowledge and artefacts levels. This is evidenced by a heavy emphasis on cybersecurity awareness training (knowledge level), followed by measurement of employee behaviour e.g., via simulated phishing campaigns (artefacts level). It may be that the layers in between – espoused values and tacit assumptions – are not included in cybersecurity strategies because these are often much more difficult to address, since they must be inferred from what employees in the organisation say and do, and they are difficult to measure.

This is unsurprising considering the earlier point that IT professionals are often tasked with the responsibility of implementing cybersecurity defence measures, whereas addressing human factors like espoused values and tacit assumptions requires knowledge of domains such as behavioural psychology and cognitive psychology (Chaudhary et al., 2023) – subjects which are not typically included within the IT professional domain.

4. Effecting Cultural Change

Safety culture emphasises the need to address tacit assumptions and espoused values to ensure that cultural change can be effective. Tacit assumptions refer to deeply ingrained beliefs about risk, responsibility and safety that can shape how individuals and groups behave in an organisation (Reegård et al., 2019). These can be difficult to identify because they might not be

immediately obvious, even to the individuals and groups that hold those beliefs.

Examples of tacit assumptions in the cybersecurity industry are that humans are often viewed as the weakest link in the cybersecurity defence chain, and that human error is the root cause of most cybersecurity breaches. These assumptions remain, even in the face of overwhelming evidence to the contrary, probably because they are so deeply embedded in this very technical industry.

Espoused values are the official policies, principles, and priorities that organisations claim to embody. An example might be when an organisation makes the statement that cybersecurity is a top priority, and that the organisation is committed to securing their clients' data. However, technical solutions for cybersecurity are often not human-centered and create obstacles for employees in their work, meaning that employees may have to bypass or undermine cybersecurity measures to get their work done (Daniel, 2024).

4.1. *How to Implement a Cybersecurity Culture*

Corradini (2020) describes several steps that organisations can follow to implement a cybersecurity culture, which closely align with lessons learned from safety culture:

1. *Adopt a holistic approach to cybersecurity:* like safety culture, this step acknowledges that security isn't just about physical (e.g., a locked door) or technical (e.g., anti-virus software) measures, but rather requires a holistic approach that includes behaviours, processes, and a shared organisational mindset.
2. *Understand human nature and behaviour:* safety culture emphasises the need to understand and improve employee's behaviour and attitudes towards safety; in cybersecurity this translates to understanding why people take risks, how they think about cybersecurity and whether/how they understand the cybersecurity policies and procedures in place.
3. *Communicate clearly so that everyone can understand:* in cybersecurity, it cannot be assumed that all employees know technical language and concepts and so information must be communicated clearly to ensure everyone understands. Similarly, safety culture emphasises the need for clear, simple language to explain safety protocols to ensure everyone understands how these should be applied in their own work.
4. *Integrate cybersecurity into organisational culture:* to be effective, cybersecurity culture must be integrated with and considered as a core part of organisational culture to reinforce the message that it is everybody's responsibility. This aligns with the safety culture goal of making safety an integral part of the organisation, and visible in every aspect of the work.
5. *Build awareness through continuous education and training:* lessons learned from safety culture clearly show that it requires continuous effort to maintain the desired safety behaviours and attitudes. This is also true for cybersecurity, especially as new threats and technologies emerge, to ensure that employees remain informed and understand how to defend against threats.
6. *Encourage open and effective communication:* in safety culture, the focus is on identification of system failures, rather than blaming individuals for mistakes or accidents, and employees are encouraged to speak up when they see something unsafe, without fear of punishment, to encourage safety behaviour. Open communication is a core aspect of cybersecurity culture, to ensure employees feel comfortable to report e.g., a phishing attempt or if they have identified a security vulnerability.
7. *Solutions should be practical:* in both safety culture and cybersecurity culture, solutions need to be practical and applicable, to address issues directly without overcomplicating the process or interfering with people's ability to perform their job.

4.2. *Sustaining Cultural Change Over Time*

Cultural change takes time, and experience from safety culture shows that this requires a long-term, sustained effort (Hudson, 2001). The change cannot be achieved with a "one-and-done" approach, which is often seen within the cybersecurity industry, where one-time awareness training sessions are considered sufficient to imbed the necessary behavioural

changes to defend against cyber threats and attacks.

Although one-time training can create initial engagement and interest, failure to follow that up with leadership commitment and demonstration, integration of policies and processes into daily life, and further education and training will result in that initial engagement quickly fading. Furthermore, and especially for cybersecurity culture, the nature of the threat is continuously and rapidly evolving as attackers gain access to, and competence in, increasingly sophisticated and complex tools. Training is likely to quickly become outdated and so continuous effort is needed to stay current and relevant to the threat landscape.

4.3. *Measuring Cultural Change and Maturity*

An important method for sustaining cultural change over time involves the ability to measure an organisation's culture. A commonly used tool within the security and cybersecurity industries is the culture maturity model. Originally developed in the 1980s as a Capability Maturity Model (CMM) to assist organisations in measuring and enhancing software development processes, the CMM typically consists of 5 levels of maturity, as shown in Fig. 3.

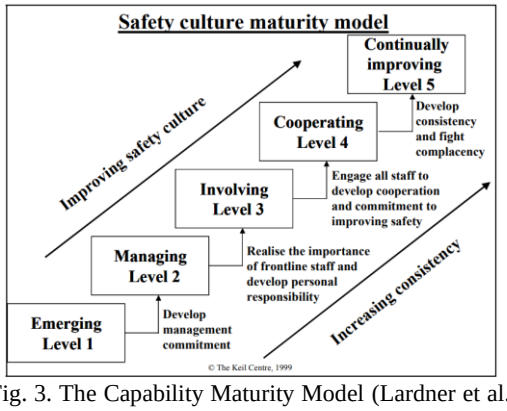

Fig. 3. The Capability Maturity Model (Lardner et al., 2001)

Recognising the potential value and effectiveness of this approach, the CMM was soon adapted to safety culture as a way for organisations to measure their current level of safety culture, and to identify strengths and areas where they need to improve. More recently, the concept was adapted to security culture, with the five levels now defined as (KnowBe4, 2022):

- *Level 1:* basic compliance,
- *Level 2:* security awareness foundation,
- *Level 3:* programmatic security awareness & behaviour,
- *Level 4:* security behaviour management, and
- *Level 5:* sustainable security culture.

The security culture maturity model (SCMM) has been recognised as a way for organisations to systematically assess their maturity level, identify areas that need attention, and develop targeted strategies to address these areas and progress to the next level of maturity.

However, there has been some criticism of the safety culture maturity model approach, which bears consideration for organisations interested in using this approach for the implementation of cybersecurity culture (Filho and Waterson, 2018; Tappura et al., 2022). Experience from the safety culture domain indicates that, while these models can provide a snapshot of the current maturity of an organisational culture, the models do not provide practical support for how to address any identified gaps to further mature the culture. The models tend to focus on quantifiable measures of cultural change (e.g., number of near misses reported), without necessarily taking into consideration qualitative aspects of culture, such as changes in employee beliefs and attitudes (tacit assumptions). Maturity models have also been criticised in the safety culture domain due to the lack of empirical verification of the models and their application.

4.4. *Managing Cultural Plateaus and Setbacks*

Maturity models tend to present a linear progression of cultural improvement, whereas in reality organisations often experience plateaus, or even occasional setbacks when it can seem that safety standards have deteriorated. A common example of this seen in the safety culture domain, and now in the cybersecurity domain, is the phenomenon of safety/security fatigue, sometimes referred to as *moral disengagement* in safety culture theory (Petitta et al., 2017). In this context, fatigue does not refer to tiredness, but rather to the feeling of being desensitised, disengaged or indifferent to safety/security messages and protocol.

This can happen because of the perceived repetitive nature of safety/security measures, or heavy focus on and/or irrelevance of the

measures. Such perceptions do not tend to occur in isolation, but often result from a lack of leadership engagement in and demonstration of safety/security values and measures, problems with communication of safety/security within organisations, failure to create a safe environment for people to speak up about safety/security concerns, and the implementation of safety/security measures that create obstacles or make it more difficult for people to perform their jobs and reach their targets or goals.

This may be especially common at the early stages of culture development when the organisation is first trying to implement cultural change and moving from a familiar culture to an unfamiliar one. When fatigue sets in, the organisation may begin to see that less attention is being paid to safety/security messaging and measures, people are starting to engage in more risky behaviour again, and there may be an overall decline in safety performance, e.g., numbers of incidents start to increase again.

A recent cybersecurity incident illustrates how cyber criminals may now be deliberately designing attacks to exploit phenomena such as security fatigue. In 2023 a phishing campaign was uncovered in which emails, pretending to be from the organisation's IT department, with embedded quick-response (QR) codes were used to try to trick employees at several different companies into sharing their Microsoft login credentials. Taking advantage of the popularity of QR codes, the email required the reader to scan the code which would then direct them to a (fake) website to enter their login details.

This was a clever attack, for several different reasons. The email itself did not include any suspicious code or links that could trigger spam email filters. Instead, it used an embedded image or document attachment with the QR code, to bypass spam filters. The email required the reader to use a secondary device to scan the QR code. There was a high likelihood that the reader might use their mobile phone, which may be outside of the protection of the organisation's anti-virus software or firewall that would typically be installed on their main work device. The email said that the person had to complete this step within two to three days, or by a specific date, or else they would lose access to their Microsoft account, thus adding a sense of urgency to the situation. The email appeared to exploit the fact that many employees probably no longer know the individuals working in their organisation's IT department. In the modern workplace, it is now quite common for the IT department to be based in a different location than other employees, or maybe is even outsourced to a different company (or country). Thus, it was less likely that the person would attempt to verify that the email really did come from their IT department.

And, finally, the email appeared to be designed to specifically exploit the reader's security fatigue as, unfortunately, emails about having to update login credentials are a necessary but irritating part of modern working life. If not possible to ignore or work around, then the employee will try to deal with the issue as quickly as possible (with minimal attention) so they can get back to doing their work.

All these factors increased the likelihood that the receivers of these emails would not question the legitimacy of the email and would simply follow the instructions contained within. The company that uncovered the attack, Cofense, did not provide information about whether any of the targeted companies were successfully breached as a result of this phishing campaign. However, since this attack was first detected in 2023, Cofense has reported an increase in similar types of QR code campaigns of 270% each month, and by more than 2400% overall since May 2023 (Cofense, 2023).

4.5. *Mitigating Plateaus and Setbacks*

There are several ways that organisations can mitigate cultural plateaus and setbacks. Safety culture theory notes that organisations can reinvigorate engagement and results by focusing on moving beyond compliance-based approaches. For example:

- Instead of focusing only on failures, encourage the reporting of near-misses and examine these to identify what went right to avoid this becoming an accident (Nemeth and Hollnagel, 2014).
- Strengthen the organisation's defences by actively fostering and promoting a just culture so that employees feel safe reporting issues (Reason, 1997).
- Visibly prioritise safety/security over productivity pressures to reinforce the importance of safety/security within the

organisation (Edmondson, 1999) and ensure alignment between policies, leadership behaviour and everyday frontline practices (Schein, 2010).
- Reinforce positive safety/security behaviours through recognition and rewards (Schein, 2010), and invest in training and engagement to reinforce the desired values and behaviours (Edmondson, 1999).

By focusing on leadership commitment, continuous learning and improvement, psychological safety for employees and prioritising safety/security values and practices, organisations can overcome stagnation, or even regression, and get back on the path to achieving positive cultural change.

5. The Potential for Goal Conflict

A final point for consideration concerns the potential for goal conflict for organisations tasked with implementing both a safety culture and a cybersecurity culture. This will be the case for most organisations operating within safety-critical industries today as these industries become increasingly digitalised. Organisations need to be aware of the potential for conflict between safety culture and cybersecurity culture when considering (Glesner et al., 2020):

- How to allocate resources effectively for implementation of initiatives to develop and promote both cultures at the same time.
- How to ensure that the development of one culture does not take priority over the other leading to imbalance in organisational focus.
- How to ensure that employees maintain vigilance across two separate domains, perhaps at the same time, which could result in cognitive overload, competing expectations and confusion.

Furthermore, the potential for conflicting objectives, approaches and messaging towards safety and security may create tensions within an organisation. For example, safety culture often promotes transparency and the sharing of information to promote a questioning attitude. However, to protect against cyber-attacks and breaches, cybersecurity culture often requires confidentiality, restrictions on access to information and control of information sharing to protect data (ibid.). The potential for contradiction between the objectives and values of safety culture and cybersecurity culture can be high. Organisations need to take care to identify potential conflicts, and develop strategies to resolve these, for example:

- Identification of shared or overlapping mitigations or layers of protection to strengthen the defence-in-depth of the organisation (Menon and Vidalis, 2021).
- Developing integrated training programs that cover both safety and cybersecurity topics and how they interact (Corradini, 2020).
- Performing risk assessments that evaluate both safety threats and cybersecurity threats, to identify potential vulnerabilities and conflicts (Agbo and Mehrpouyan, 2023).

6. Conclusions

The cybersecurity industry is undergoing an evolution of thinking in terms of how and why security events occur, and there is growing understanding of the role of human error in these events. Many of these developments mirror the evolution of safety culture in safety critical industries, and there is great potential for learning from the almost 40 years' experience of safety culture in the development and implementation of cybersecurity culture. An important lesson learned is that the implementation of a successful, sustainable cultural change requires long-term effort, and it is normal for organisations to experience plateaus or even temporary setbacks along the way. However, experience from the safety culture industry is clear that sustained commitment from leadership, focus on learning and improvement, ensuring psychological safety for employees and promotion of security values can help organisations to overcome any stagnation and continue to develop the desired cultural changes.

References

Agbo, C. and Mehrpouyan, H. (2022). Conflict Analysis and Resolution of Safety and Security Boundary Conditions for Industrial Control Systems. Proceedings of 6th International Conferences on System Reliability and Safety. Venice, Italy, November 23-25.

Baltuttis, D., Teubner, T. and Adam, M.T.P. (2024). A typology of cybersecurity behaviour among knowledge workers. *Computers & Security, Vol 140.*

Chaudhary, S., Gkioulos, V. and Katsika, S. (2023). A Quest for Research and Knowledge Gaps in Cybersecurity Awareness for Small and Medium-Sized Enterprises. *Computer Science Review, Vol. 50*.

Cofense (2023). Major Energy Company Targeted in Large QR Code Phishing Campaign. *Cofense*, 16 August, 2023. https://cofense.com/blog/major-energy-company-targeted-in-large-qr-code-campaign/

Corradini, I (2020). Building a Cybersecurity Culture in Organizations: How to Bridge the Gap Between People and Digital Technology. *Springer Nature*, Berlin/Heidelberg, Germany.

Daniel, L. (2024). 65% Of Employees Bypass Cybersecurity Measures, New Study Finds. *Forbes*, 5 December, 2024. https://www.forbes.com/sites/larsdaniel/2024/12/05/new-study-finds-65-of-employees-bypass-cybersecurity-measures/?utm_source=chatgpt.com

Dornheim, P. and Zarnekow, R. (2023). Determining cybersecurity culture maturity and deriving verifiable improvement measures. *Information & Computer Security, Vol. 32(2),* 179-196.

Ebert, N., Schaltegger, T., Ambuehl, B., Schöni, L., Zimmermann, V. and Knieps, M. (2023). Learning from Safety Science: A Way Forward for Studying Cybersecurity Incidents in Organizations. *Computers & Security, Vol 134*.

Edmondson, A. (1999). Psychological Safety and Learning Behavior in Work Teams. *Administrative Science Quarterly*, *Vol. 44*(2), 350-383

Filho, A.P.G. and Waterson, P. (2018). Maturity models and safety culture: A critical review. *Safety Science, Vol.105*, 192-211.

Glesner, C., Van Oudheusden, M., Turcanu, C. and Fallon, C. (2020). Bringing symmetry between and within safety and security cultures in highrisk organizations. *Safety Science, Vol 132*.

Hudson, P. (2001). Safety management and safety culture: The long, hard and winding road. Proceedings of the First National Conference. Melbourne, Australia.

IAEA (1991). Safety Culture. Safety Series No.75-INSAG-4. International Atomic Energy Agency, Vienna, Austria.

Kerner, M. (2022). Colonial Pipeline hack explained: Everything you need to know. *TechTarget*, 26 April 2022. https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

KnowBe4 (2022). Introducing the Security Culture Maturity Model. Retrieved Jan 12, 2024 at: https://www.bu.edu/tech/files/2022/08/Resource_Security-Culture-Maturity-Model-WP_EN-US.pdf

Lardner, R., Fleming, M. and Joyner, P. (2001). Towards a Mature Safety Culture. Symposium series n.148 of the Institution of Chemical Engineers (IChemE), pp. 635-642.

Menon, C. and Vidalis, S. (2021). Towards the Resolution of Safety and Security Conflicts. Proceedings of International Carnahan Conference on Security Technology (ICCST), Hatfield, UK, October 11-15.

Nemeth, C.P. and Hollnagel, E. (2014). Resilience Engineering in Practice: Becoming Resilient. Ashgate Studies in Resilience Engineering, vol. 2, Ashgate.

Nixu (2023). Reduce the Risk of a Cyberattack by Building a Health Security Culture, White Paper. https://www.dnv.com/cyber/insights/publications/reduce-the-risk-of-a-cyber-attack-by-building-a-healthy-security-culture/

Petitta, L., Probst, T.M. and Barbaranelli, C. (2017). Safety Culture, Moral Disengagement, and Accident Underreporting. *Journal of Business Ethics, Vol 141*, 489-504.

Reason, J. (1997). Managing the Risks of Organizational Accidents. Ashgate, London.

Reason, J., Carthey, J. and de Level, M.R. (2001). Diagnosing "vulnerable system syndrome": an essential prerequisite to effective risk management. *Quality in Health Care, Vol 10(Suppl II)*, ii21-ii25.

Reegård, K., Blackett, C. and Katta, V. (2019). The Concept of Cybersecurity Culture. In Proceedings of 29th European Safety and Reliability Conference, Hannover, Germany, September 22-26.

Schein, E. (2010). Organizational Culture and Leadership (4th ed.). San Francisco, CA: Jossey-Bass.

Sutton, A. and Tompson, L. (2024). Towards a cybersecurity culture-behaviour framework: A rapid evidence review. *Computers & Security, Vol. 148*.

Tappura, S., Jääskeläinen, A. and Pirhonen, J. (2022). Creation of Satisfactory Safety Culture by Developing its Key Dimensions. *Safety Science, Vol. 154*.

Van Niekerk, J.F. & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security, Vol. 29*, 476-486.

Widdowson, A. (2022). How to Enhance Resilience by Addressing Human Factors. *Thales Group*, 7 June, 2022. https://www.thalesgroup.com/en/united-kingdom/news/how-enhance-resilience-addressing-human-factors