Exploring the Security Culture of Operational Technology (OT) Organisations: The Role of External Consultancy in Overcoming Organisational Barriers

Stefanos Evripidou, *University College London;* Uchenna D Ani, *University of Keele;*
Stephen Hailes and Jeremy D McK. Watson, *University College London*

https://www.usenix.org/conference/soups2023/presentation/evripidou

This paper is included in the Proceedings of the Nineteenth Symposium on Usable Privacy and Security.

August 7–8, 2023 • Anaheim, CA, USA

978-1-939133-36-6

Open access to the Proceedings of the Nineteenth Symposium on Usable Privacy and Security is sponsored by USENIX.

Exploring the Security Culture of Operational Technology (OT) Organisations: The Role of External Consultancy in Overcoming Organisational Barriers

Stefanos Evripidou, *University College London* Uchenna D Ani, *University of Keele*
Stephen Hailes, *University College London* Jeremy D McK. Watson, *University College London*

Abstract

Operational Technology (OT) refers to systems that control and monitor industrial processes. Organisations that use OT can be found in many sectors, including water and energy, and often operate a nation's critical infrastructure. These organisations have been under a digitalisation process, which along with increasing regulatory pressures have necessitated changes in their cybersecurity practices. The lack of internal resources has often compelled these organisations to turn to external consultancy to enhance their security. Given the differences between OT and Information Technology (IT) security practices and that OT cybersecurity is still in its infancy, developing a security culture in OT environments remains a challenge, with little research investigating this topic.

We have conducted 33 interviews with professionals with a security related role working in various OT sectors in the UK, on the subject of security culture development. Our analysis indicates three key organisational barriers to the development of a security culture: governance structures, lack of communication between functions, and the lack of OT cybersecurity expertise. Subsequently, the role of consultants and security solution vendors in overcoming these barriers through consultancy is demonstrated. We therefore argue that these stakeholders play a crucial part in the development of security culture in OT and conclude with recommendations for these organisations.

1. Introduction

Organisations that use Operational Technology (OT) have embarked on a digital transformation over the past years, a process known as Industry 4.0 [1], IT/OT convergence [2], or the Industrial Internet of Things (IIoT) [3]. This digitalisation provides many benefits, including reduced costs, and more efficient and accurate data collection [1]. However, it has also increased OT systems' security risks, as OT and IT are becoming more interconnected [2]. As these organisations are often responsible for operating a nation's critical infrastructure, like those in the energy, transport, and water sectors, their cybersecurity is of paramount concern [4].

Operational Technology (OT) refers to systems that control and monitor industrial processes and equipment [5]. Various other terms are used to describe operational technology, including Supervisory Control and Data Acquisition (SCADA) systems and Industrial Control Systems (ICS) [2], with OT being the one most commonly used. Given OT's cyber-physical nature, a cyber-attack can have financial as well as physical impact, leading to injury, loss of life, and environmental damage [6]. Previous such attacks include Stuxnet, which targeted Iran's nuclear capabilities, and the Ukrainian energy system attacks in 2015-16, which resulted in wide-spread power outages [7]. More recently, when ransomware hit their enterprise estate, Colonial Pipeline had to proactively halt their operations over fears that it would spread to their OT estates, which led to fuel shortages [8].

Aside from the increased rates of cyber-attacks on OT, regulation was another factor that has practically forced these OT organisations to enhance their cybersecurity practices. Namely, the EU's Network and Information Systems (NIS) directive, which was passed into United Kingdom (UK) law in 2018, designated organisations operating critical infrastructure as operators of essential services (OES) [9]. Similar measures have been taken in sectors where the NIS does not apply, such as the OG-86 directive for major hazard industries like oil and gas [10], and the International Maritime Organisation's guidelines on maritime cyber risk management [11].

Against this backdrop, attempts to improve the cybersecurity of organisations using OT have necessitated changes in their technology, processes, and people. Nevertheless, OT cybersecurity has followed a similar trajectory to information security [12] with research in OT cybersecurity technologies (e.g., [13]), and accordingly processes (e.g., [14]), reaching a level of maturity that people-related security research in OT has not reached yet [15]. People in OT organisations are often targeted as an initial access vector via techniques like spear-phishing, as is the case in most recorded OT attacks in since 2013 [7]. As such, developing a security culture in OT has been promoted by various in-

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2022. August 7 -- 9, 2022, Boston, MA, Canada.

dustrial [16] and governmental bodies [17], since a strong organisational security culture ensures that security is an intrinsic part of employees' duties, and that security is perceived positively and pursued in all levels of management [18].

Most research in security culture has been conducted in IT organisations. Nevertheless, organisations that use OT differ from the ones using IT on their structure, values, as well as technology used. Firstly, these organisations use OT in their various industrial sites, as well as IT in the enterprise part of their business [19]. OT has a lifespan of decades, thus necessitating tailored security practices compared to IT [6]. Likewise, the safety and uptime of their services is of paramount importance, with security only recently becoming a concern [6]. Moreover, various stakeholders have a vested interest in OT cybersecurity, ranging from the government to their supply chain [20]. Additionally, security consultancies and security product vendors are also heavily involved in OT cybersecurity [21].

We therefore follow the argument that different types of organisations need tailored approaches to develop their cybersecurity culture to conduct our research [22]. Organisations using OT are additionally an ideal case study at security culture development as they usually are at early stages of this process. We have conducted 33 interviews with professionals with a security related role in various sectors in the UK, including water, transport, and energy. More specifically, we aim to answer the following research questions in this work:

1. What are the biggest organisational barriers to developing a cybersecurity culture for OT environments?
2. How do security consultants and security solution vendors contribute to overcome these barriers?

Our results demonstrate:

- Three key organisational obstacles towards a security culture: (i) governance structures, (ii) lack of communication between functions, and (iii) lack of OT cybersecurity expertise.
- The role of security consultants and solution vendors in overcoming these obstacles through consultancy, and in turn, influencing the security culture development of these organisations.

Our findings present insights to the research in OT cybersecurity by providing practical recommendations on how common organisational obstacles can be overcome. Additionally, our research contributes to the wider security culture literature by describing the complexities OT organisations face in their attempts at developing a security culture and, more importantly, the role of external stakeholders in shaping this culture.

2. Related work

2.1 Differences between IT and OT

Many significant differences between OT and IT exist, which necessitate tailored security approaches and ultimately affect an organisation's security culture. For example, OT's lifespan, which is typically decades long, complicates its security. Updates for a system might not be available, because the manufacturer might have stopped supporting the product, or in some cases, has ceased operating. Generally, patching and updating practices cannot be directly translated from IT to OT environments, as they must be in continuous operation [6]. This requires patches to be applied in tightly planned maintenance windows which take place a few times a year. Even measures such as longer passwords are not acceptable in time-critical scenarios, where availability and safety concerns are of greatest priority [23].

Aside from the technical differences, organisations using OT differ structurally from IT ones. They have a hierarchical structure, where the enterprise part of the business is separated from the industrial one, both physically and digitally. This separation is demonstrated by the Purdue model, a typical architecture reference model for OT, which consists of three zones and six levels: an enterprise zone and an industrial zone, separated by a demilitarized zone (DMZ) (see Appendix A for a diagram) [24]. Accordingly, different functions with divergent priorities are responsible for the technology and budget of each zone. For example, established information security principles in IT like the confidentiality, integrity, and availability (CIA) triad need to be reshaped to fit OT priorities, by including values such as safety and resilience [25]. Finally, security expertise in OT is relatively scarce. While incidents like Stuxnet have alarmed some organisations on the importance of cybersecurity, it was not until the NIS regulations that most organisations were propelled to act on their OT cybersecurity.

2.2 Security culture background

Security culture is a subculture of the wider organisational culture (i.e., 'The way things are done here' in an organisation). Many culture theories have been proposed, with Schein's model being the most common in security culture research [26]. Accordingly, culture is broken-down into three increasingly observable layers: tacit assumptions, i.e., the values taken for granted in a company, the level of espoused values, and the artefacts and creations level [27]. In the case of security, the assumptions level includes core operational values, which are often taken for granted, such as an organisation's risk-taking appetite. The espoused values level encompasses employees' security attitudes and perceptions. Finally, the observable artefacts level includes objects like training material and policies and procedures around security [26].

Research has predominantly focused on information security culture with research in cybersecurity culture recently becoming more prominent [22], as cybersecurity encompasses the protection of other assets aside from information, including the people that operate in cyberspace [28]. Nevertheless, as OT security has a strong cyber-physical element, we suggest that security culture is a more suitable and encompassing term for this area of research.

As culture is a construct, a variety of definitions on its constituent elements exist [29] , with the overwhelming majority focusing on attributes such as perceptions, values, attitudes, and behaviours around security [30]. ENISA's definition is a typical example, with culture defined as: 'The knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity and how they manifest in people's behaviour with information technologies.' [18]. Accordingly, several factors that affect security culture have been proposed in the literature [22]. These include management support, i.e., the involvement and leadership displayed by a company's management, and security policies and their attributes such as accessibility and clarity. More recently, the effect of national culture and regulation have also started receiving attention as culture influencing factors [22].

Nevertheless, the literature on security culture has a few gaps. Firstly, the most prominent culture influencing factors are associated with internal processes of an organisation, with little consideration given to exogenous factors. Aside from the role of the senior management and the security function, the role of different stakeholders in shaping an organisational security culture is often unexplored, especially those outside an organisation such as regulators, governments, or consultancies. Finally, the research area is dominated by theoretical frameworks, followed by quantitative approaches, with qualitative research lagging behind [22]. Our research attempts to fill some of these gaps, by demonstrating the role of other external stakeholders in shaping these companies' security culture, as is the case with consultancies and solution vendors in the OT space. Additionally, qualitative research can provide more in-depth insights in the security professionals' espoused security values, compared to quantitative approaches.

2.3 Security and safety cultures in OT

Safety culture is another part of the wider organisational culture in OT organisations. It became prominent following the nuclear accidents at Three Mile Island and Chernobyl, with the report on Chernobyl's aftermath often cited as the first use of the term [31]. What initially started with a focus on nuclear facilities, has in recent decades spread over into other industrial sectors that use OT including energy, oil and gas, and water. Compared to security, safety is now an established culture in these companies, and its effects are visible in all organisational levels, from small proactive acts like holding the handrail, to safety being a core organisational value, appearing in annual reports and in boards' communications to employees [25]. Nevertheless, there are many commonalities between the two cultures, with factors such as top management support and training considered as important in their development [32].

Research in organisational factors and security culture is an emerging area, with a few researchers looking into the topic in the past decade. Security workers in OT environments were described as 'shadow workers' due to the many obstructions they faced when attempting to fulfil their responsibilities. One such obstacle was that security was perceived as a concern to be exclusively handled by security personnel. Additionally, organisational divisions obstructed the visibility of their function and hindered security communications, further complicating their tasks [33]. Nævestad et al. have assessed the security culture of a critical infrastructure company in Norway. Their second study [34], two years after the first [35], demonstrated that the organisation's security culture had improved, with the authors attributing it to measures such as improved security communications between supervisors and employees.

Dewey et al., in their case studies of four UK nuclear organisations, highlighted various restructuring efforts aiming to integrate security into existing business structures. Additionally they demonstrated various challenges faced by security employees in their efforts to improve their organisation's security culture [31]. For example, mediums such as email were not as effective in distributing security communications, due to the non-office nature of many employees (e.g., rail operators, engineers, maritime). Finally, given the prevalence of safety culture, employees were more appreciative of the need for safety compared to security.

The impact of NIS in several UK sectors, including water [36] and energy [37] has also been investigated. Given its infancy, considerable inter-organisational collaboration was undertaken to transpose NIS into sectoral contexts, through various self-organising networks [20]. For example, the NIS necessitated closer collaboration between competent authorities and governmental entities, to translate the NCSC's Cyber Assessment Framework (CAF) to the needs of each sector. Other instances of inter-organisational collaboration include working groups between OT companies and critical suppliers where common security requirements were examined. Finally, Michalec et al. [36], in their case study of the water industry, have proposed that these collaborations were also influential in shaping the wider water sector's governance strategies.

These collaborations helped improve the sectoral understanding of the NIS, contributing to the knowledge and understanding of OT cybersecurity issues, and in turn, strengthened both the sectoral and national security cultures in the UK. However, there is still little work on how OT cybersecurity knowledge and understanding are developed in an organisational context. As evidenced by these intra-organisational collaborations, cybersecurity in OT companies depends on various stakeholders, including the government, competent authorities, original equipment suppliers, and system integrators. Additionally, our research aims to highlight the role other external stakeholders have in shaping this culture, namely, security consultants and security solution vendors.

2.4 Consultancy background

Organisations lacking expertise in a topic [38] or facing a lack of professionals in the employment marketplace often turn to consultancy to fill these gaps [39]. Knowledge sharing, the delegation of functional activities, and the design of processes and procedures are among some of the potential outcomes of the consultancy process [40]. Consultancies vary in sizes and offerings, including mega consultancies offering a variety of services (e.g., tax, accounting, IT etc.), independent consultancies specialising in fewer areas, and vendor consultants whose services relate to the support of their software and hardware offerings [40]. Generally, consultants have been described as 'therapists', 'doctors', and 'gurus' in the literature, and are often seen as 'obligatory passage points' supplying expertise to organisations [41]. OT cybersecurity is currently one such area where consultancy is recognised as the first step towards cybersecurity maturity [21].

Consultancy in IT, often focused on the implementation of Information Sharing (IS) [42] and Enterprise Resource Planning (ERP) systems [43], is one area close to cybersecurity which has received considerable academic attention. Broadly, the extant literature on consultancy can be summarised under the following topics: factors that contribute to consultancy's success [44], the client-consultant relationship [41], and the consultants' roles which can range from change agents to uncertainty managers and fashion setters [45], [46]. In the case of consultants as change agents, their role in knowledge sharing has often been recognised, with research demonstrating that it is more probable that an organisation's personnel will value knowledge from external sources compared to internal ones [47], especially when an organisations' own internal capabilities are lacking [39].

Cybersecurity research into consultancy compared to IT is scarce. While the cybersecurity and IT implementation consultancy processes have many commonalities, the literature in IT implementation often emphasizes the value of IT transformation in terms of cost reduction, increased effectiveness etc. [46]. The value of cybersecurity on the other hand is not as clear-cut, with companies regarding cybersecurity as an additional cost. Nevertheless, consultants have been described as cyber advocates i.e., individuals who can persuade organisations to adopt positive security practices [48]. Empirically, Gale et al. have found consultancy to be a driver influencing companies' cybersecurity decisions [49]. Finally, Poller et al. have investigated the effect of external consultancy on the organisational practices of a company's software development groups [50]. While the consultancy had some positive short-term effects, an overall lack of long-term sustainable change was reported.

3. Methodology

We have conducted a qualitative study through semi-structured interviews with professionals with a security-related role from a variety of OT sectors. The research has been approved by the authors' institutional ethics committee. The following sections provide more details on the sampling and recruitment process, interview conducting, and data analysis.

3.1 Sample and recruitment

We have employed theoretical sampling, with participants identified based on gaps in the collected data, or to explore emerging concepts [51]. Additionally, we employed snowball sampling by asking participants to refer us to other potential participants based on their role, which resulted in 11 of the 33 interviews [51]. Participant recruitment was undertaken via LinkedIn. We have decided to stop conducting interviews once our findings have reached theoretical saturation [51], i.e., interviews did not provide any new categories of inquiry or relevant data with respect to organisational barriers and consultancy's role in overcoming them.

While the water sector was our initial focus, the first few interviews led to the choice of including additional sectors, as our participants perceived that most OT sectors were facing similar cultural and security challenges. Our interest into external stakeholders also arose after the first few interviews, as the heavy presence of consultants and security solution vendors in the OT cybersecurity space was made apparent. Finally, our sample choice has presented a few obstacles. The population size is relatively small as organisations that use OT are bounded by regulation and geography, as is the case with UK water organisations which are effectively regional monopolies. Additionally, given the critical nature of operations of these organisations, some secrecy and hesitation were expected. Accordingly, research topics were tailored to be as non-intrusive, based around organizational structures, personnel's attitudes and perceptions etc., as to not be perceived as overtly sensitive by the study's participants.

3.2 Interview design and data collection

Interviews were conducted via Microsoft Teams between July 2022 and January 2023, lasting on average around an hour, and ranging from 45 to 70 minutes. Participants were not compensated for their contribution. Two participants opted to not be recorded, and therefore, data were collected through note taking. The participants' pool includes professionals working in OT companies with roles such as Chief Information Security Officers (CISOs), security managers, and OT managers, as well as external stakeholders including consultants and regulators. With respect to consultancies, we have included participants from large consultancies, smaller consultancies focused primarily on OT cybersecurity, and vendor ones. Overall, our study includes the views of 33 participants from 25 different organisations. A full breakdown of the participants' role and sector can be found in Appendix B.

Semi-structured interviews were used as their flexibility allows the point of view of the interviewee to come across more predominantly than other interview methods such as structured ones [51]. Often, questions did not follow the guide's outline and going on tangents was encouraged, as it provided an indication of what participants think is relevant. Interview guides were tailored based on the participant's role and a sample guide can be found in Appendix C.

3.3 Data Analysis

Microsoft Teams' built-in recording tool automatically produces a transcription. As such, we have used that tool to reduce the time needed to transcribe interviews, compared to a transcription done fully by ear. To code and analyse the transcriptions, the NVivo 12 software was used.

Thematic analysis was chosen to analyse the data, following the recommendations by Braun and Clarke [52], who provide a six-step process, and Ryan and Bernand [53], who provide techniques on how to identify themes. The first author coded all the data, following an open-axial-selective coding process [54]. This required an initial familiarisation with the data, which was aided by theoretical memoing. An open, primarily inductive process was used to develop an initial codebook. Accordingly, through an iterative process, codes were discussed with the other authors in weekly meetings, leading to further refinement, and eventually, to the themes presented in this work.

Using thematic analysis allowed us to identify themes both deductively, i.e., in-line with the literature, including factors such as policies and procedures, but primarily through induction, i.e., from an analysis of the data, such as the differences in mindsets and values between engineers and IT/security personnel. Examples of relevant codes can be found in Appendix D.

3.4 Limitations

We had to resort to online means for recruiting participants, as data collection was conducted during the Covid pandemic. In some cases, our attempts were perceived as social engineering, which was potentially amplified by campaigns such as 'Think before you link', by the National Protective Security Authority (NPSA) in the UK [55]. Paired with the overall small population size, a considerable amount of time and effort was spent to reach potential participants and obtain their trust.

Moreover, while our data have been collected from a variety of security professionals both internal and external to these organisations, and from various OT sectors in the UK, we do not claim a high level of external validity. Other nations, with different regulations on the cybersecurity of OT, or where organisations using OT have different operational models (e.g., utilities are publicly owned), might not necessarily face the same organisational obstacles, or the role of consultancy might be mediated by other stakeholders such as the government.

4. Results

4.1 The OT security landscape

The introduction of the NIS regulations and other similar directives prompted organisations using OT to actively take measures to improve their cybersecurity, leading to the realisation that becoming cyber-secure would be a challenging task. Many of these organisations have been reaping the benefits of digitalisation for years, without securing their technology, further complicating this task. As such, organisations often had a *"knee-jerk" (P29)* reaction, allocating OT cybersecurity responsibilities to their IT function, or their security function which would still be IT-focused. Given the lack of resources and inability to cultivate OT cybersecurity expertise internally, as well as the urgency of the matter due to the newly introduced cybersecurity directives, external consultancy was often the solution. Consultancies recognized this business opportunity - *"their eyes light up at the mention of OT security" (P09)* - and moved swiftly to fill this gap. Security solution vendors also found themselves in a similar position of business opportunity to provide consultancy services.

The rush to secure OT systems, combined with the lack of OT security expertise, allowed poor quality security practices to proliferate. Often a company supplying OT cybersecurity services would have never *"stepped foot" (P27)* below the DMZ, both physically, by visiting OT sites to understand their equipment and processes, as well as digitally. Substandard technical solutions, such as poorly designed network infrastructures, weak segregation between IT and OT networks, and penetration testing were often mentioned. Namely, penetration testing would often be a simple vulnerability assessment, without any contextual information on how that affects operations. Moreover, it would rarely go beyond the DMZ, limited to testing the segregation from the enterprise to the manufacturing zone. While penetration tests in OT carry substantial risks given the concerns about availability and the presence of legacy equipment, their limited scope provided OT customers with a false sense of assurance.

This lack of understanding extends beyond technology to a cultural level. OT personnel have been trained for years to value the availability and safety of their systems, where Service Level Agreements (SLAs) exist on the amount of allowed downtime. Additionally, safety is of paramount importance, with many systems being safety critical. On the other hand, IT and security professionals are eager to apply changes to secure OT systems, often by trying to directly translate from the IT to the OT world. Ultimately, the insufficient experience in OT environments has led to inferior quality risk assessments, where the cyber-physical nature of these systems was often lost, and an attack's impact on safety and the environment was not being considered:

"The experts that are brought in to do some of the risk assessments are maybe 27001 [standard] *qualified and they look at it* [rolling stock] *almost as an IT system. While there's a lot of overlap, 62443 incorporates the safety side as well and includes that with the CIA risk factors. And that's something that quite often we have to go back and say, well, you haven't considered safety on this one. What's the knock-on effect?" - P30, Consultant*

Note – ISO/IEC 27001 is an international information security management standard, whereas IEC 62243 is the equivalent series of standards for OT cybersecurity.

4.2 Organisational barriers

While the overall security maturity in OT organisations is improving, we have identified three recurring organisational obstacles that pose a challenge to the development of a security culture in OT: (i) governance structures, (ii) lack of communication between different functions, and (iii) lack of OT cybersecurity expertise.

4.2.1 Governance

Cybersecurity in OT is constrained by the operational models of these organisations. Typically, the operations and engineering functions are responsible for the industrial sites and their operational technology. IT and security sit on the enterprise side of the business, having historically being tasked with its information security. As these functions have grown organically over the years, and cybersecurity for OT has only recently become a concern, this governance model complicates security knowledge exchange and communication efforts.

These functions typically have different reporting lines, leading to a situation where managers do not speak directly with their counterparts but use a chain of commands where information must travel upwards and then downwards. This often allows other organisational politics to get involved, and information can get diluted. Additionally, the number of people involved in a cybersecurity decision, including personnel from both IT and OT responsible functions, also hinders the decision-making process.

Another obstacle is the ownership of operational assets. While the IT department is usually tasked with a company's cybersecurity, the budget and resources for OT are typically owned by the operations function, which has different priorities on how they should be spent. Participant 02 recalled the pushback they had received when a decision to install an intrusion detection solution their OT estate was made:

"That got a lot of pushback with the OT teams because it's quite expensive. When you look at some of the IT technologies, spending half a million pound on something is neither here nor there, that's general. But when you spend half a million pound in the OT is 'Why are we spending so much on that? That's ridiculous. That's technology. I could spend that and repair all these different systems and repair this and repair that'." – P02, OT Manager

Finally, the problem of ownership and governance is intensified in sectors which operate offshore and onshore assets, as they can be subject to different cybersecurity regulations or accountable to different regulatory authorities. Similarly, in sectors like oil and gas, joint ventures and the outsourcing of the operations are common practices, which often leads to certain stakeholders having a disproportionate amount of responsibility. The international operations of some organisations also complicate cybersecurity, as is the case with the maritime industry. While cybersecurity risk assessments were made mandatory by the IMO since 2021, there is no guarantee that this is upheld by the relevant national authorities - *"There's not many countries taking that seriously". - P28, Academia and industry coordinator*

4.2.2 Lack of communication

The lack of communication between functions with cybersecurity responsibilities was another commonly referred barrier obstructing the development of a security culture. The non-desk nature of many OT roles, along with practices like shared workstations and user accounts limit the effectiveness of communication mediums such as e-mails or intranets in delivering cybersecurity relevant information. This is further exacerbated by the existing governance structures, as well as the lack of OT experience. As P15 bluntly stated:

"If you talk to the IT department, they don't have any expertise in OT and they don't really talk to the engineering de-

partment because the engineering department doesn't want to talk to IT people." - P15, Security solutions vendor

The different value systems or *"mindsets"* of these two groups also contribute to this communication barrier. The *"engineering mindset"* prioritizes the stability and service of their systems. Additionally, both occupational and functional safety are paramount given the potential physical consequences of safety incident. Accordingly, engineers are *"conservative with a little c" (P29)* when it comes to changes in their equipment and practices. Often, a reticence by OT engineers exists in installing new equipment in OT systems given the potential disruption they can cause – *"Something is working. Don't touch it" (P29).* On the other hand, IT and security professionals with a *"technology mindset"* are typically more familiar with newer technologies and more relaxed on their implementation. As such, IT and security experts are often perceived as intruders in OT environments, with both teams viewing each other as hindrance.

The different mindsets and lack of communication can lead to futile attempts at securing OT, with the example of OT professionals not allowing changes in their environments being regularly mentioned. Moreover, substandard security practices have damaged the trust between these two functions and diminished the willingness for future collaboration. Participant 22 recalled their experience with unimplementable directives coming from the IT department in a previous engineering role they had:

"We got directives through about centralised antivirus update for your OT systems, password protection policies and things like that. And you went trying to implement, things like IT security experts [saying] *this is what your password complexity is. Read up on it, sent an email 'Sorry but Windows can't do that'.*

It's as silly as that, and these are IT security experts and they're asking you to do something that Windows can't even do. It's an example of things that filtered down. And it starts making you go; 'Am I going to read and do everything they send down to me now? Probably not'." - P22, Consultant

4.2.3 Lack of expertise

The third major barrier towards an OT security culture is the lack of OT cybersecurity expertise, with both governance and communications issues obstructing its development. In turn, the lack of expertise leads to communication obstacles and diminished trust between stakeholders with cybersecurity responsibilities. By defining expertise as a measure of knowledge and experience, it follows that expertise is not easily achievable unless there is sufficient hands-on experience in a specific context [56]. In the case of OT cybersecurity, this would entail both cybersecurity experience, but more importantly, experience in industrial environments using OT.

Nevertheless, there are a few challenges that prevent this expertise gap from closing, aside from the field's current immaturity. One such challenge is the different professional routes towards a job in engineering compared to cybersecurity. Engineers and other OT professionals *"have come up on the tools" (P27),* primarily through vocational education such an apprenticeship after finishing secondary education. OT personnel may hold an engineering-related degree or diploma, but a master's degree is rarely a prerequisite for such roles. On the other hand, security is becoming a profession where a degree is increasingly desired, compared to previous decades where information security had been creeping into the role descriptions of IT professionals. In our sample, at least five participants had obtained a security or technology-related degree later in their career, which facilitated their move to a cybersecurity role.

In the case of OT, cybersecurity was typically added to personnel's existing job descriptions, without these organisations firstly supplying resources to train their personnel on cybersecurity. OT personnel who for years have been primed to value the safety and uptime of their systems suddenly also had to value cybersecurity. Accordingly, the need for cybersecurity would not be appreciated, especially if there were no targeted efforts to communicate its value and link it to their priorities. Moreover, incorporating security in their everyday tasks adds to their workload, and as such, they will often pushback to such changes. Similarly, the IT and information security side was often additionally tasked with the cybersecurity responsibilities for OT. Realising their lack of expertise and the difficulty in setting up relationships and communication corridors with the operations and engineering functions, accepting these responsibilities is a difficult choice:

"CISO's five years ago did not have oversight on the onboard stuff, and now it's come into question there is a kind of defensive, you know, how do you admit you were wrong in the past? Also, if you're a CISO with limited budget and pressures on your existing infrastructure, to willingly lift the lid and say, 'All this new stuff, [is] *now in my scope and I'd have to argue for more budget', that just makes your life more difficult as well." – P26, Security solutions vendor*

Finally, another factor which complicates the closing of this expertise gap is the preference companies have on hiring professionals from their sector. Participant 15 recalled an interaction with an oil and gas company:

"And then when they were bemoaning, you know, the lack of skills and the lack of people who they could get involved in cyber security. 'We can do that, we've got some great guys working in shipping now who would be really good for your

offshore installations'. And the answer I got was: 'So not oil and gas men then'." – P15, Security solutions vendor

4.3 The role of external experts

This section discusses the role of security consultancies and solution vendors in overcoming these organisational barriers. Consultancies and vendors operate across a variety of sectors and their accumulated experience on the threats and security solutions for OT is sought after by OT organisations. Additionally, their expertise in both the engineering and cybersecurity domains makes them efficient mediators between organisational functions. As these stakeholders commonly work with OT organisations at the initial stages of their cybersecurity journey, we argue that they shape OT organisations' thinking and actions around cybersecurity, and therefore, play a part in shaping their security culture. Security consultancy can take many forms, varying from long-term contracts where consultants are embedded into the client organisation, to shorter-term contracts with a specific focus (e.g., auditing, regulation). The unique challenges faced by OT organisations such as the disperse nature of their assets and legacy equipment, and the fact that IT security practices cannot be directly translated to OT have created a market for OT-specific solutions. However, our study's participants working in the security solutions industry acknowledged that the need for OT security solutions is not always appreciated by the market.

"Why aren't we selling more? Because the market doesn't understand so we have to get the market to understand so that we can sell more." – P15, Security solutions vendor

The theme of *"educational sales"* was a common occurrence in our interviews, where potential customers need to be taken through a journey of understanding of their underlying needs before a sale can take place and solutions are implemented and supported. As security solutions are not a one-off purchase, security vendors often resort to consultancy to improve their potential customers' understanding of security.

4.3.1 Overcoming organisational barriers

Making sense of the governance and responsibility structure of their customers is typically the first task these stakeholders undergo, as OT security responsibilities are not always clear cut:

"The first thing you have to work out is who's doing what and who does the company think is running their OT security." - P15, Security solutions vendor

The value of a proposed solution then needs to be demonstrated to the relevant stakeholders. However, given the lack of communication and understanding between different functions, these external stakeholders are often asked to support the IT and/or operations teams to present a solid business case to their management. Moreover, given the internal lack of expertise, external experts have a detrimental role is in effectively delivering these solutions, be it technical or procedural. Additionally, these experts can influence changes in governance, by guiding new teams such as joint IT and operations functions. They also guide the allocation of cybersecurity responsibilities; both internally, by advising on the responsibilities for different roles, as well as intra-organisationally, in the case of joint ventures between multiple companies.

Consultants and vendors also act as translators between different teams. Having observed the confusion caused by different uses of common terminology, such as TTL which means time-to-live, transistor-to-transistor logic, or threat-to-life to different stakeholders, one participant had created a glossary to improve the understanding of the security-responsible functions. More broadly, these external experts often sit in the middle of different teams, acting as facilitators and helping build bridges between them. Participant 18 recalled their experience during a workshop where communication problems between functions were present:

"It was very clear from day one ... that there was this issue because it was all engineering and operations on the left of the room and IT was on the right and they were always just sort of looking over and then sort of switching their heads back... It was obvious that there was some clashes and some politics there. ... So that's when the consultants would come in and do a bit more facilitation and say, well, have you thought about this ... and you'd play the sort of the mediator between them. And more often than not, it actually becomes resolved."- P18, Consultant

Finally, consultants and security vendors contribute to the security culture of an organisation by equipping employees with an understanding and knowledge about OT cybersecurity. There is a multitude of ways for knowledge exchange to happen, as these experts are typically brought in an organisation with low cybersecurity maturity. Aside from bringing various teams together and increasing their cohesion, they advise on suitable technical security solutions. Moreover, they work on developing policies, as is the case of equipment procurement, pushing cybersecurity requirements into the supply chain. In other cases, they collaborate with communication teams to distribute security awareness material, or mentor OT professionals towards a cybersecurity certification or degree.

Given the continuously evolving nature of cybersecurity, both in terms of technology and threat landscape, cybersecurity services should be supported and reviewed on a continuous basis. As these collaborations are usually long-term, the concept of taking customers on a journey was often referenced by participants, necessitating the development of long-term relationships between these stakeholders and their customers. Several factors can affect their success, with security professionals with an engineering background feeling that they could more easily appreciate OT engineers' needs and earn their trust. This also extends to the organisational level, with consultancies with engineering expertise finding it easier to build relationships with OT staff, given their common backgrounds.

"I'm probably a bit better at it because I've come from that background, so I kind of understand their way they do risk assessments". – P22, Consultant

Nevertheless, participants often recognised that their attempts at building these relationships will be futile if relevant stakeholders have not been engaged by their organisation beforehand. Additionally, they can be met with distrust from other functions, or individuals, as they are perceived as part of the team that has contracted them. Participant 12 recalled their experience with a client organisation:

"There was big hostility for what we were trying to do to the point we were doing assessment questionnaires and they [the industrial site] *were being deliberately evasive.… For whatever reason, there was a huge distrust between the asset and headquarters." – P12, Consultant*

Finally, technical solutions themselves contribute to the security culture of these companies. Whether it is an asset discovery tool, a network gateway, or an intrusion detection system, technical solutions give OT organisations *"a window into their networks that they didn't have before" (P15),* by exposing new, security related information. For example, asset discovery is a substantial challenge for OT companies, as assets have been accumulating over time and are dispersed in vast geographical areas. As such, asset discovery tools are the first step towards understanding the presence of a variety of operational equipment in OT estates. Similarly, network monitoring solutions can produce alerts on the state of OT networks, allow only specific communications via whitelisting, or alert operators about anomalous behaviours. This information can then aid the security and operations teams to make more educated decisions on how to prioritise and distribute their budgets, ultimately enabling better quality security risk assessments.

5. Discussion

We have identified a few restructuring efforts in these OT organisations through our study, including a merger of operations and IT and the creation of an independent cybersecurity function, all aiming to improve the organisational management of cybersecurity. However, restructuring is not an easy task, especially when departments have grown organically over time. Targeting the lack of communications and expertise can improve an organisation's security culture without a disruptive and costly restructuring effort. Initiatives like workshops and steering groups are a common practice, enabling cross-pollination between various stakeholders. Nevertheless, care should be taken when deploying such initiatives, as it is crucial that the divergence in values and terminology between OT and IT personnel are addressed beforehand.

Given the infancy of the field, the lack of OT cybersecurity expertise is a harder challenge to overcome compared to communication issues. Nevertheless, organisations should aim to close this gap by being less reluctant to hiring OT experts from other sectors, as well as investing in training their OT personnel. Due to the increased digitalisation of OT, IT equipment is increasingly used in OT environments, making OT cybersecurity more accessible to outsiders. However, we suggest that expertise in OT is harder to obtain compared one in cybersecurity. This is primarily due to the different "mindsets" between engineers and IT personnel. Appreciating the engineering way of working and their concerns was often cited as a difficult challenge for IT-based professionals. While both approaches work; IT security professionals moving to OT, and OT professionals moving to security, the latter requires less effort. As such, aside from cross-sectoral hiring, organisations can invest in developing their OT personnel's cybersecurity expertise, by sponsoring OT professionals towards a cybersecurity certification or degree, as well as introducing security training at the early stages of engineer's career, in apprenticeships and other vocational schemes.

Previous research in OT organisations has proposed that they were under heightened pressure to acquire such expertise, with OT cybersecurity lacking a typical career trajectory [19]. Our findings suggest that this situation has been improving, with security roles and responsibilities becoming more standardised, and security becoming more prominent as an organisational function. Nevertheless, this expertise gap will continue posing a challenge and will be further amplified given increased government pressure and proposed changes in regulation. The NIS 2 which will replace current regulation, expands the scope of what constitutes an operator of essential services by including organisations from sectors like wastewater, and provides additional powers to competent authorities [57]. Consequently, an increased number of organisations will be looking to acquire expertise from a limited pool of available talent, further amplifying the need for organisations using OT to tackle this challenge by training their existing personnel.

The identified obstacles of governance, expertise, and communications commonly recur in organisational cybersecurity contexts [58], [59]. These obstacles are often intertwined [60], and have been shown to affect individuals' security behaviours [61], as well as an organisation's security culture [22]. For example, our analysis demonstrates that the lack of OT knowledge by IT professionals leads to diminished trust and ineffective communications between the IT function and their OT counterpart. At the same time, the lack of communication between these functions impedes the sharing of OT and cybersecurity knowledge. Overall, security practitioners can apply many of the culture literature's recommendations more or less directly, such as two-way communications between different stakeholders [62], and the development of non-technical skills (e.g., communication, leadership, etc.) by security professionals [62], [63], targeting the issues of communication, and subsequently, knowledge sharing.

However, the differences between the organisations using OT and IT should not be overlooked, especially when developing a culture of security in their industrial zones. While most research on communications focuses on the exchanges between the security function and end users [64] or senior stakeholders [65], our analysis shows that in OT organisations communication and knowledge exchange between the functions responsible for IT and OT are a prerequisite to ensure optimal cybersecurity practices. Research in knowledge and awareness also focuses on cybersecurity education of various personnel [66], and simultaneously the need for security professionals to understand personnels' priorities and work processes [64]. This dialectic process in turn allows for the effective tailoring of security procedures, to better suit personnel's workload and organisational goals, preventing shadow security practices [64].

Nevertheless, the technology underlying most human-centred cybersecurity research is IT, in which security professionals are experienced. The obstacle of security knowledge is amplified in OT contexts, as security practitioners need to understand the underlying operational technology, as well as its end-users' priorities (e.g., safety, availability). Usability research has demonstrated how OT users' security perceptions are affected by the design constraints of their equipment, and their familiarity with IT equipment [67]. Additionally, our research demonstrates how the different "mindsets" between OT and IT stakeholders act as a barrier towards effective cybersecurity, by undermining the trust and collaboration between these functions, and thus hindering communications and knowledge exchange.

Decisions at the organisational level are also affected by the potential for physical impact caused by an OT incident (e.g., loss of service, injury). As such, OT-centred organisations have developed a culture of safety over the years [68], which is uncommon in IT-based organisations. The OT digitalization has also brought the prospect of a cyber incident causing physical damage. However, the relationship between the two cultures is still unclear. Future research could investigate the extent to which these two cultures overlap, or how the predominant safety culture (e.g., perceptions, attitudes) affect the security culture both at an organisational and managerial level, as well as at the individual level.

According to our analysis, external stakeholders impact the security culture of OT organisations, with their primary contribution being knowledge transfer at a point where most organisations have low OT security maturity. Previous research has demonstrated external stakeholders' impact on a company's knowledge and organisational practices [69], with knowledge communicated through various informal and formal mediums (e.g., steering groups, conversations, training, policies and procedures) [40], as also demonstrated through our analysis. To our knowledge, our study is one of very few looking at the effect of consultancy on cybersecurity practices, and accordingly, security culture in organisations. Generally, the consultancy processes described in this work have led to changes in how cybersecurity is perceived and managed in OT organisations. This is partly owned to the elevation of cybersecurity to a visible business goal in recent years, which has strengthened the remit of change for these external stakeholders. This contrasts with Poller et al.'s case study [50], where it was recognised that the consultants' remit did not explicitly include advising on organisational practices, thus failing to have long term impact.

Aside from their positive contributions, we have also observed a move of OT cybersecurity experts to consultancies during our research. The acquisition of talent by consultancies which can offer higher salaries and other benefits is hurting organisations that use OT, as it further limits the pool of OT expertise they can tap into. Moreover, substandard security works by consultancies and solution vendors were also commonly referenced in our participants' responses. Given the limited security understanding of many of these organisations, work from these external stakeholders can provide them with a false sense of assurance. Accordingly, this leads to a situation where organisational security culture cannot flourish, as cybersecurity is perceived as an issue that was addressed by external stakeholders.

Organisations can partially prevent these substandard solutions by building their 'intelligent customer' capability [70], i.e., obtaining an adequate level of security knowledge and a wider understanding of how security fits into their operations. This in turn enables organisations to make informed choices when outsourcing their security, as well as being able assess the quality of the work delivered. This is a sensible approach for many aspects of security, including the procurement of services such as intrusion detection systems (IDS) or security operation centres (SOC). However, while a company's technology and processes are often tailored by external professionals, and security knowledge is transferred to the relevant functions, other, softer sides of culture, need to be developed in-house.

Namely, the role of management and security communications are two essential culture-affecting factors which cannot be as easily influenced by these external stakeholders [71]. The top management's role in developing a security culture is commonly referenced in the literature [22], with our participants also agreeing that this top-down approach is necessary, especially at the current stage where organisations have only recently started improving their cybersecurity practices. Interventions, coordination, and communication from the upper echelons of a company must be present to engage employees and convince them about the importance of cybersecurity [72]. The role of direct supervision is also important, as employees' security perceptions are impacted by the prioritization of security by their direct managers [73]. Finally, existing communication channels and methods need to be leveraged with language that is familiar to employees, to embed security into other core organisational values including safety and the provision of essential services such as clean water or electricity.

All in all, external security experts have the potential to greatly benefit organisations using OT. They set strong foundations through designing security processes and procedures and improving their technology. Additionally, they are influential in shaping various factors regarded as important to enhance a security culture, including liaising with an organisation's management to coordinate security efforts. More importantly, their collaboration with cybersecurity responsible personnel can directly affect their personnel's attitudes and perceptions around security.

Nevertheless, organisations need to have the absorptive capacity to exploit this external knowledge [74], by obtaining it, and assimilating it internally [75]. We have demonstrated how external experts through the process of consultancy are crucial in this knowledge exchange with organisations using OT. However, as cybersecurity is not a one-off purchase, organisations using OT should make active efforts to communicate the need for security by considering the different mindsets and values of OT employees, as well as by providing relevant security awareness and training, to assimilate this knowledge. This in turn, can lead to an enhanced security culture, where security becomes embedded into everyday processes and practices, as well as employees' duties.

6. Conclusion and recommendations

Cybersecurity for OT is a fast-growing area, requiring organisations using OT to make drastic changes of their practices, technologies, and people. Accordingly, these changes constitute the first step towards developing a security culture. Through our analysis of 33 interviews with professionals with a security related role in the OT space, we have identified three key organisational obstacles: governance, lack of communication, and lack of expertise. Moreover, we have demonstrated the role of security consultants and security solution vendors have in overcoming them. Consequently, these stakeholders set some of the foundations for developing this culture by breaking down communication and knowledge barriers and shaping various culture affecting factors such as policies and procedures. Overall, our work highlights the role external stakeholders have in the development of an organisational security culture, an aspect that is overlooked in the security culture literature.

While these external experts contribute to the early stages of culture development, organisations using OT need to be able to absorb their expertise and expand the scope of their efforts to achieve a strong security culture. Future research could investigate which conditions make an organisation better at absorbing this external knowledge, and how its assimilation can lead to a stronger security culture. As such, we conclude with three recommendations for organisations using OT.

1. Target different employees based on their roles and "mindsets" on the need for cybersecurity. Accordingly, meditate these differences to allow for improved understanding between functions and increased knowledge absorption both from external sources as well as inter-departmentally.
2. Rather than over relying on IT-based security expertise, training OT personnel in cybersecurity at various stages of their career through apprenticeships, certifications, and degrees, can help accelerate the closing of the expertise gap.
3. The use of external expertise through consultancy and solution vendors can help build strong foundations for cybersecurity, but it takes more to cultivate a security culture. A top-down effort to convey the need for cybersecurity to the various functions responsible and targeted communications are especially important to increase your organisation's absorption capabilities before efforts are made to assimilate this knowledge and enhance your security culture.

Acknowledgments

This project was funded by the UK EPSRC grant EP/S022503/1 that supports the Centre for Doctoral Training in Cybersecurity delivered by UCL's Departments of Computer Science, Security and Crime Science, and Science, Technology, Engineering and Public Policy.

We would also like to thank the four anonymous reviewers whose insightful comments and suggestions have improved this paper.

References

[1] Symantec, ‘Smarter Security for Manufacturing in The Industry 4.0 Era’, 2017. https://docs.broadcom.com/doc/industry-4.0-en (accessed Aug. 15, 2022).

[2] 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.

[3] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, ‘The industrial internet of things (IIoT): An analysis framework’, *Computers in Industry*, vol. 101, pp. 1–12, Oct. 2018, doi: 10.1016/j.compind.2018.04.015.

[4] ‘Critical National Infrastructure | CPNI’. https://www.cpni.gov.uk/critical-national-infrastructure-0 (accessed Aug. 01, 2021).

[5] ‘Definition of Operational Technology (OT) - Gartner Information Technology Glossary’, *Gartner*. https://www.gartner.com/en/information-technology/glossary/operational-technology-ot (accessed Feb. 12, 2023).

[6] N. Tuptuk and S. Hailes, ‘Security of smart manufacturing systems’, *Journal of Manufacturing Systems*, vol. 47, pp. 93–106, Apr. 2018, doi: 10.1016/j.jmsy.2018.04.007.

[7] 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.

[8] Sean Michael Kerner, ‘Colonial Pipeline hack explained: Everything you need to know’, *WhatIs.com*. https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know (accessed Feb. 12, 2023).

[9] NCSC, ‘NIS introduction’, 2019. https://www.ncsc.gov.uk/collection/caf/nis-introduction (accessed Aug. 15, 2022).

[10] ‘Cyber security - Electrical, Control and Instrumentation (E, C&I) - HSE’. https://www.hse.gov.uk/eci/cyber-security.htm (accessed Feb. 12, 2023).

[11] ‘Maritime cyber risk’. https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx (accessed Feb. 12, 2023).

[12] ‘The 5 Waves of Information Security – From Kristian Beckman to the Present | SpringerLink’. https://link.springer.com/chapter/10.1007/978-3-642-15257-3_1 (accessed Feb. 12, 2023).

[13] 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.

[14] 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.

[15] S. Evripidou, U. D. Ani, J. D McK. Watson, and S. Hailes, ‘Security Culture in Industrial Control Systems Organisations: A Literature Review’, in *Human Aspects of Information Security and Assurance*, in IFIP Advances in Information and Communication Technology. Cham: Springer International Publishing, 2022, pp. 133–146. doi: 10.1007/978-3-031-12172-2_11.

[16] DCMS, ‘Water Sector Cyber Security Strategy’, p. 12.

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

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

[19] O. A. Michalec, D. van der Linden, S. Milyaeva, and A. Rashid, ‘Industry Responses to the European Directive on Security of Network and Information Systems (NIS): Understanding policy implementation practices across critical infrastructures’, presented at the Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020), 2020, pp. 301–317. Accessed: Feb. 01, 2022. [Online]. Available: https://www.usenix.org/conference/soups2020/presentation/michalec

[20] T. Wallis and C. Johnson, *Implementing the NIS Directive, driving cybersecurity improvements for Essential Services*. 2020, p. 10. doi: 10.1109/CyberSA49311.2020.9139641.

[21] Idaho National Laboratory, ‘Building an Industrial Cybersecurity Workforce, A Manager’s Guide’. Idaho National Laboratory. Accessed: Feb. 21, 2023. [Online]. Available: https://inl.gov/wp-content/uploads/2021/02/ICS_Workforce-ManagersGuide2021.pdf

[22] 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.

[23] O. Michalec, S. Milyaeva, and A. Rashid, ‘When the future meets the past: Can safety and cyber security coexist in modern critical infrastructures?’, *Big Data & Society*, vol. 9, no. 1, p. 20539517221108370, Jan. 2022, doi: 10.1177/20539517221108369.

[24] 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.

[25] 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.

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

[27] E. H. Schein, 'Organizational Culture and Leadership', p. 458, 1985.

[28] R. von Solms and J. van Niekerk, 'From information security to cyber security', *Computers & Security*, vol. 38, pp. 97–102, Oct. 2013, doi: 10.1016/j.cose.2013.04.004.

[29] F. W. Guldenmund, 'The nature of safety culture: a review of theory and research', *Safety Science*, vol. 34, no. 1, pp. 215–257, Feb. 2000, doi: 10.1016/S0925-7535(00)00014-X.

[30] 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.

[31] K. Dewey, G. Foster, C. Hobbs, and D. D. Salisbury, 'Nuclear Security Culture in Practice', p. 46, 2021.

[32] T. M. Bisbey, M. P. Kilcullen, E. J. Thomas, M. J. Ottosen, K. Tsao, and E. Salas, 'Safety Culture: An Integration of Existing Models and a Framework for Understanding Its Development', *Hum Factors*, vol. 63, no. 1, pp. 88–110, Feb. 2021, doi: 10.1177/0018720819868878.

[33] 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.

[34] T. O. Naevestad, 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*, S. Haugen, A. Barros, C. VanGulijk, T. Kongsvik, and J. E. Vinnem, Eds., Leiden: Crc Press-Balkema, 2018, pp. 3031–3039. Accessed: Feb. 28, 2022. [Online]. Available: https://www.webofscience.com/wos/woscc/summary/0c5f245f-6b80-49b6-8e6f-0a8b788258c4-267f1b99/relevance/1

[35] T. O. Naevestad, 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*, S. Haugen, A. Barros, C. VanGulijk, T. Kongsvik, and J. E. Vinnem, Eds., Leiden: Crc Press-Balkema, 2018, pp. 3021–3029. doi: 10.1201/9781351174664-379.

[36] 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, 2021, doi: 10.1111/rego.12423.

[37] T. Wallis, G. Paul, and J. Irvine, *Organisational Contexts of Energy Cybersecurity*. 2021.

[38] J. B. Quinn, 'Strategic Outsourcing: Leveraging Knowledge Capabilities', *MIT SMR*, Jul. 1999, Accessed: Feb. 18, 2023. [Online]. Available: https://sloanreview.mit.edu/article/strategic-outsourcing-leveraging-knowledge-capabilities/

[39] S. Nevo, M. R. Wade, and W. D. Cook, 'An examination of the trade-off between internal and external IT capabilities', *The Journal of Strategic Information Systems*, vol. 16, no. 1, pp. 5–23, Mar. 2007, doi: 10.1016/j.jsis.2006.10.002.

[40] A. Bradshaw, V. Pulakanam, and P. Cragg, 'Knowledge Sharing in IT Consultant and SME Interactions', *AJIS*, vol. 19, Oct. 2015, doi: 10.3127/ajis.v19i0.1026.

[41] M. Pozzebon and A. Pinsonneault, 'The Dynamics of Client-Consultant Relationships: Exploring the Interplay of Power and Knowledge', *Journal of Information Technology*, vol. 27, no. 1, pp. 35–56, Mar. 2012, doi: 10.1057/jit.2011.32.

[42] A. Bradshaw, P. Cragg, and V. Pulakanam, 'Do IS consultants enhance IS competences in SMEs?', *The Electronic Journal of Information Systems Evaluation*, vol. 16, pp. 13–24, Jan. 2012.

[43] Y. M. Ha and H. J. Ahn, 'Factors affecting the performance of Enterprise Resource Planning (ERP) systems in the post-implementation stage', *Behaviour & Information Technology*, vol. 33, no. 10, pp. 1065–1081, Oct. 2014, doi: 10.1080/0144929X.2013.799229.

[44] D.-G. Ko, L. J. Kirsch, and W. R. King, 'Antecedents of Knowledge Transfer from Consultants to Clients in Enterprise System Implementations', *MIS Quarterly*, vol. 29, no. 1, pp. 59–85, 2005, doi: 10.2307/25148668.

[45] C. Cerruti, E. Tavoletti, and C. Grieco, 'Management consulting: a review of fifty years of scholarly research', *Management Research Review*, vol. 42, no. 8, pp. 902–925, Jan. 2019, doi: 10.1108/MRR-03-2018-0100.

[46] B. P. Bloomfield and A. Danieli, 'The Role of Management Consultants in the Development of Information Technology: The Indissoluble Nature of Socio-Political and Technical Skills*', *Journal of Management Studies*, vol. 32, no. 1, pp. 23–46, 1995, doi: 10.1111/j.1467-6486.1995.tb00644.x.

[47] L. Argote, B. McEvily, and R. Reagans, 'Managing Knowledge in Organizations: An Integrative Frame-

work and Review of Emerging Themes', *Management Science*, vol. 49, no. 4, pp. 571–582, 2003.

[48] J. Haney, W. Lutters, and J. Jacobs, 'Cybersecurity Advocates: Force Multipliers in Security Behavior Change', *IEEE Security & Privacy*, vol. 19, no. 4, pp. 54–59, Jul. 2021, doi: 10.1109/MSEC.2021.3077405.

[49] M. Gale, I. Bongiovanni, and S. Slapnicar, 'Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead', *Computers & Security*, vol. 121, p. 102840, Oct. 2022, doi: 10.1016/j.cose.2022.102840.

[50] A. Poller, L. Kocksch, S. Türpe, F. A. Epp, and K. Kinder-Kurlanda, 'Can Security Become a Routine?: A Study of Organizational Change in an Agile Software Development Group', in *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, Portland Oregon USA: ACM, Feb. 2017, pp. 2489–2503. doi: 10.1145/2998181.2998191.

[51] A. Bryman, *Social Research Methods*. Oxford University Press, 2016.

[52] V. Braun and V. Clarke, 'Using thematic analysis in psychology', *Qualitative Research in Psychology*, vol. 3, no. 2, pp. 77–101, Jan. 2006, doi: 10.1191/1478088706qp063oa.

[53] G. W. Ryan and H. R. Bernard, 'Techniques to Identify Themes', *Field Methods*, vol. 15, no. 1, pp. 85–109, Feb. 2003, doi: 10.1177/1525822X02239569.

[54] M. Williams and T. Moser, 'The art of coding and thematic exploration in qualitative research', *International Management Review*, vol. 15, no. 1, pp. 45–55, 2019.

[55] National Protective Security Authority, 'Think Before You Link (TBYL) | NPSA'. https://www.npsa.gov.uk/security-campaigns/think-you-link-tbyl-0 (accessed May 18, 2023).

[56] E. C. Page, 'Bureaucrats and expertise: Elucidating a problematic relationship in three tableaux and six jurisdictions', *Sociologie du Travail*, vol. 52, no. 2, pp. 255–273, Apr. 2010, doi: 10.1016/j.soctra.2010.03.021.

[57] European Parliament, 'The NIS2 Directive: A high common level of cybersecurity in the EU | Think Tank | European Parliament'. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333 (accessed Aug. 15, 2022).

[58] W. Alkalabi, L. Simpson, and H. Morarji, 'Barriers and Incentives to Cybersecurity Threat Information Sharing in Developing Countries: A Case Study of Saudi Arabia', in *2021 Australasian Computer Science Week Multiconference*, Dunedin New Zealand: ACM, Feb. 2021, pp. 1–8. doi: 10.1145/3437378.3437391.

[59] D. Norris, A. Joshi, and T. Finin, 'Cybersecurity Challenges to American State and Local Governments', presented at the 15th European Conference on eGovernment, 2015.

[60] D. Ashenden, 'Information Security management: A human challenge?', *Information Security Technical Report*, vol. 13, no. 4, pp. 195–201, Nov. 2008, doi: 10.1016/j.istr.2008.10.006.

[61] J. M. Blythe, L. Coventry, and L. Little, 'Unpacking security policy compliance: The motivators and barriers of employees' security behaviors', presented at the Symposium on Usable Privacy and Security (SOUPS), 2015.

[62] D. Ashenden and A. Sasse, 'CISOs and organisational culture: Their own worst enemy?', *Computers & Security*, vol. 39, pp. 396–405, Nov. 2013, doi: 10.1016/j.cose.2013.09.004.

[63] D. Burrell, 'An Exploration of the Critical Need for Formal Training in Leadership for Cybersecurity and Technology Management Professionals', 2019, pp. 1420–1432. doi: 10.4018/978-1-5225-8356-1.ch069.

[64] 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.

[65] S. Schinagl and R. Paans, 'Communication Barriers in the Decision-making Process: System Language and System Thinking', presented at the Hawaii International Conference on System Sciences, 2017. doi: 10.24251/HICSS.2017.738.

[66] M. Bada, A. M. Sasse, and J. R. C. Nurse, 'Cyber Security Awareness Campaigns: Why do they fail to change behaviour?', p. 11.

[67] K. Li, K. M. Ramokapane, and A. Rashid, '"Yeah, it does have a...Windows `98 Vibe'': Usability Study of Security Features in Programmable Logic Controllers'. arXiv, Aug. 04, 2022. Accessed: Sep. 29, 2022. [Online]. Available: http://arxiv.org/abs/2208.02500

[68] J. C. Le Coze, 'How safety culture can make us think', *Safety Science*, vol. 118, pp. 221–229, Oct. 2019, doi: 10.1016/j.ssci.2019.05.026.

[69] R. L. D. Costa, N. António, M. Sampaio, and I. Miguel, 'The boundaries in the area of knowledge transfer in management consulting', *Gest. Prod.*, vol. 28, no. 1, p. e4956, 2021, doi: 10.1590/1806-9649.2020v28e4956.

[70] 'Human factors/ergonomics – Intelligent customer capability'. https://www.hse.gov.uk/humanfactors/topics/customers.htm (accessed Feb. 14, 2023).

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

[72] J. D'Arcy and G. Greene, 'Security culture and the employment relationship as drivers of employees' security compliance', *Information Management & Computer Security*, vol. 22, no. 5, pp. 474–489, Jan. 2014, doi: 10.1108/IMCS-08-2013-0057.

[73] 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.

[74] W. M. Cohen and D. A. Levinthal, ‘Absorptive Capacity: A New Perspective on Learning and Innovation’, *Administrative Science Quarterly*, vol. 35, no. 1, pp. 128–152, 1990, doi: 10.2307/2393553.

[75] S. A. Zahra and G. George, ‘Absorptive Capacity: A Review, Reconceptualization, and Extension’, *The Academy of Management Review*, vol. 27, no. 2, pp. 185–203, 2002, doi: 10.2307/4134351.

A Purdue Reference Architecture Model

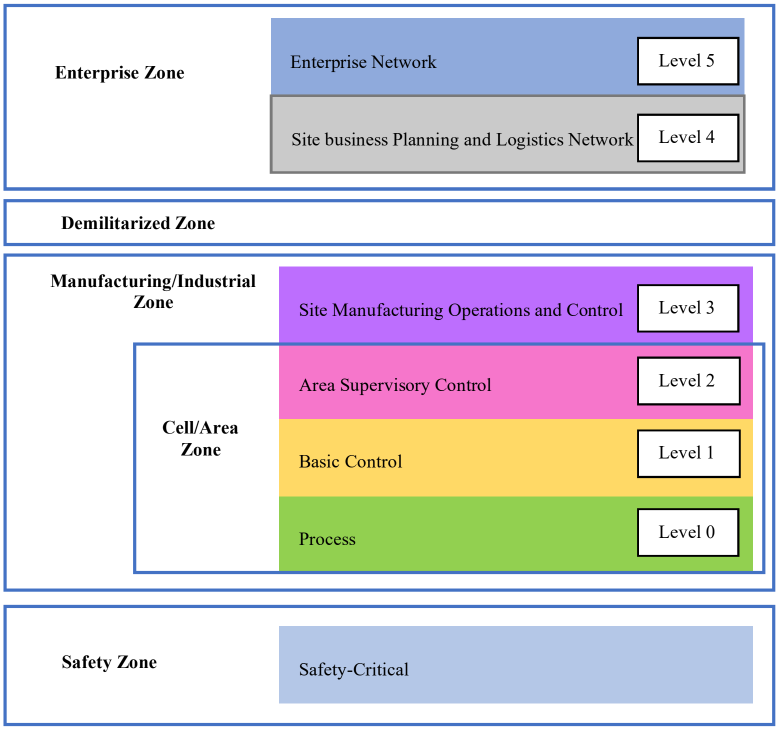

Fig. 1 Purdue Reference Architecture Model

B Participants’ Role and Sector

#	Role	Sectors
P01	OT Manager	Water
P02	OT Manager	Water
P03	OT Manager	Energy
P04	Consultant	Transport
P05	Security Researcher	Manufacturing
P06	Security Manager	Water
P07	CISO	Energy
P08	CISO	Water
P09	Consultant	Transport
P10	Consultant	Various, p. Transport
P11	Security Manager	Energy
P12	Consultant	Various, p. Oil & Gas
P13	CISO	Transport
P14	Security Manager	Transport
P15	Security solutions vendor	Various
P16	Consultant	Various, p. Energy
P17	Security solutions vendor	Various
P18	Consultant	Various
P19	Regulator	Energy
P20	Regulator	Transport
P21	Consultant	Various, p. Manufacturing
P22	Consultant	Various, p. Oil and Gas
P23	Technology Manager	Water
P24	Government & Organisations Coordinator	Various, p. Maritime
P25	OT Manager	Energy
P26	Security solutions vendor	Transport
P27	Security Researcher	Various
P28	Academia & Industry Coordinator	Maritime
P29	Consultant	Various
P30	Consultant	Transport
P31	Consultant	Energy

P32	Consultant	Various
P33	Security Manager	Energy

Note: various p. signifies that a participant works across various sectors but primarily operates in one.

C Sample interview topic guide

We provide a sample interview guide that was used as a basis for our interviews with consultants and security product vendors.

- Participant's background
  - o Previous & Current roles
- Details about company: services provided, structure of the company.
  - o Can you describe the typical sales/consultancy process and/or a challenging case?
- In-depth questions about products, services
  - o Relate to publicly available information (blogposts, websites, talks etc.) and previous conversations/emails.
- Security culture: How would you define it?
  - o Who is responsible? Who else plays a part?
  - o Challenges? What works?
  - o If safety culture is mentioned – parallels, differences?
- Intra-organisational collaborations (if applicable)
  - o Partnerships between vendors and consultancies,
  - o Security solution providers' relationship with their supply chain etc.
  - o Relationships with competent authorities
- Differences between sectors and/or companies
  - o On how they utilise participants' services
  - o Generally, with respect to their security maturity
- Debriefing & thanking for participation

D Codebook

We provide some key themes reported on this work, with a description and example quotes. Codes in bold are axial codes representing a wider theme, while those underlined are more specific open codes.

Governance and Management

Description: Instances of governance and management issues, or ways to improve this

<u>Governance issues</u>: *"As companies have organically grown over the years and I've typically seen this in all the oil and gas sector is, and in the electricity sector, departments become quite heavily siloed and fragmented, and they only talk up when they actually sit alongside each other and they're all actually doing something in a chain."*

Communication

Description: Instances of communication barriers, or ways to improve this situation.

<u>OT and IT communication:</u> *"And often a standing point where neither of them effectively communicates with each other."*

"We will be there sat in between the IT department and their engineering OT department trying to kind of translate between the two and get them to understand each other's point of view and this kind of stuff."

<u>Communication with the board:</u> *"I asked the NCSC to come and present to the board with me. So we had a kind of government lens and a ... member of the security services stood in front of the board telling them there's a real risk. Really, really made people think, wake up and think."*

Expertise

Description: Instances of gaps in expertise, or ways to bridge the expertise gap.

<u>OT Expertise:</u> *"They often have an educational divide between cybersecurity teams that often don't understand operational technology and engineering teams who don't understand cybersecurity."*

"There is a talent shortage in OT cybersecurity at least for the energy sector. But my understanding is the energy sector is fairly mature, well, relatively mature and at the other sectors are further behind with the exception of maybe some oil and gas stuff."

<u>General training</u>: *"So one of the people from that team moved to my team and we've sponsored them on an MSc and so and that's the case. People who are more on the compliance side, where we're looking at NIS regulations, then they're looking more at sort of management of risk and qualifications or system, you know, the certificate in security management type qualifications. And then the security engineers that deal with operational technology, they tend*

to be more in the SANS space of the IEC 622443 type training. And so yeah it, as I say it really depends on the particular thing. And then you know intelligence analysts, we would use CREST training for, that would be the most relevant for them."

Security Culture

Description: Mentions of what a security culture entails, what falls under a security culture change process, or comparisons with other cultures

What is security culture: *"That cultural piece ... it's that understanding and inherent sort of guessing, ... you know you asked the right questions, you adopt the right behaviours, ... you design things securely, you make solutions that are secure."*

Comparisons with safety culture: *"I think security, if they've got a good safety culture it's not that much of a stretch for them to develop a good security culture on the OT side of things."*

Security culture and consultants

Description: Ways consultants contribute to an organisation, either by overcoming the three organisational obstacles or more generally how they shape factors that affect culture

Contribution of consultants: *"All about helping people who have OT plants to understand what their risks are. Usually start from absolute zero knowledge of OT security and help them get their head around where the gaps are, where the best place for them to spend their money is."*

Need for consultancy: *"There's a mix of reasons, so there are some ... companies that are really small. They have no security staff and now they're subject to NIS and then they can't, can't just build the team out of nowhere. Right. You have to delegate almost all responsibilities in other instances. It's just that the expertise isn't there."*

Security culture and security product vendors

Description: Ways security product vendors contribute to an organisation, either by overcoming the three organisational obstacles or more generally how they shape factors that affect culture

Contribution by vendors: "*We have to educate and bring people along with our way of thinking and understanding. ... Umm, but we have to be successful, get people asking the right questions.*

"We were primarily currently selling products of course, ... so I suppose from that from that sense, you know we're enabling this in that the alerts we produce and the data we can produce for companies, give them a window into their networks that they didn't have before. So knowledge, one of the foundations of culture is knowledge."

State of OT cybersecurity

Description: General comments on the state of OT cybersecurity by practitioners

State of OT cybersecurity: "*The cybersecurity industry is starting; they are babies at this game."*

"It's embryonic within the rail sector."

Important triggers for increased cybersecurity awareness: *"It's also the other last thing I would say with that as well is a rise in ransomware, is a massive concern as well, and we know that you know, for every ransomware attack that makes a headlines, there's many, many more that don't, because companies just end up paying it because they don't want the bad publicity."*