Understanding Operational Technology Personnel's Mindsets and Their Effect on Cybersecurity Perceptions: A Qualitative Study With Operational Technology Cybersecurity Practitioners

Stefanos Evripidou

Centre for Doctoral Training in Cybersecurity, University College London (UCL), stefanos.evripidou.16@ucl.ac.uk

Jeremy D McK. Watson

Department of Science Technology Engineering and Public Policy (STEaPP), University College London (UCL), jeremy.watson@ucl.ac.uk

Operational Technology (OT) is hardware and software that monitor and control industrial processes in sectors such as water and energy. OT's increased digitalisation which expanded its attack surface, heightened institutional pressures including regulation, and the evolving threat landscape have compelled companies using OT to improve their cybersecurity. Security often clashes with employees' values and hinders them from performing their primary job tasks, leading to its circumvention. OT personnel are a user group with distinctive characteristics, including the cyber-physical technology they use, and subsequently, their safety culture. Nevertheless, there's little research on how OT personnel's mindsets are formed, and in turn, how these mindsets affect their cybersecurity beliefs and behaviours.

As such, we have conducted 72 interviews with OT cybersecurity practitioners across various sectors on their experiences working with OT practitioners. Our analysis demonstrates a number of factors that shape OT personnel's mindsets: namely, the prioritisation of other operational values, operational realities and challenges, and their occupational pathways. In turn, these factors lead to misperceptions around cybersecurity, specifically in two areas: technological misperceptions, and the stereotyping of occupational practices between IT and OT. Accordingly, we discuss OT cybersecurity practitioners' efforts to influence cybersecurity in these environments, and how the acknowledgment of these factors and misperceptions aids their efforts. Finally, we call for a better understanding of OT personnel's relationship with cybersecurity by proposing future research avenues.

CCS CONCEPTS •**Security and privacy~Human and societal aspects of security and privacy~Usability in security and privacy, •Social and professional topics~Computing / technology policy**

Additional Keywords and Phrases: Operational Technology, Security Culture, Mindsets, Mental Models, Cybersecurity, Organisational Cybersecurity

1 INTRODUCTION

Operational technology (OT) consists of hardware and software that monitor and control industrial processes [1], in sectors such as water, energy, and transport, and is often used to operate a nation's critical infrastructure (CI) [2]. Ensuring the cybersecurity of OT is essential, given its importance to nations' economy, safety, and security [2]. In recent years, an increased digitalisation in OT has expanded its attack surface (e.g., IT/OT convergence [3], Industry 4.0 [4]), with recent

reports by national security agencies warning about 'enduring and significant' threats to CI cybersecurity [5, 6]. Governments and other institutions have introduced regulations [7], directives [8], and standards [9] in an effort to boost OT cybersecurity practices. In turn, many companies using OT are in the process of improving their practices and technologies, and attempting to influence OT personnel's beliefs and behaviours around cybersecurity [10]. Despite that, organisational and people-centred research on OT cybersecurity is scarce [11], and there's little research focusing on what shapes OT personnels' mindsets and how they affect their cybersecurity beliefs and behaviours.

OT cybersecurity poses some distinct challenges compared to IT cybersecurity [12]. Given the differences in technology and operational processes, security practices need be tailored to operational needs (e.g., OT systems have a much longer lifespan than IT). OT cybersecurity is also complicated by the diversity of stakeholders involved in the process. At the institutional level, governments have a responsibility for improving OT companies' cybersecurity in the interests of national security and public safety [13, 14]. Organisationally, various functions, including engineering, operations, IT, and security, need to collaborate [15]. The extant literature has described various challenges which impede OT cybersecurity efforts, including governance issues and lack of communication between the OT and IT functions [10], and differences in practices between safety and security practitioners [16].

Research in human-centred cybersecurity has long recognised that users' security behaviours are influenced by their goals, needs, and beliefs (e.g., perceptions, attitudes etc.) [17, 18, 19]. At the organisational level, research has investigated how users' security decisions are affected by the usability of security, as well as other competing pressures and values (e.g. workload, efficiency) [20, 21]. Factors such as communication issues and the lack of cybersecurity ownership have also been show to affect organisational cybersecurity [10, 22]. Similar challenges currently faced by cybersecurity have had to be overcome by OT companies in their attempts to develop a culture of safety in the past decades (e.g., friction with other values, influencing beliefs and behaviours etc.) [23, 24]. Nevertheless, there's scant academic research on how OT personnel's mindsets (i.e., their set of values, beliefs, perceptions etc.) are shaped and, in turn, how they affect their cybersecurity beliefs and behaviours.

Against this backdrop, identifying the factors that affect OT personnels' mindsets can enable a more effective tailoring of cybersecurity to their values and needs, easing the implementation of security measures. Accordingly, such efforts can lead to the strengthening of the cybersecurity culture of companies using OT. As such, we have interviewed 72 practitioners with OT cybersecurity related roles on the topic of security culture development at various levels (e.g., institutional, organisational, personnel etc.). In this paper, we report our findings which aim to answer the following questions:

1. Which factors shape OT personnel's mindsets according to OT cybersecurity practitioners' experiences?
2. How do these factors influence OT personnel's cybersecurity beliefs and behaviours?

Our results demonstrate a number of factors that shape OT personnel's mindsets: namely, the prioritisation of values such as process safety and availability, operational realities which have been altered by technological change, and their occupational development pathways. In turn, these factors influence a number of cybersecurity misperceptions, which we categorise in two areas: technological misperceptions and the stereotyping of occupational practices between IT and OT. We demonstrate security practitioners' efforts to improve cybersecurity in OT environments, including the pushback they receive. Accordingly, we discuss our findings, propose future research avenues, and conclude with recommendations on how OT personnel's cybersecurity beliefs and behaviours can be improved. Our key contribution is the identification of a number of factors that affect OT personnel's mindsets, and in turn, cybersecurity beliefs and behaviours.

2 BACKGROUND AND RELATED WORK

2.1 Human-centred Cybersecurity

Researchers have investigated users' interactions with security technologies and processes, aiming to dispel beliefs that users were to blame for non-compliance with security (i.e., 'the weakest link') [25, 26]. Accordingly, research has demonstrated how the lack of user-centred design approaches [27], or the incompatibility of security measures with work practices (e.g. passwords), leads to non-compliance [17, 28]. To our knowledge, the only usability studies in OT cybersecurity have been conducted by Li et al. [29, 30] where the relationship between the design of PLCs, which are the central control units of a process, and security decisions were investigated. Accordingly, security misperceptions caused by various design constraints were uncovered (e.g., misleading terminology, label and layout design etc.).

Human centred cybersecurity research has been influenced by various domains, including Human Computer Interaction (HCI) [31], organisational [32], and experimental psychology [18], and users' interactions with cybersecurity have been studied using a range of concepts and techniques. Personas, stemming from the HCI field, are user representations designed around users' characteristics, values, and needs [33]. Accordingly, they aim to elicit sympathy for, and improve designers' understanding of potential users, leading to well-informed user-centred design requirements. Personas have been used to study various user groups, such as older adults [34], and millennials [35]. In the context of OT cybersecurity, Faily and Flechais [36] have used personas to elicit security engineering requirements and improve user-centred design in a water utility. The persona of Barry, an instrument technician with maintenance responsibilities, helped showcase the limited visibility IT teams had into water plants and treatment systems, similar to challenges identified elsewhere in the OT cybersecurity literature [10].

Mental models are another concept used in cybersecurity research, stemming from cognitive science. Broadly, mental models are a collection of abstract mental structures representing a user's understanding of a problem or a system [37, 38]. They have been used in various research areas (e.g., risk communication, system dynamics) to improve the design of technologies, as well as educational material [39]. Mental models have also been studied in a variety of cybersecurity domains across different user types (e.g., experts and non-experts [40], journalists [41], young people [42]), as well as applications, tools, and technologies (e.g. smart environments [43], adversarial machine learning [44], cryptocurrency systems [45] etc.). Often, techniques like participants' drawings are used to elicit these mental models [38, 44], with semi-structured interviews also being common [41]. Overall, while mental models have become a common concept in cybersecurity research, some studies use the term mental models as a substitute for attributes like beliefs and perceptions, rather than trying to elicit users' structural understanding of the workings of a system or technology.

Mindsets are another term used in cybersecurity studies [46]. Mindsets have not been researched as extensively as personas or mental models, due to their ambiguity and difficulty in quantifying compared to these more established terms. A mindset has been described a set of abilities, a set of traits, or a set of attitudes, beliefs, and values [46]. As Dutton notes, mindsets as a term can arise from interviews and can be useful as a 'sensitizing concept', helping readers and participants make sense of a more complex set of patterns or observations [47], which was also the case for our research.

Compared to research on users' interactions with security mechanisms in non-work environments, or with specific security tools, there is less research into usable security and the 'friction' it causes in organisational settings [48]. Nevertheless organisational contexts such as the shared working practices, pressures, needs, and established policies and procedures, are bound to affect users' interactions with cybersecurity. For example, research into organisational contexts has demonstrated that security measures can be perceived as a blocker, stifling productivity by adding overhead to employees' workload [49]. Other organisational barriers to cybersecurity commonly include communication issues (e.g.,

software developers and security experts [22, 50], OT and IT teams [10], boards and security practitioners [51]), increased complexity due to the number of stakeholders involved [52], lack of governance and accountability [10, 22] etc.

Security often clashes with users' other, primary tasks. Beautement et al. [28] proposed the concept of the Compliance Budget, which states that individuals have a set cumulative capacity towards security compliance, given its additional effort. Each time an employee is faced with a compliance decision, the compliance cost is accumulated until a breaking point is reached where non-compliance occurs. Karlsson et al. [21] similarly demonstrated that the conflict between security and other organisational values (e.g. efficiency, safety) is the main measure of employees' security compliance, compared to other measures such as employees' intentions to comply, awareness, and self-efficacy. Hu et al. [53] identified two organisational challenges to cybersecurity: the need for data accessibility and work mobility, and the need for efficiency. Subsequently, attempts to limit data access or introduce other security procedures that hinder employees' workload led to worsening attitudes around cybersecurity. Finally, Kirlappos et al. [54] proposed that compliance is not a binary choice, with 'shadow security' emerging as a third option. Accordingly, due to security's impact on their tasks, employees seek less demanding workarounds (i.e. 'shadow security') with a lesser impact on their regular work.

Research has also examined cybersecurity from the perspective of security practitioners. Hielscher et al. [55] have investigated CISOs understanding of human-centred security, demonstrating the non-alignment of industry practices with state of the art research. Reinfelder et al. [56] demonstrated how the lack of organisational structures that include users into security decision making leads to employees being negatively perceived by security personnel. Albrechtsen and Hovden [57] similarly indicated this divide, demonstrating the differing risk perceptions between users and information security managers and the subsequent poor alignment of security with users' workload. Accordingly, researchers have proposed mechanisms to alleviate such these communication and value-conflict issues including Ashenden's and Lawrence's [58] security dialogue workshops, and Hedström et al.'s [59] value-based compliance model.

2.2 Background in OT

OT is commonly found in industrial and automation environments, as well as transport sectors (e.g., rail [60], maritime [61]). Industries using OT are typically categorised as process (e.g. oil, electrical), or discrete processing industries (e.g., consumer goods manufacturing) [62]. Nevertheless, distinctions between engineering processes are rarely made in cybersecurity discourse, and most industrial sectors are clustered under the term OT [63]. OT's cyber-physical nature differentiates it from information technology (IT), which is typically found in home and enterprise environments. The Purdue model is a typical multi-level architecture model for OT, consisting of various technologies. Those at the higher levels, like Industrial Control Systems (ICS), supervise and control more specialised and computationally-limited technologies at the lower levels, such as PLCs and sensors [64]. In the past decades, there has been increased digitalisation and connectivity in OT (e.g., IT/OT convergence [3], Industry 4.0 [4]). Moreover, a trend towards automation has changed the workload of many operators, with their tasks becoming less physical and more supervisory [62]. Despite the technological change's benefits, the OT attack surface has also increased, necessitating the strengthening of its cybersecurity.

OT differs from IT in various technical aspects. For example, OT's lifespan is often in the decades whereas IT has a shorter lifespan of a few years [12], with many OT infrastructures operating legacy ('brownfield') systems, as is the case in the UK where our research was predominantly based. Moreover, OT has historically used numerous, often proprietary, communication protocols compared to the standardised Ethernet protocol in IT [64]. Given OT's technical differences to IT, OT security measures need to be tailored to fit operational realities. Namely, updates in OT require longer timeframes than IT, as OT systems cannot be shut down as easily. As such, updates are undertaken in maintenance windows which are

planned months to years in advance [12]. Another challenge centres around digital forensics, as logging capabilities in existing OT systems, including logs and alarms, are often inadequate to support digital forensics investigations [64]. styles applied. If your figure contains third-party material, you must clearly identify it as such, as shown in the examples.

2.3 Institutional and Organisational OT Cybersecurity

Aside from the technical differences, other organisational and institutional factors complicate OT cybersecurity efforts. For example, the UK's 2018 Network and Information Systems (NIS) regulation resulted in significant cybersecurity improvements in sectors like water, energy, and transportation. Extant research has described how NIS has fostered various inter-organisational collaborations between operators, competent authorities, supply chains, and other stakeholders [60], aiming to adapt NIS to sector-specific contexts [61], or to identify common security requirements between operators and equipment manufacturers [62]. Recent institutional developments further highlight governments' involvement in OT cybersecurity [8], such as the European Union's NIS 2 [63].

At the organisational level, research has looked at the interactions between functions with OT cybersecurity responsibilities. McBride et al. [64] have compared OT and IT cybersecurity practices to create an OT cybersecurity workforce development framework. One such difference is IT's prioritisation of the confidentiality, integrity and availability (CIA) of data, and OT's prioritisation of the safety, reliability, and availability (SRA) of processes. Zanutto et al. [15] described OT cybersecurity as a 'grey area', due to the variety of demands and stakeholders involved in the process, and its complexity in terms of organisational challenges. Namely, cybersecurity efforts were often found to be hindered by top-down management approaches which were incompatible with unexpected situations at industrial sites, and the lack of information sharing between different organisational functions. Evripidou et al. [10] have looked at organisational barriers at the IT/OT border, identifying similar challenges on OT cybersecurity governance and accountability. The lack of expertise and collaboration between OT and IT functions were also found to hinder OT cybersecurity maturity. As such, the role of external experts (e.g., consultants, security service vendors) in helping companies alleviate these challenges was demonstrated. Finally, Michalec et al. [16] investigated the intersection of safety and security, demonstrating how practices such as risk assessments are hampered by the different logics of these practitioners, including safety thinking's more prescriptive nature compared to security thinking.

A number of different roles exist in OT environments. Given the lack of standardised naming conventions, terms like 'automation', 'mechatronics', and 'control systems' professionals are used [65]. Nevertheless, typical roles include operators, who monitor and adjust OT processes, usually split into control room operators and field operators [66]. Another role is that of technicians, who are responsible for maintaining and administering these systems. In the UK, such practitioners are often referred to as engineers, possibly due to differences in vocational education from other countries [67]. Such technicians are not to be confused with the user category of engineers, who are typically responsible for the design of processes, and their roles similarly vary based on industry, specialisation, and organisational needs (e.g., mechanical, shift, control, instrument, process etc.). Accordingly, engineers shape the interaction that users have with OT systems and process environments, including operators and technicians [68]. As OT environments are hierarchically operated with clear chains of command, other roles include shift supervisors, plant managers, and asset owners [69, 73].

OT cybersecurity is a relatively nascent field, and expertise is relatively scarce. Accordingly, efforts to improve OT personnel's cybersecurity skills and create OT cybersecurity professionals have been made in the context of OT/ICS [74, 75], Cyber Physical Systems (CPS) [72], Industry 4.0 [73], and similar offerings exist in the industry [78, 79]. McBride et al. [80, 81] proposed 5 archetypical roles for the future OT cybersecurity workforce after consolidating 81 different operational roles gathered through a workshop: engineer, technicians, analysts, researchers, and managers. The variability

of roles in OT cybersecurity was also highlighted by Ramezan et al. [78] in their analysis of 100 job postings. Nevertheless, gaps exist in current workforce development efforts. Given the limited amount of literature on the topic, some academic reviews revealed no new insights [79]. Criticisms for commercial workforce development efforts and cybersecurity education standards include the fact that their proprietary nature limits the availability of information on their methodology and workings. Moreover, they often do not account for the typical career paths of industrial professionals [74, 83]. While some works provide high-level skills and competencies, they often fail to provide real world examples on operational realities and how they affect cybersecurity (e.g., clashes with other values leading to security friction).

Overall, research in IT companies has described security's clash with other values, the distance between security practitioners and employees, and various other structural factors that affect cybersecurity. Nevertheless, companies using OT differ from many IT companies in terms of values, processes, as well as technology. There is a gap of qualitative studies in OT cybersecurity looking at OT personnel's relationship with cybersecurity. Existing research has mainly focused on organisational challenges between different functions [10, 15], as well as wider institutional challenges (e.g., regulation, supply chain issues) [65, 66]. As such, our research aims to detail the prevalent values and current realities in OT environments and their effect on cybersecurity in a more systematic way, as experienced by OT cybersecurity practitioners.

3 METHODOLOGY

3.1 Population Sample and Recruitment

We have conducted 72 semi-structured interviews with participants with OT cybersecurity related roles. This research has been approved by the authors' institutional ethics committee (ID number: Z6364106/2022/04/115). Participants provided their consent by signing a consent form. Codes were used to replace participants' identifiable information in order to pseudonymise them, and access to the data was only granted to the research team. Participants agreed for their responses to appear in future publications pseudonymously and, where possible, paraphrased to avoid identification. In the following sections we will cover the sampling, recruitment, interviewing, and data analysis processes in more detail.

3.2 Interview Design and Data Collection

Our sampling technique was informed by theoretical sampling, where future participants were sought based on the need to validate and expand identified themes in a bottom-up refinement way [81]. Accordingly, our participant focus had shifted based on preliminary findings. Namely, initial findings suggested that most OT sectors share similar cybersecurity challenges, which widened our initial scope from the energy and water sectors. More importantly, the role of external stakeholders in OT cybersecurity also become apparent, as considerable OT cybersecurity expertise is found in the security and consulting industries, rather than in companies that use OT. As such, we expanded our potential participant pool to include practitioners from additional sectors (e.g., transport, oil & gas, manufacturing), and more importantly, various external practitioners to provide a more complete and accurate picture of the OT cybersecurity landscape.

Participants were primarily recruited through LinkedIn, and the primary author's attendance, delivering of presentations, and networking in industry events. Additionally, snowball sampling was used, where participants were asked for an introduction to potential future participants. The final sample includes 72 internal and external professionals from various OT sectors, working across 49 companies. Broadly, participants working in companies that use OT had managerial roles (OT managers, CISOs etc.). External practitioners had OT security related roles in consultancies, security product and service providers, original equipment manufacturers (OEMs), universities, and competent authorities (i.e., regulators).

OT cybersecurity is a relatively young field, complicating expertise judgements, and we will refrain from doing so. The market demand for such expertise has led many practitioners to move to external security roles in consultancies and security companies. Many participants had recently changed jobs, or have done so since the interview. Despite having an external or cybersecurity role at the time of the interview, many of our participants had extensive experience in OT environments, as is the case for the majority of quoted participants. Overall, at least 45 of the 72 participants had considerable experience in an engineering or automation role in OT environments. Appendix A.1 provides more details on our participants' roles, company types, and the complexity of defining the roles existing in OT, as well as expertise in OT cybersecurity.

3.3 Data Analysis

We have used Microsoft Teams' recording and transcribing functionalities. We subsequently used the NVivo software to code the transcripts, and employed reflexive thematic analysis to analyse the collected data [85, 86]. More specifically, our analysis was based on Braun and Clarke's version of reflexive thematic analysis [82]. Over the past two decades, they have contributed to the refinement and development of their approach, emphasising the centrality of the researcher in knowledge production, and a more fluid and recursive approach compared to coding reliability and codebook approaches [87, 88]. The primary author was instrumental in the data familiarisation, coding, and theme searching phases. More specifically, interesting or potentially useful points were noted down at the end of each interview. Subsequently, the primary author revisited the audio interview, edited the transcription, and further supplemented existing notes. Accordingly, data was entered into NVivo and coded in a recursive manner. Collaborative discussion with the other authors ensued to further review and refine the identified themes. Finally, the primary author was responsible for writing up this work. We provide more examples of codes and themes used in this work in Appendix A.3.

As part of the renewed discussion on reflexive thematic analysis [89, 90], and following the advice of Braun and Clarke [83], we attempt to locate this research upon different theoretical and conceptual assumptions. Namely, key assumptions about thematic analysis can be expressed in spectrums including: experiential versus critical orientation to data, inductive versus deductive analysis, and semantic versus latent coding of data [86]. In this research, we take a more experiential approach, ceding the meaning to the participant, as participants have been purposely selected based on their experience and knowledge in cybersecurity and OT environments.

With respect to inductive and deductive analysis [88], our approach used both analyses. Namely, we employed both deductive and inductive means to analyse the conflict between security and other organisational values. Similar conflicts have been described in the literature in non-OT organisational contexts. As such, we have enquired about them, as well as deductively inferred other factors which are not as common in other organisational contexts (e.g., safety). The distinction between semantic and latent analysis focuses on how much the analysis is capturing explicitly stated meanings, or whether it is occupied with the ideas and assumptions that underpin the data [82]. The primary author has a background in computer science and cybersecurity. While their research focuses on institutional and organisational phenomena, they do not have a first-hand experience of practicing cybersecurity outside of academia. As such, our analysis was more semantic than latent, given that our participants were the ones with significant experience in OT cybersecurity and OT environments.

3.4 Terminology Considerations

While mental models have been used far more frequently in research, we have chosen the term mindset for this work. The Oxford English dictionary's definition of mindset [89]*"An established set of attitudes, esp. regarded as typical of a particular group's social or cultural values; the outlook, philosophy, or values of a person; (now also more generally)*

frame of mind, attitude, disposition" falls in line with our thinking, as we aimed to describe this collection of values, attitudes, beliefs etc. of a group of practitioners - OT practitioners in our case.

As previously discussed, some research has used mental models liberally as a substitute for attributes like beliefs and perceptions, rather than trying to elicit users' structural understanding of the workings of a system or technology. Moreover, we did not interview OT practitioners directly. Even though the majority of our participants had an OT background, we decided to not use the term mental models. As such, we adopted the approach described by Dutton [47], where mindsets can arise from the data collection, and can be useful a 'sensitizing' concept for participants to reflect on their cybersecurity experiences. This was true in our case, with mindset arising in 18 of our interviews and mentality in 6. Moreover, when asked to described different mindsets, participants widely understood the question and provided relevant values, perceptions, and behaviours. 'OT' or 'engineering' mindsets were contrasted with 'IT' and 'security' mindsets. While these are simplifications of more complex phenomena, they allowed participants to detail their experiences and perceptions on what makes OT security practices and values different from more conventional information security practices.

4 RESULTS

4.1 Operational Needs and Values (Availability, Production, Safety)

Personnel working in OT environments would often be described as "performance focused", with attributes like the "stability and service" of operations being their primary concern. Similar qualities, such as "availability", "uptime", "production", and "keeping everything running" were mentioned, demonstrating their prioritisation of stable and uninterrupted operations. Many OT companies have to abide to Service Level Agreements (SLAs), which allow for minimal interruptions of service availability, and are often regulated as is the case for essential service providers (e.g., water and energy companies). Similar contractual agreements also exist in non-regulated sectors, such as those between manufacturing companies and their customers. Attributes like availability and downtime can be part of OT personnel's Key Performance Indicators (KPIs) and even monetary bonuses, further amplifying their importance. Accordingly, the introduction of cybersecurity can result in pushback as it is perceived to negatively impact process availability.

> "In the operational technology side, it's all about the availability. So it's just keeping everything up and running. What drives them is not changing anything, it's just having a stable service, you know? And if that means they don't patch anything, they don't upgrade anything for years, they're happy with it because it will just run and that's it. Stability and service is what they want." P_78, Chief Information Security Officer, Energy sector

Safety was also highlighted as a priority in operational environments, with many participants reflecting on the penetration of safety thinking and practices in their industries. For example, many unsafe practices were no longer tolerated and were replaced with safer alternatives, such as not using the stairs' handrails, or leaving items that could lead to safety accidents on the shop floor. This change has also led to the creation of challenging and reporting cultures where personnel are expected to challenge unsafe behaviours and report safety incidents. Commitment to safety was also demonstrated by the variety of safety practices participants mentioned, including "taking 5" and tool checking, where employees are reminded to asses potential safety risks, and check whether they have the requisite equipment before commencing a safety related task. Similarly, companies will run safety "moments", where safety can be raised and discussed between employees and managers (e.g., start of meetings, stand-alone presentations etc.).

Safety and cybersecurity actions were often contrasted, with the lack of similar reporting and challenge cybersecurity cultures being partly attributed to the different risk perceptions between unsafe and insecure practices. Whereas unsafe

actions can have a physical and immediate impact to an individual, an insecure action will not necessarily have a physical or immediate impact on the individual or the operational process. Moreover, the weak understanding of the effects of cybersecurity on OT, combined with the lack of incidents in operational environments leads to actions not being perceived as insecure or challenged. While cybersecurity awareness training attempts were often mentioned, they were not at the level of detail and frequency as the aforementioned safety practices.

> "I would say that there's a perception by the people that work on the plant that cyber security isn't a problem. Umm, because nothing's ever happened before. We used to hear that all the time on the safety side of things. So I was involved in investigating explosives' accidents. People killed, massive damage all around and they say, 'Well, it never happened before'. Well, it's gonna happen at some point." P_36, Cybersecurity Training Professional, Various sectors

Aside from individual behaviours, the permeation of safety in OT environments is evident in the development of safety management systems, and the creation of functions responsible for safety with safety-specialised engineers. Participants who had lived through the safety culture development would recognise the need for cybersecurity to be embedded into organisational practices in a similar manner. More importantly, safety practices have evolved beyond challenging and reporting unsafe actions, to a proactive approach with direct management support, where OT personnel are encouraged to stop tasks they deem unsafe without repercussions, which further highlights the organisational emphasis on safety.

> "We had the culture of everyone has the right to stop a job if they see or feel that it's unsafe, that there's something unsafe going on. If I am the control and instrumentation engineer and I see all the racks that I don't touch, but they're open, I have the right to question that. If I see someone who's putting their hand into those right, I have the right to go and stop them and ask for a permit to work. Like, do you have the right to be here? What are you doing? Who are you? That is part of the safety culture." P_12, OT Cybersecurity Consultant, Various sectors

4.2 Operational Realities

Aside from the prioritisation of process availability, production, and the organisational commitment to safety, OT personnel's mindsets have also been affected by the technological change in OT systems. Over the years, OT systems have been through a process of digitalisation, increased connectivity and automation. By automating, companies aimed to improve their production, profits, as well as safeguard against human error. Nevertheless, this has also led to a decrease in workforce sizes and the loss of tacit experience, and simultaneously increased the tasks and responsibilities of remaining OT personnel. Participants would describe the strain placed in OT personnel using metaphors such as "putting out fires", "busy keeping the lights on" etc. Accordingly, this strain hampers cybersecurity progress as OT personnel do not have the capacity to deal with cybersecurity issues, or prioritise learning about cybersecurity.

> "Maybe they're working one job and they're not qualified to do it, or experienced. Therefore, they're just about swimming. They're just about staying on top of their workload, and because cybersecurity hasn't ever organically been part of their role, it's in my opinion still fairly new, adding that onto their plate is just another thing for them to do." P_20, OT Cybersecurity Consultant, Various sectors

Alongside the shift towards automation, OT's increasing digitalisation and connectivity have also affected operational realities. Companies benefit from digitalisation and connectivity through improvements in maintenance, data sharing, and safety, as potentially unsafe actions can be conducted remotely without personnel being physically present. However, this has led to an increased attack surface, as various external actors have become connected to OT systems, including joint

operators of large infrastructures (e.g., oil fields) and supply chain partners, who require various data for operational, monitoring, and maintenance purposes. The proliferation of outsourced cybersecurity services, including Security Operations Centres (SoCs), implies that security companies also have a degree of access to these systems.

Participants reflected on technological changes where cybersecurity was neglected, leading to the design and deployment of OT systems without cybersecurity measures in place. This lack of prioritisation was partly caused by the historical isolation of operational environments, which had less "exposure to the rest of the world of IT and the problems that come with it" P_43, CISO, Water. Moreover, OT was commonly run on a project basis, where processes were designed, implemented, and maintained without many updates, compared to the "evergreen", continuously updated basis typical in IT. As such, OT practitioners have for years been used to insecure organisational practices and technical systems, and only recently there's been an increasing realisation of the scale of the cybersecurity challenge.

> "You just find, almost no matter where you look, the things that you would presume to be fixed in an IT environment, just are never done in an OT environment, and to a certain extent deliberately, right? The primary reason that a lot of those pieces of equipment were installed is that they react in real time, they're very fast. And therefore the overheads of additional layers of security and checks, they slow it down and you don't want that. And for a lot of them, for a long time the best measure of your automation equipment was how quickly does it respond. And so I think a lot of corners were cut for the sake of that. And unfortunately, like the hangover is now, we're in a pretty dire situation." P_90, OT Cybersecurity Product & Services Provider, Various sectors

Aside from technological change, OT environments' cybersecurity readiness is affected by other factors, including companies' size and operating models. For example, there are tens of thousands water utilities in the US, compared to about 25 in the UK, where the sector is more consolidated, with the US electricity sector also being similarly structured. Accordingly, many US companies are small and regional with only a few technical personnel, and their size hinders the development of OT cybersecurity capabilities (P_1)[1]. Cybersecurity perceptions are also affected by the availability of information in operational environments. While such information is becoming increasingly available from various external actors (e.g., security companies, communities of interest etc.), companies might not have the necessary structures or technology that facilitate communication and visibility between security and IT departments and OT environments.

> "Very recently I gave a presentation about cyber threats. At the end of the presentation, there was about 200 people in the room, I asked [them] to put their hands up if this was all a surprise to them. And about half the room put their hands [up]. From a very rough estimate, around about x% of engineering are completely unaware of the threats from hacktivists, from cyber criminals, and especially from APTs and their potential impact. This week, the NCSC and CISA put out a guidance around making sure that your systems are not connected directly to the Internet and default passwords. Well, it falls on deaf ears when it comes to the engineering world." P_49, OT Cybersecurity Consultant, Various sectors

4.3 Occupational and Professional Development

OT personnel's occupational and professional development pathways also affect their mindset and behaviours. Despite the variety of roles present in OT (e.g. operators, technicians, engineers), some common factors influence OT personnel's relationship with cybersecurity. One typical career entry route for OT practitioners is through vocational studies (e.g., apprenticeships), especially in operator or technician roles. Engineering roles on the other hand require a degree in their

[1] Conversation topic in an industry OT cybersecurity event where the author was present in the United States, August 2024.

respective engineering field along with professional accreditation. Nevertheless, neither of these educational pathways has typically included cybersecurity training. Similarly, cybersecurity was not placed at the same level of significance as process availability or safety in OT personnel's working career.

> "We have to increase people's knowledge through education and ongoing training. In engineering, I think universities are very guilty of not doing this. I'm actually trying to change the situation with academia [as] there's not enough training going on in engineering courses around OT security. Any controlled and instrumentation course, any engineering course should have cyber in it. We have to change people's understanding and we have to change their training and education." P_49, OT Cybersecurity Consultant, Various sectors

It is common for OT practitioners to have extensive working experience in the same, or similar operational environments, with this stability and tacit experience strongly shaping their working practices and habits, and reinforcing misperceptions around these environments' cybersecurity. Additionally, the hierarchical structures within OT environments often lead to OT practitioners advancing to senior roles, including senior process engineers who oversee and design operational processes, and asset owners that are ultimately accountable for specific assets, plants, or facilities. Over the past years, such roles have had to take on additional cybersecurity responsibilities. Given the lack of cybersecurity input during their careers, this can lead to these senior stakeholders becoming a bottleneck for cybersecurity adoption, by accepting high cybersecurity risks, or diminishing the importance of cybersecurity measures. On the other hand, such individuals are crucial for providing top down support for OT cybersecurity.

In terms of OT career trajectories, cybersecurity is a recent development with high market demand, and there has been a shift of practitioners specialising in OT cybersecurity (e.g., upskilling, qualifications, job experience, tertiary education etc.). Companies have focused on upskilling engineers, such as those with control and instrumentation roles, to becoming OT cybersecurity specialists. External companies (e.g., consultancies, service providers) often hire such experts from companies operating OT, leading to a consolidation of such expertise outside OT companies. In turn, this can affect OT companies' cybersecurity capabilities, by depriving them of valuable expertise. This was exemplified by P_68, who had taken up the responsibilities of a colleague who moved to the consulting sector. Given the demand for such skillsets, OT companies might find it challenging to compete with external actors in hiring or retaining such personnel, thus further affecting their OT capabilities in the longer term.

4.4 Perceptions of IT and Cybersecurity

Despite the technological changes and their effect on OT systems connectivity and automation, some cybersecurity misperceptions have persisted to a degree in operational environments. We have identified three such cybersecurity 'myths' based on technological assumptions, namely OT systems' connectivity, obscurity, and viability as potential targets. Additionally, our results highlight that the differences and perceived stereotypes of the working and cybersecurity practices between IT and OT practitioners also influence OT personnel's cybersecurity perceptions.

4.4.1 Technological Misperceptions

The first OT cybersecurity myth centres around OT systems' connectivity. For years, many OTs systems were "air-gapped" (i.e., disconnected from the internet), and in turn, more secure. Currently, few systems remain air-gapped, such as ones operating critical infrastructure in sectors like nuclear, which are deliberately kept so. Increased digitalisation and connectivity have altered these systems' cybersecurity risk (e.g., supply chain demands, remote work demands due to COVID-19). Human actions can also affect OT systems' connectivity, including the use of removable media, or

maintenance laptops by employees and third party contractors. Nevertheless, the effects of increased connectivity have often not been fully anticipated or accounted for, and misperceptions have persisted due to the lack of visibility into OT.

Secondly, the often proprietary nature and age of OT systems have contributed to their obscurity, and have accordingly led to misperceptions around their cybersecurity. Despite many OT systems not being designed and integrated with cybersecurity in mind, OT practitioners can perceive such obscurity to be providing greater security. Nevertheless, OT's increased digitalisation paired with the market consolidation of supply chains stakeholders (OEMs, integrators etc.) challenge the notion of 'security-by-obscurity', as more of these systems utilise commercially available software and hardware, and are designed, supplied, and integrated by a smaller pool of supply chain stakeholders. Moreover, the increased number of OT vulnerability disclosures and incidents further weakens this notion, as ultimately a system's obscurity is not an adequate deterrent for an attacker with the requisite skills and motivation.

The third identified cybersecurity misperception centres around a 'why would they attack us?' mentality, i.e., a company's viability as a potential cyberattack target. Such beliefs can be influenced by companies' size and criticality of operations. Even in critical infrastructure, we believe that perceptions of 'irrelevancy' are stronger in sectors like water or transport, compared to energy or nuclear. Moreover, the size, profitability, and importance of operational assets can affect these perceptions. As such, similar notions of irrelevancy can exist in smaller, less critical OT facilities or companies (e.g., smaller manufacturing facilities, a decommissioning oil platform etc.).

> "We can say this is happening in other critical national, other CNI industries, but then they go, 'Yes, but we are the railway, we are not a nuclear power plant'." P_9, OT Cybersecurity Consultant, Rail Sector

These misperceptions demonstrate that OT personnel may often lack well-formed mental models on cybersecurity's effects on operational environments. Many participants would highlight the challenge of integrating cybersecurity in OT mindsets and working practices, such as getting practitioners to consider the possibility that equipment's malfunction or process disruption could be caused by cyber means. Given the lack of visibility as well of cybersecurity experience in many OT environments, cybersecurity incidents can presumably remain undetected. Malfunctioning equipment may be replaced before cybersecurity investigations can take place, and shortcuts might be taken during maintenance, given the need for uptime and process availability. Similarly, in the case of passwords, process availability and safety concerns may often lead personnel to share or note them down, despite the security risks of such behaviours.

> "That operator's often the first line of defence, or the first person to understand a malfunction, misfunction or a misaction on their control system. So they may see that 'Hey, my server is slowing down, or I can't do anything, or I've got a ransomware screen on my HMI. What do I do?' And so I think what's really valuable for that is an operator to think now. 'Ohh this could be security'. For a technician to think that 'Ohh my control system. This may not be [a case of] I need to go out and swap out a bunch of cards. This could be a security, you know, [a] time adversarial attack'. So those people normally communicate again very well. But it's were they are stumped oftentimes, is thinking about, it's that paradigm mind shift of this may be security and what do I do about it now. And a lot of times [they'll] pull up their operational procedures which tell them how to start up and shutdown the unit. But it says nothing about security" P_1, OT Cybersecurity Consultant, Various sectors

4.4.2 Stereotyping of Practices

Participants would also contrast between IT and OT practices in terms of complexity, timescales, impact, ease of implementation etc. Accordingly, these differences can lead to the stereotyping ("othering" P_57 OT Manager, Energy) of each function's practices, impeding OT cybersecurity progress. Namely, IT practices were considered as more dynamic

than OT practices, with this difference in dynamics partly caused by operational realities which dictate a longer lifecycle for equipment and updates than IT. Compared to practices like Microsoft's "Patch Tuesdays", updates in operational environments are less streamlined, as they involve a larger number of stakeholders such as OEMs and integrators, and require advanced planning to fit designated maintenance windows. Moreover, cybersecurity updates in critical OT may require a renewal of the safety assurance case, which is another cumbersome procedure often requiring regulatory approval. On the other hand, engineering practices are less dynamic and more calculated, with participants noting that engineers tend to be more averse to risk and change. Concerns around safety and availability do not allow for the trial and error approaches that many IT professionals are used to, and similarly, the need for caution and precision clashes with cybersecurity's dynamic nature.

> "[The] cultural clash between the IT and the engineering [is] you can't just turn up and start installing equipment. You can't just bring the system down for 10 minutes while we do this. And certainly, in certain critical national infrastructure, you are literally having to plan these things years in advance. So yeah, there is a big difference there. I [always] say engineers are generally conservative with a little c you know, things work. 'Something's working. Don't touch it'. Yeah, whereas IT always got that. 'Well, we can make this better. We can improve this. We can do this'." P_64, OT Cybersecurity Consultant, Various sectors

In addition to its dynamic nature, IT equipment was perceived to be more standardised and homogenised, which facilitates its security. This homogenisation is partly caused by IT's shorter lifecycle which allows for more frequent equipment refresh. On the other hand, OT equipment is much less homogenised due to the age of many systems which are often run past their operational due date, and the wider variety of technologies which have historically originated from a broader set of OEMs. Overall, the more homogenised and dynamic nature of IT leads to the belief that changes are less risky, with lower potential impact compared to OT changes. The complexity of operations and the variety of equipment in OT means that standardised 'security hygiene' practices require a more contextualised and localised approach, including risk assessments and the input of subject matter experts, rather than straightforward rollout of updates common in IT.

> "Culturally, from an engineering background, I'm working on this assumption that everything in IT is really straightforward and most IT people have no idea what they're doing. Why do I have that impression? So when I used to work in the plant, that SCADA system we talked about where my Windows NT box is on and it had a bunch of routers and a bunch of connectivity out. Our cabinets were like engineering cabinets, right? All of the cables were like nicely dressed in and labelled and all that stuff, right? It was neat. It was tidy and it was clearly done by engineers. Just across the way, there's an IT cabinet. You can't close the door in the cabinet because it's just so much cable like pouring and there's not a label on it anywhere. Nobody actually knows what anything is. There's no drawings, there's nothing. Because IT people are complete amateurs, says the engineer." P_15, Senior Automation Manager, Oil & Gas sector

Additionally, security practices are less prescriptive compared to other practices operational personnel are familiar with, such as safety protocols or physical security measures. In OT processes, adherence to specific setpoints or boundaries is crucial to produce an acceptable physical product, like in water treatment, oil refinement etc. In some areas, such as physical security, practices and even mitigations are often recommended by competent authorities. Similarly, despite their intertwined nature, differences between safety and security practices can hamper OT cybersecurity progress. For example, risk assessment practices in safety are quantitative and well-established, whereas OT cybersecurity risk is typically assessed qualitatively and assessment practices are less mature. Despite recognising that security risk assessment would remain

qualitative, some participants felt that collaboration with their safety counterparts was hampered by these different logics, and the perception that security risk assessment is less mature and systematic. Accordingly, a better understanding of each side's methods and practices, increased willingness for collaboration, and the gradual maturity of OT cybersecurity risk assessments can enable better practices at the intersection of safety and security.

4.5 Security Practitioners' efforts

Overall, changing operational personnel's beliefs and practices is a challenge, especially as those have remained relatively consistent and unchallenged over the years. However, participants' reflections on their efforts indicated a spectrum of acceptance and pushback from OT personnel. Security is often initially perceived as an external value imposed to operational realities, rather than being recognised as an essential part of maintaining operational availability. This leads to OT personnel becoming defensive and pushing back on cybersecurity, or even apprehensive, feeling that they are called out by security practitioners for doing things wrong. The lack of previous interactions or relationships between enterprise and industrial assets can also lead to defensiveness, as in some cases security practitioners and especially external ones (e.g., consultants, auditors), can be perceived to be intruding in OT environments. At one end of the pushback spectrum, some participants expressed the belief that not every OT practitioner will buy-in to cybersecurity, such as personnel with extensive career experience who were "cruising towards retirement" (P_4, OT Cybersecurity Consultant, Manufacturing). At the opposite extreme, the role of OT personnel who are "IT hobbyists" (e.g., having an interest in networking) was recognised. Such individuals have the potential to influence their coworkers beliefs acting as security champions, and may even be upskilled with OT cybersecurity skills.

Conversations would commonly centre on the need to achieve a balance between cybersecurity and OT personnel's needs and ways of working, without security impeding process availability. For example, P_43 reflected on a decision to not implement a security control as it would ultimately provide minimal value, given that the outcome it was trying to prevent could have been achieved through other means. However, in many cases, security measures had to be implement despite the pushback, such as stricter access control, not allowing the downloading of software through the internet, or limiting the use of removable media. The importance of soft skills and ability to develop relationships with OT personnel were often cited as important for achieving buy-in for cybersecurity in OT environments. Many participants with OT backgrounds (e.g., engineers, integrators etc.), felt that it eased their interactions with OT personnel, as they were familiar with their language, culture, and working practices. More importantly, the value of being able to listen to the other side's concerns, and being reasonable with security proposals was commonly touched upon.

> "To paraphrase X, 'We've got two ears and one mouth, and you should probably use them in that ratio'. You got to listen to what people are telling you, because I understand the processes to a degree, but each platform in the oil and gas space will operate in a slightly different way. So you got to listen to what they're telling you, and then work out what the business needs" P_66, OT Cybersecurity Consultant, Various sectors

5 DISCUSSION

Our results demonstrated a number of factors that affect OT personnels' mindsets, and in turn, cybersecurity beliefs and behaviours, as experienced by OT cybersecurity professionals. These include the prioritisation of operational needs like process availability and safety, and the operationsal challenges brought by technological change. We also touched on the effect of OT personnels' occupational pathways and practices. Accordingly, we distinguished between two closely intertwined misperception areas around OT cybersecurity: technological misperceptions based on systems' connectivity, obscurity, and attractiveness as a cyber-attack target, and the stereotyping of the occupational practices between the IT and

engineering worlds. We then described security practitioners attempts' to influence OT personnel's cybersecurity beliefs, demonstrating the pushback they often encounter.

With respect to operational needs and values, cybersecurity is not at the same pedestal as process availability or safety. Safety wasn't always as valued in these environments and safety culture development efforts over the past decades were instrumental in shifting perceptions in companies using OT [90]. While research has demonstrated how organisational support for safety does not necessarily lead to safe actions, especially when safety clashes with values like production [91], the permeation of safety thinking in OT environments is undeniable. In turn, the relatively lower maturity of cybersecurity initiatives (e.g., management support, open, reporting, and challenging cultures etc.) hinders cybersecurity from rising to comparable levels to safety. Cybersecurity measures can often be perceived as additional hurdles to OT personnel's workload (e.g., loss of admin rights, access controls hindering workload). More importantly, cybersecurity is typically perceived as a potential disruptor of operations, leading to push back, similar to tensions described elsewhere [28, 48].

OT environments have gone through considerable technological change over the past decades, through increased digitalisation, automation, and connectivity. The lack of pressures (e.g., regulation, incidents) allowed many OT stakeholders (e.g., OT companies, vendors etc.) to conveniently ignore cybersecurity. Combined with the fact that OT consists of legacy technology which is infrequently updated, and where the need for process availability can lead to quick fixes, such systems have accumulated significant 'technical debt' [92]. Unfortunately, the effects of this change on cybersecurity were only picked up late in this process, with the accumulated 'technical debt' hindering cybersecurity. The reduction of personnel numbers in these environments, and by extension, weakened capabilities for cybersecurity learning, was another outcome of technological change. Research has demonstrated the negative effects of higher automation levels on operators' situational awareness and manual skills [93]. Overall, weakened situational awareness and the lack of personnel can also affect cybersecurity (e.g. during incident response, as operators are OT systems' first line of defence).

Accordingly, we have described three cybersecurity misperceptions around OT systems' connectivity, obscurity, and attractiveness as a target. Reason's influential research into human errors and safety has argued that incidents are a combination of active failures (slips, procedural violations etc.), and latent conditions (stemming from decisions made by system designers and management) [94]. The combination of cybersecurity misperceptions around OT systems' controllability or boundaries, and latent conditions (e.g. the insecurity and legacy of OT equipment), has been shown to cause past OT cybersecurity incidents [95]. More broadly, research has demonstrated how factors like knowledge, experience, threat and response evaluation affect users' security behaviours [18]. Our security participants with first-hand experiences in OT environments have often highlighted how such factors are often weak or non-existent. As such, the three misperceptions we've identified and the broader lack of cybersecurity thinking in OT can in combination with latent conditions lead to cybersecurity incidents.

Nevertheless, notable progress has been made in changing these misperceptions. The increased use of commonly available IT equipment in operational environments, OT system's enhanced connectivity, and enhanced visibility aided by advancements in areas like asset management and anomaly detection have contributed to weakening misperceptions around connectivity and obscurity. The misperceptions around these systems attractiveness can be more difficult to alleviate, with participants describing the existence of similar perceptions at higher organisational levels. However, past attacks have demonstrated that OT systems can be affected even if not directly targeted (e.g., ransomware, attacks in the enterprise domain impacting OT) [96]. Moreover, techniques like 'living off the land' are a reality for such companies [6]. As such, misperceptions around OT companies and systems attractiveness need to be effectively targeted at all organisational levels.

OT personnel's mindsets are also shaped through their occupational development. Despite the variety of entry points for OT careers, there is an overall lack of cybersecurity input in most of them (e.g., awareness, training). Currently, only a

few OT cybersecurity academic qualifications exist at either the engineering, or cybersecurity sides [100, 101]. Moreover, OT practitioners typically have extended careers in similar operational environments. Paired with the fact that learning in such environments happens through less formal methods (e.g., on-the-job training, co-worker training) [69], perceptions around acceptable working beliefs and practices are solidified over time, which has augmented opposition to cybersecurity.

The hierarchical structure in OT environments also affects cybersecurity. Senior management leadership, support, and involvement are widely regarded as the most important factors in developing a security culture [99]. However, such positions might currently be filled by people who have had minimal cybersecurity input throughout their careers, thus hindering cybersecurity adoption. Research has also demonstrated governance barriers in companies over the distribution of OT cybersecurity responsibilities [10], another area where such practitioners' involvement can be instrumental. The demand for OT cybersecurity expertise has led many practitioners moving to external roles (e.g., consultancies), negatively affecting organisational cybersecurity capabilities. Similar issues around the consulting industry's negative effects on businesses' and governments' capabilities have been described in other areas (e.g., management consulting [100]). Nevertheless, research has also demonstrated that external expertise can have a positive role in alleviating organisational OT cybersecurity barriers [10].

We have also demonstrated how differences between IT and OT practices lead to misperceptions and stereotypes. IT practices are generally more dynamic, aided by the more homogeneous equipment, whereas OT practices are engineering-based, thus being more calculative and prescriptive. Research has demonstrated differences between occupational security cultures (e.g. information security, accounting), as well as a relationship between professional identities, occupational beliefs, and security (e.g., rule compliance in accountants) [101]. Our results similarly demonstrate that OT personnel, while not being a singular profession, constitute a distinct security subculture, and that their security beliefs are affected by their general mindsets (e.g., engineering values).

Finally, we have demonstrated the varying levels of pushback (from denial to engage, to gradual acceptance, safety concerns etc.) that security practitioners face. Positively, many participants realised the importance of soft skills and strong relationships in facilitating effective collaboration and improving cybersecurity perceptions and practices. Some OT practitioners, especially ones with extensive experience nearing retirement, were perceived as a challenge by some participants, who expressed a belief that these practitioners may never buy-in into cybersecurity. Overall however, our participants' security practices demonstrated a more collaborative and risk-based approach compared to approaches where cybersecurity is effectively imposed on other functions by a single department. This collaborative approach is a necessity given the unique dynamic between IT and security and OT practitioners, which differs from other interactions between security practitioners and 'end-users'. Namely, while security practitioners are still perceived as the 'experts' when it comes to the technology used in their interactions with 'end-users' (e.g., an accounting department), their lack of experience and expertise in the OT world weakens their positions and necessitates more collaborative approaches.

5.1 Limitations and Avenues for Future Research

Our work has a number of limitations which offer avenues for future research. First, our participant sample consisted of practitioners with OT cybersecurity related roles, as our research investigated security culture development efforts in companies that use OT. While many participants had a background and extensive experience in OT roles (e.g., engineer, operators), future research should be conducted directly with OT practitioners.

A second related limitation is that our findings were aggregated at the OT level. We posit that our findings are valid across OT roles, but some differences can affect the strength of each identified factor. Engineers with design responsibilities can be compared to software developers, whereas operator roles are more closely related to 'end-users', and technicians

sit in-between these two roles. Tensions can arise between functions that design OT systems, and the ones operating them. For example, the lack of cybersecurity mechanisms designed into OT systems will influence operators' cybersecurity perceptions. On the other hand, it is typical for specific engineering roles (e.g., control and instrumentation) to be handed cybersecurity responsibilities, with companies firstly aiming to upskill such roles. This can lead to a situation where companies may not target other OT roles as effectively. Given the diversity of roles in OT and the challenge of identifying those with a strong cybersecurity mindset, we suggest that seniority, interaction with digitalized technology, and process or equipment design responsibilities are key indicators of OT practitioners' cybersecurity mindset. Overall, the different roles in operational environments have rarely been studied in-depth, aside from [102] where differences in cybersecurity perceptions between operators and maintenance staff in OT environments were identified. Further research could look into potential differences in OT cybersecurity perceptions between different OT personnel roles.

Finally, the majority of our participants are based in the UK. Some participants were active in other geographical areas due to their roles (e.g., consultants, vendors), predominantly in Western Europe and the United States. We believe that our findings hold some external validity across different geographical areas. Nevertheless, differences can arise due to different institutional factors (e.g., OT cybersecurity regulation). Given that OT personnel's occupational pathways affect cybersecurity perceptions, differences in vocational studies and certification mechanisms might also have an effect. Finally, we've described the technological shift in OT and its effects on cybersecurity. Nevertheless, this technological shift varies between companies and sectors. Sectors like nuclear might be on the conservative side of such technological shifts, whereas oil and gas companies have more openly embraced technological advancements. As such, future research could look into cybersecurity perception differences, based on a company's degree of technological adoption, existence of regulation etc.

6 CONCLUSIONS

OT cybersecurity is an area which has only received considerable attention in the recent past. Currently, many companies are in the process of improving their OT cybersecurity. Nevertheless, there is little research into OT personnel's interactions with cybersecurity. Our analysis of 72 interviews with OT security practitioners demonstrated the effects of operational values such as process safety and availability, technological advancements, and OT personnel's occupational pathways on OT mindsets. Accordingly, we've identified how these mindsets give rise to cybersecurity misperceptions into two broad categories. Firstly, advancements in technology have shifted operational realities, by reducing workforce numbers and increasing their security risk. In turn, misperceptions around these systems' connectivity, obscurity, and attractiveness as a target arise. The other broad category of misperceptions is centred around the occupational practices of IT and OT personnel. Finally, our results demonstrate the pushback OT security practitioners receive, as well as the importance of soft skills and strong relationships with OT personnel in achieving their buy-in.

Overall, our work contributes to the scarce research into OT personnel's cybersecurity interactions by identifying factors that affect OT personnel's mindsets and subsequently their cybersecurity perceptions, through the experiences of OT cybersecurity practitioners. By acknowledging this work's limitations, we've raised some avenues future research. We conclude with recommendations for OT companies:

1. Finding effective means to demonstrate cybersecurity's effect into OT processes. Disastrous industrial accidents and common safety incidents (e.g., falls) affect OT personnel's safety risk thinking. Given the limited amount of similar cybersecurity incidents, companies must find ways to demonstrate the risk and impact of cybersecurity into operational environments, including simulations, cyber-ranges, and table-top exercises.

2. Companies and other stakeholders such as original equipment manufacturers (OEMs), professional bodies etc., should push for increased cybersecurity education in tertiary and vocational studies. Similarly, if apprenticeships are the common entry point for some roles, companies should provide similar education and training at the induction stages.
3. Companies should focus on including cybersecurity into OT personnel's mindsets and working practices. While our results demonstrate considerable and successful efforts into upskilling key engineers into OT cybersecurity, the effects of other OT awareness and training efforts are less clear.

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 three anonymous reviewers whose insightful comments and suggestions have improved this work.

REFERENCES

[1] Gartner, "Definition of Operational Technology (OT) - Gartner Information Technology Glossary," Gartner. Accessed: May 17, 2024. [Online]. Available: https://www.gartner.com/en/information-technology/glossary/operational-technology-ot

[2] National Protective Security Authority, "Critical National Infrastructure | NPSA." Accessed: May 17, 2024. [Online]. Available: https://www.npsa.gov.uk/critical-national-infrastructure-0

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

[4] M. Lezzi, M. Lazoi, and A. Corallo, "Cybersecurity for Industry 4.0 in the current literature: A reference framework," *Computers in Industry*, vol. 103, pp. 97–110, Dec. 2018, doi: 10.1016/j.compind.2018.09.004.

[5] National Cyber Security Centre, "NCSC warns of emerging threat to critical national infrastructure." Accessed: May 17, 2024. [Online]. Available: https://www.ncsc.gov.uk/news/ncsc-warns-of-emerging-threat-to-critical-national-infrastructure

[6] Cybersecruity & Infrastructure National Agency, "Identifying and Mitigating Living Off the Land Techniques | CISA." Accessed: May 23, 2024. [Online]. Available: https://www.cisa.gov/resources-tools/resources/identifying-and-mitigating-living-land-techniques

[7] UK Government, "The NIS Regulations 2018," GOV.UK. Accessed: May 17, 2024. [Online]. Available: https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018

[8] Cybersecruity & Infrastructure National Agency, "National Security Memorandum on Critical Infrastructure Security and Resilience | CISA." Accessed: May 17, 2024. [Online]. Available: https://www.cisa.gov/national-security-memorandum-critical-infrastructure-security-and-resilience

[9] International Society of Automation, "ISA/IEC 62443 Series of Standards - ISA," isa.org. Accessed: May 17, 2024. [Online]. Available: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

[10] S. Evripidou, U. D. Ani, S. Hailes, and J. D. M. Watson, "Exploring the Security Culture of Operational Technology (OT) Organisations: the Role of External Consultancy in Overcoming Organisational Barriers," presented at the Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023), 2023, pp. 113–129. Accessed: Jan. 25, 2024. [Online]. Available: https://www.usenix.org/conference/soups2023/presentation/evripidou

[11] 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.

[12] 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.

[13] I. Abele-Wigert, "Challenges Governments Face in the Field of Critical Information Infrastructure Protection (CIIP): Stakeholders and Perspectives," 2006.

[14] D. Assaf, "Government Intervention in Information Infrastructure Protection," in *Critical Infrastructure Protection*, E. Goetz and S. Shenoi, Eds., in IFIP International Federation for Information Processing. Boston, MA: Springer US, 2008, pp. 29–39. doi: 10.1007/978-0-387-75462-8_3.

[15] 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.

[16] 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. 20539517221108369, Jan. 2022, doi: 10.1177/20539517221108369.

[17] A. Adams and M. A. Sasse, "Users are not the enemy," *Commun. ACM*, vol. 42, no. 12, pp. 40–46, Dec. 1999, doi: 10.1145/322796.322806.

[18] J. M. Blythe, L. Coventry, and L. Little, "Unpacking security policy compliance: the motivators and barriers of employees' security behaviors," in *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security*, in SOUPS '15. USA: USENIX Association, Jul. 2015, pp. 103–122.

[19] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)," *Computers & Security*, vol. 42, pp. 165–176, May 2014, doi: 10.1016/j.cose.2013.12.003.

[20] A. Beautement, I. Becker, S. Parkin, K. Krol, and A. Sasse, "Productive Security: A Scalable Methodology for Analysing Employee Security Behaviours," presented at the Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016), 2016, pp. 253–270. [Online]. Available: https://www.usenix.org/conference/soups2016/technical-sessions/presentation/beautement

[21] F. Karlsson, M. Karlsson, and J. Åström, "Measuring employees' compliance – the importance of value pluralism," *Information & Computer Security*, vol. 25, no. 3, pp. 279–299, Jan. 2017, doi: 10.1108/ICS-11-2016-0084.

[22] A. Mokhberi and K. Beznosov, "SoK: Human, Organizational, and Technological Dimensions of Developers' Challenges in Engineering Secure Software," in *Proceedings of the 2021 European Symposium on Usable Security*, in EuroUSEC '21. New York, NY, USA: Association for Computing Machinery, Dec. 2021, pp. 59–75. doi: 10.1145/3481357.3481522.

[23] S. Evripidou, U. D. Ani, S. Hailes, and J. D. McK. Watson, "Drawing on the Success of Developing a Safety Culture to Improve the Security Culture in Companies That Use Operational Technology," in *Proceeding of the 33rd European Safety and Reliability Conference*, Research Publishing Services, 2023, pp. 3455–3462. doi: 10.3850/978-981-18-8071-1_P297-cd.

[24] 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.

[25] M. A. Sasse, S. Brostoff, and D. Weirich, "Transforming the 'Weakest Link' — a Human/Computer Interaction Approach to Usable and Effective Security," *BT Technology Journal*, vol. 19, no. 3, pp. 122–131, Jul. 2001, doi: 10.1023/A:1011902718709.

[26] S. Brostoff and M. A. Sasse, "Safe and sound: a safety-critical approach to security," in *Proceedings of the 2001 workshop on New security paradigms*, in NSPW '01. New York, NY, USA: Association for Computing Machinery, Sep. 2001, pp. 41–50. doi: 10.1145/508171.508178.

[27] A. Whitten and J. D. Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of {PGP} 5.0," presented at the 8th {USENIX} Security Symposium ({USENIX} Security 99), 1999. Accessed: Aug. 01, 2021. [Online]. Available: https://www.usenix.org/conference/8th-usenix-security-symposium/why-johnny-cant-encrypt-usability-evaluation-pgp-50

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

[29] 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," Aug. 04, 2022, *arXiv*: arXiv:2208.02500. Accessed: Oct. 02, 2022. [Online]. Available: http://arxiv.org/abs/2208.02500

[30] K. Li, A. Rashid, and A. Roudaut, "Usable Security Model for Industrial Control Systems - Authentication and Authorisation Workflow," in *Proceedings of the 2023 European Symposium on Usable Security*, in EuroUSEC '23. New York, NY, USA: Association for Computing Machinery, Oct. 2023, pp. 205–217. doi: 10.1145/3617072.3617114.

[31] F. Carroll, "Usable Security and Aesthetics: Designing for engaging online security warnings and cautions to optimise user security whilst affording ease of use," in *Proceedings of the 2021 European Symposium on Usable Security*, in EuroUSEC '21. New York, NY, USA: Association for Computing Machinery, Dec. 2021, pp. 23–28. doi: 10.1145/3481357.3481376.

[32] J. Hielscher, A. Kluge, U. Menges, and M. A. Sasse, "'Taking out the Trash': Why Security Behavior Change requires Intentional Forgetting," in *Proceedings of the 2021 New Security Paradigms Workshop*, in NSPW '21. New York, NY, USA: Association for Computing Machinery, Dec. 2022, pp. 108–122. doi: 10.1145/3498891.3498902.

[33] E. Kim, J. Yoon, J. Kwon, T. Liaw, and A. M. Agogino, "From Innocent Irene to Parental Patrick: Framing User Characteristics and Personas to Design for Cybersecurity," *Proceedings of the Design Society: International Conference on Engineering Design*, vol. 1, no. 1, pp. 1773–1782, Jul. 2019, doi: 10.1017/dsi.2019.183.

[34] B. A. Morrison, J. Nicholson, L. Coventry, and P. Briggs, "Recognising Diversity in Older Adults' Cybersecurity Needs," in *Proceedings of the 2023 ACM Conference on Information Technology for Social Good*, in GoodIT '23. New York, NY, USA: Association for Computing Machinery, Sep. 2023, pp. 437–445. doi: 10.1145/3582515.3609565.

[35] M. Lee *et al.*, "Developing personas & use cases with user survey data: A study on the millennials' media usage," *Journal of Retailing and Consumer Services*, vol. 54, p. 102051, May 2020, doi: 10.1016/j.jretconser.2020.102051.

[36] S. Faily, "Barry is not the weakest link: Eliciting Secure System Requirements with Personas," presented at the Proceedings of HCI 2010, BCS Learning & Development, Sep. 2010. doi: 10.14236/ewic/HCI2010.17.

[37] M. Dark, "Thinking about Cybersecurity," *IEEE Security & Privacy*, vol. 13, no. 1, pp. 61–65, Jan. 2015, doi: 10.1109/MSP.2015.17.

[38] R. Kang, L. Dabbish, N. Fruchter, and S. Kiesler, "'My data just goes everywhere': user mental models of the internet and implications for privacy and security," in *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security*, in SOUPS '15. USA: USENIX Association, Jul. 2015, pp. 39–52.

[39] J. K. Doyle and D. N. Ford, "Mental models concepts for system dynamics research," *System Dynamics Review*, vol. 14, no. 1, pp. 3–29, 1998, doi: 10.1002/(SICI)1099-1727(199821)14:1<3::AID-SDR140>3.0.CO;2-K.

[40] I. Ion, R. Reeder, and S. Consolvo, "{'...No} one Can Hack My {Mind'}: Comparing Expert and {Non-Expert} Security Practices," presented at the Eleventh Symposium On Usable Privacy and Security (SOUPS 2015), 2015, pp. 327–346. Accessed: May 19, 2024. [Online]. Available: https://www.usenix.org/conference/soups2015/proceedings/presentation/ion

[41] S. McGregor and E. Watkins, *"Security by Obscurity": Journalists' Mental Models of Information Security.* 2016.

[42] J. Nicholson, J. Terry, H. Beckett, and P. Kumar, "Understanding Young People's Experiences of Cybersecurity," in *Proceedings of the 2021 European Symposium on Usable Security*, in EuroUSEC '21. New York, NY, USA: Association for Computing Machinery, Dec. 2021, pp. 200–210. doi: 10.1145/3481357.3481520.

[43] B. Breve, G. Desolda, F. Greco, and V. Deufemia, "Democratizing Cybersecurity in Smart Environments: Investigating the Mental Models of Novices and Experts," in *End-User Development*, L. D. Spano, A. Schmidt, C. Santoro, and S. Stumpf, Eds., Cham: Springer Nature Switzerland, 2023, pp. 145–161. doi: 10.1007/978-3-031-34433-6_9.

[44] L. Bieringer, K. Grosse, M. Backes, B. Biggio, and K. Krombholz, "Industrial practitioners' mental models of adversarial machine learning," presented at the Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022), 2022, pp. 97–116. Accessed: May 19, 2024. [Online]. Available: https://www.usenix.org/conference/soups2022/presentation/bieringer

[45] A. Mai, K. Pfeffer, M. Gusenbauer, E. Weippl, and K. Krombholz, "User mental models of cryptocurrency systems - a grounded theory approach," in *Proceedings of the Sixteenth USENIX Conference on Usable Privacy and Security*, in SOUPS'20. USA: USENIX Association, Aug. 2020, pp. 341–358.

[46] K. Schoenmakers, D. Greene, S. Stutterheim, H. Lin, and M. J. Palmer, "The security mindset: characteristics, development, and consequences," *Journal of Cybersecurity*, vol. 9, no. 1, p. tyad010, Jan. 2023, doi: 10.1093/cybsec/tyad010.

[47] W. Dutton, "Fostering a cyber security mindset," *Internet Policy Review*, vol. 6, Jan. 2017, doi: 10.14763/2017.1.443.

[48] J. Hielscher, M. Schöps, U. Menges, M. Gutfleisch, M. Helbling, and M. A. Sasse, "Lacking the Tools and Support to Fix Friction: Results from an Interview Study with Security Managers," presented at the Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023), 2023, pp. 131–150. Accessed: May 19, 2024. [Online]. Available: https://www.usenix.org/conference/soups2023/presentation/hielscher

[49] A. Beautement and A. Sasse, "The economics of user effort in information security," *Computer Fraud & Security*, vol. 2009, no. 10, pp. 8–12, Oct. 2009, doi: 10.1016/S1361-3723(09)70127-7.

[50] M. Gutfleisch, J. H. Klemmer, N. Busch, Y. Acar, M. A. Sasse, and S. Fahl, "How Does Usable Security (Not) End Up in Software Products? Results From a Qualitative Interview Study," in *2022 IEEE Symposium on Security and Privacy (SP)*, May 2022, pp. 893–910. doi: 10.1109/SP46214.2022.9833756.

[51] 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.

[52] D. Branley-Bell, L. Coventry, and P. Briggs, "Cyber Insurance from the stakeholder's perspective: A qualitative analysis of barriers and facilitators to adoption," in *Proceedings of the 2022 European Symposium on Usable Security*, in EuroUSEC '22. New York, NY, USA: Association for Computing Machinery, Sep. 2022, pp. 151–159. doi: 10.1145/3549015.3554206.

[53] Q. Hu, P. Hart, and D. Cooke, "The role of external and internal influences on information systems security – a neo-institutional perspective," *The Journal of Strategic Information Systems*, vol. 16, no. 2, pp. 153–172, Jun. 2007, doi: 10.1016/j.jsis.2007.05.004.

[54] 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.

[55] J. Hielscher, U. Menges, S. Parkin, A. Kluge, and M. A. Sasse, "{'Employees} Who {Don't} Accept the Time Security Takes Are Not Aware {Enough'}: The {CISO} View of {Human-Centred} Security," presented at the 32nd USENIX Security Symposium (USENIX Security 23), 2023, pp. 2311–2328. Accessed: Jul. 19, 2024. [Online]. Available: https://www.usenix.org/conference/usenixsecurity23/presentation/hielscher

[56] L. Reinfelder, R. Landwirth, and Z. Benenson, "Security Managers Are Not The Enemy Either," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, in CHI '19. New York, NY, USA: Association for Computing Machinery, May 2019, pp. 1–7. doi: 10.1145/3290605.3300663.

[57] E. Albrechtsen and J. Hovden, "The information security digital divide between information security managers and users," *Computers & Security*, vol. 28, no. 6, pp. 476–490, Sep. 2009, doi: 10.1016/j.cose.2009.01.003.

[58] D. Ashenden and D. Lawrence, "Security Dialogues: Building Better Relationships between Security and Business," *IEEE Secur. Privacy*, vol. 14, no. 3, pp. 82–87, May 2016, doi: 10.1109/MSP.2016.57.

[59] K. Hedström, E. Kolkowska, F. Karlsson, and J. P. Allen, "Value conflicts for information security management," *The Journal of Strategic Information Systems*, vol. 20, no. 4, pp. 373–384, Dec. 2011, doi: 10.1016/j.jsis.2011.06.001.

[60] 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

[61] T. Wallis and C. Johnson, "Implementing the NIS Directive, driving cybersecurity improvements for Essential Services," in *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, Jun. 2020, pp. 1–10. doi: 10.1109/CyberSA49311.2020.9139641.

[62] T. Wallis, C. Johnson, and M. Khamis, "Tania Wallis, Chris Johnson, and Mohamed Khamis, Interorganizational Cooperation in Supply Chain Cybersecurity: A Cross-Industry Study of the Effectiveness of the UK Implementation of the NIS Directive," *Information & Security: An International Journal*, vol. 48, Jan. 2021, doi: 10.11610/isij.4812.

[63] European Union Agency for Cybersecurity, "NIS Directive," ENISA. Accessed: Jan. 25, 2024. [Online]. Available: https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new

[64] S. M. McBride, C. D. Schou, and J. Slay, "A Security Workforce to Bridge the IT-OT Gap".

[65] N. Gross, "Control and Automation Engineering Education Programs: Challenges and Opportunities - News." Accessed: May 17, 2024. [Online]. Available: https://control.com/news/the-landscape-of-engineering-education-challenges-and-opportunities/

[66] R. Müller and L. Oehm, "Process industries versus discrete processing: how system characteristics affect operator tasks," *Cogn Tech Work*, vol. 21, no. 2, pp. 337–356, May 2019, doi: 10.1007/s10111-018-0511-1.

[67] E. S. Madsen, A. Bilberg, and D. Grube Hansen, "Industry 4.0 and digitalization call for vocational skills, applied industrial engineering, and less for pure academics: 5th World Conference on Production and Operations Management," *Proceedings of the 5th P&OM World Confernece*, 2016.

[68] J. Schmidt and R. Müller, "Discipline differences in mental models: How mechanical engineers and automation engineers evaluate machine processes," *Human Factors and Ergonomics in Manufacturing & Service Industries*, vol. 33, no. 6, pp. 521–536, 2023, doi: 10.1002/hfm.21005.

[69] "A Guide to the Automation Body of Knowledge, Third Edition," automation.com. Accessed: May 23, 2024. [Online]. Available: https://www.automation.com/en-us/products/featured-products-2020/a-comprehensive-overview-of-automation

[70] I. Ngambeki, S. McBride, and J. Slay, "Knowledge Gaps in Curricular Guidance for ICS Security," *Journal of The Colloquium for Information Systems Security Education*, vol. 9, p. 6, Mar. 2022, doi: 10.53735/cisse.v9i1.149.

[71] B. Hamdan and R. A. Nsour, "Curriculum Development for Teaching Cybersecurity of Industrial Control Systems & Critical Infrastructure," in *2022 Intermountain Engineering, Technology and Computing (IETC)*, May 2022, pp. 1–5. doi: 10.1109/IETC54973.2022.9796664.

[72] K. McLaughlin, "Mastering the Interplay: The Role and Culture of a Cyber Physical Security (cps) Professional in Global Cybersecurity Teams," *EDPACS*, vol. 68, no. 4, pp. 38–45, Oct. 2023, doi: 10.1080/07366981.2023.2216992.

[73] J. M. Takács and M. Pogatsnik, "A systematic review of Human Aspects in Industry 4.0 and 5.0: Cybersecurity Awareness and Soft Skills," in *2023 IEEE 27th International Conference on Intelligent Engineering Systems (INES)*, Jul. 2023, pp. 000033–000040. doi: 10.1109/INES59282.2023.10297768.

[74] Industrial Society of Automation, "Cybersecurity Certificates - ISA," isa.org. Accessed: May 18, 2024. [Online]. Available: https://www.isa.org/certification/certificate-programs/isa-iec-62443-cybersecurity-certificate-program

[75] SANS Institute, "Industrial Control Systems (ICS) | SANS Institute." Accessed: May 18, 2024. [Online]. Available: https://www.sans.org/industrial-control-systems-security/

[76] 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

[77] S. McBride, S. McBride, C. Schou, and J. Slay, "An Initial Industrial Cybersecurity Workforce Development Framework".

[78] C. Ramezan, P. Coffy, and J. Lemons, “Building the Operational Technology (OT) Cybersecurity Workforce: What are Employers Looking for?,” *Journal of Cybersecurity Education, Research and Practice*, vol. 2024, no. 1, Oct. 2023, doi: 10.32727/8.2023.31.
[79] “A systematic review of Human Aspects in Industry 4.0 and 5.0: Cybersecurity Awareness and Soft Skills | IEEE Conference Publication | IEEE Xplore.” Accessed: May 23, 2024. [Online]. Available: https://ieeexplore.ieee.org/document/10297768
[80] S. McBride and J. Slay, “Criteria for International Industrial Cybersecurity Education and Training Standards”.
[81] A. Bryman, *Social Research Methods*. Oxford University Press, 2016.
[82] 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.
[83] V. Braun and V. Clarke, “Reflecting on reflexive thematic analysis,” *Qualitative Research in Sport, Exercise and Health*, Aug. 2019, Accessed: Dec. 18, 2023. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/2159676X.2019.1628806
[84] V. Braun and V. Clarke, “Toward good practice in thematic analysis: Avoiding common problems and be(com)ing a knowing researcher,” *International Journal of Transgender Health*, vol. 24, no. 1, pp. 1–6, Jan. 2023, doi: 10.1080/26895269.2022.2129597.
[85] V. Braun and V. Clarke, “One size fits all? What counts as quality practice in (reflexive) thematic analysis?,” *Qualitative Research in Psychology*, vol. 18, no. 3, pp. 328–352, Jul. 2021, doi: 10.1080/14780887.2020.1769238.
[86] D. Byrne, “A worked example of Braun and Clarke’s approach to reflexive thematic analysis,” *Qual Quant*, vol. 56, no. 3, pp. 1391–1412, Jun. 2022, doi: 10.1007/s11135-021-01182-y.
[87] L. R. Trainor and A. Bundon, “Developing the craft: reflexive accounts of doing reflexive thematic analysis,” *Qualitative Research in Sport, Exercise and Health*, vol. 13, no. 5, pp. 705–726, Sep. 2021, doi: 10.1080/2159676X.2020.1840423.
[88] V. Braun, V. Clarke, and N. Rance, “How to use thematic analysis with interview data,” *The Counselling and Psychotherapy Research Handbook*, p. 183, Jan. 2014.
[89] “mindset, n. meanings, etymology and more | Oxford English Dictionary.” Accessed: Jul. 21, 2024. [Online]. Available: https://www.oed.com/dictionary/mindset_n
[90] D. A. Hofmann, M. J. Burke, and D. Zohar, “100 years of occupational safety research: From basic protections and work analysis to a multilevel view of workplace safety and risk,” *Journal of Applied Psychology*, vol. 102, pp. 375–388, 2017, doi: 10.1037/apl0000114.
[91] D. Besnard and E. Hollnagel, “I want to believe: some myths about the management of industrial safety,” *Cogn Tech Work*, vol. 16, no. 1, pp. 13–23, Feb. 2014, doi: 10.1007/s10111-012-0237-4.
[92] Barr Adivsory and Hive Systems, “The Impact of Technical Debt on Cybersecurity.” Accessed: May 23, 2024. [Online]. Available: https://www.barradvisory.com/wp-content/uploads/2022/05/The-Impact-of-Technical-Debt-on-Cybersecurity.pdf
[93] L. Onnasch, C. D. Wickens, H. Li, and D. Manzey, “Human Performance Consequences of Stages and Levels of Automation: An Integrated Meta-Analysis,” *Hum Factors*, vol. 56, no. 3, pp. 476–488, May 2014, doi: 10.1177/0018720813501549.
[94] J. Reason, “Human error: models and management,” *BMJ*, vol. 320, no. 7237, pp. 768–770, Mar. 2000, doi: 10.1136/bmj.320.7237.768.
[95] S. Frey, A. Rashid, A. Zanutto, J. Busby, and K. Follis, “On the Role of Latent Design Conditions in Cyber-Physical Systems Security,” in *2016 IEEE/ACM 2nd International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS)*, May 2016, pp. 43–46. doi: 10.1109/SEsCPS.2016.015.
[96] R. Derbyshire, “Making Sense of Operational Technology Attacks: The Past, Present, and Future,” The Hacker News. Accessed: May 23, 2024. [Online]. Available: https://thehackernews.com/2024/03/making-sense-of-operational-technology.html
[97] Everett Community College, “Industrial Cybersecurity | Everett Community College.” Accessed: May 29, 2024. [Online]. Available: https://www.everettcc.edu/programs/bat/it-program/industrial-cybersecurity
[98] Idaho State University, “Industrial Cybersecurity Engineering Technology.” Accessed: May 29, 2024. [Online]. Available: https://www.isu.edu/industrialcybersecurity/
[99] 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.
[100] M. Mazzucato and R. Collington, *The big con: how the consulting industry weakens our businesses, infantilizes our governments, and warps our economies*. Penguin, 2023.
[101] S. Ramachandran, S. V. Rao, and T. Goles, “Information Security Cultures of Four Professions: A Comparative Study,” in *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)*, Jan. 2008, pp. 454–454. doi: 10.1109/HICSS.2008.201.
[102] B. Green, D. Prince, U. Roedig, J. Busby, and D. Hutchison, “Socio-Technical Security Analysis of Industrial Control Systems (ICS),” in *2nd International Symposium for ICS & SCADA Cyber Security Research 2014*, BCS Learning & Development, Sep. 2014. doi: 10.14236/ewic/ics-csr2014.2.

A APPENDICES

In the appendix section, three levels of Appendix headings are available.

A.1 Participant Information

We provide three summative tables with some more details on our participants, their roles, and the type of company they were working for at the time of the interview. 5 of the 72 participants were female. We did not collect any other demographics such as age or experience. OT cybersecurity is an emerging and fast moving field, with many participants having only recently moved to their then current role. In some cases, participants have only moved to their then current role a few weeks to months before the interview. As such, we do not report on participants’ experience in their current role, as more often than not, such experience is misleading. Similarly, most participants had moved through various roles during

their careers, making it very hard to properly delimitate their experience in a specific field (e.g., IT, security, automation, engineering etc.). Overall, as stated in the text, at least 45 participants had a background in OT (engineering, automation, operations etc.), while the others have also been working in adjacent areas like IT or information security before moving closer to OT.

Table 1: Participants' role, sector, and specialism

Role	**Total Number of Participants with the Role**	**Sector, (specialism, if applicable), number of participants**
Chief Information Security Officer (CISO)	3	Water-1 Energy-1 Transport-1
Security Awareness/Training/Culture Specialists	7	Water-1 Energy-2 Transport-1 Space-1 Various (External)-1 Oil & Gas (Security manager)-1
Others	5	Academia-1, Academia & Industry Coordinator-1 Government & Industry Coordinator-1 Student (former Integrator)-1 Security Researcher-1
Regulators	5	Energy-1 Transport-2 Water-1 Nuclear-1
Security Product & Service Vendors (e.g., Business Development, Sales, CTO, CEO,)	9	Various sectors (Business Development)-4 Various sectors(CEO, CTO)-3 Maritime (CEO)-1 Transport (Business Development)-1
OT Managers	10	Water (IoT)-1 Water-1 Water (Security)-1 Energy-3 Oil & Gas-1 Transport-1 Transport (Security)-2
OT Cybersecurity Consultants	33	Transport-3 Energy-2 Manufacturing-1 Automotive-1 Various sectors-26

Table 2: Company type, and number of participants from each company

Company Type	Number of companies and participants at each company	Total Number of Participants in Company Type
Original Equipment Manufacturers (OEM)	3 companies with 1 participant each 1 company with 2 participants 1 company with 4 participants	9
OT Cybersecurity Product and Services Companies	5 companies with 1 participant each 3 companies with 2 participants 1 company with 3 participants	14
Consultancies and Engineering Companies providing OT Cybersecurity	9 companies with 1 participants each 4 companies with 2 participants 1 company with 4 participants	21
Regulatory and governmental bodies	6 organisations with 1 participant each	6
Oil & Gas	1 company with 1 participant 1 company with 2 participants	3
Transport	3 companies with 1 participant each 1 company with 2 participants	5
Energy	1 company with 1 participant 1 company with 5 participants	6
Water	3 companies with 1 participant each 1 company with 2 participants	5
Universities	3 universities with 1 participant each	3
Total	49 Companies	72 participants

A variety of roles exist in OT environments, and no standardised naming conventions exist. For example one participant had the role of process controller, process scientist, and process engineer in different companies with similar responsibilities. With respect to participants with OT experience, their typical career trajectory would start from a more specialized and lower in seniority role in operations, maintenance, or engineering, before progressing up the ranks to more senior engineering and/or management position, and finally, a move to an OT cybersecurity role.

Overall, we would split OT personnel's roles into the following four categories: operators, technicians, engineers, and management. We posit that our findings around OT mindsets are valid for all of these roles, and the factors described (competing values such as safety, technological change, operational realities, occupational development) are all shared to some extent among these roles.

Nevertheless, with respect to cybersecurity, senior process and control and instrumentation engineers and senior OT managers are typically the first to be involved in such conversations, and these are the roles that our OT cybersecurity practitioners (e.g., consultants) mainly liaise with. Accordingly, other roles like technicians and operators will have less interaction with OT cybersecurity practitioners, and cybersecurity measures will often be pushed down to them. Given

their limited responsibilities in the design of these processes, such roles are closer to 'end-users'. Similarly, many engineering roles are also not going to be involved in cybersecurity discussions, typically roles which operate less digitalised technology in areas as such as mechanical engineering, electrical engineering etc. As such, factors like seniority, interaction with digitalized technology, and level of design responsibilities, can be potential indicators for the strength of OT practitioners' cybersecurity mindsets.

Table 3: Roles in OT and example of job titles

Role	Examples
Operators	• Field operators (e.g., machine operators) • Control room operators
Technicians/Maintenance	• Production Technicians • Controls & Automation Specialists • Process Controller etc.
Engineers	• Process Engineer • Control and Instrumentation Engineer • Product Engineer • Project Engineer • Energy Engineer etc.
Managerial Positions	• Project Supervisor • Plant manager • Senior Engineer etc.

A.2 Interview Topic Guide

- Researcher's personal introduction, and overview of the study
    - Consent Reminder
- Participant's background
    - What has led you to your current role? When did you take an interest in OT cybersecurity? When did that become an official OT cybersecurity role?
- Details about current role and company
    - If internal practitioner – details about their function (e.g., security, OT), where does OT cybersecurity sit, what does your company make/produce?
    - If external practitioner – more details on role and services provided
        - What differentiates you from your competitors? Why do companies choose your services? How do you convince potential clients for the need for cybersecurity and your offerings?
        - How is your tool/service used? (e.g., anomaly detection, gateway, incident response services etc.)
    - Regulators and others – ask them to expand on how they work with OT companies
- Factors that have shifted organisational perceptions and practices on OT cybersecurity
    - E.g., Institutional (e.g., regulation), previous attacks, internal organisational factors (e.g., audits)
- Challenges when it comes to cybersecurity (people, processes, and technology), with a focus on OT personnel and organisational challenges

    - Discuss top-down &bottom-up approaches
- Intra-organisational collaboration with other stakeholders
    - E.g., companies and regulators, OEMs, integrators and client companies, standards committees
- Differences between companies, sectors, countries (e.g., for practitioners working in multiple sectors and/or geographies)
    - E.g., sales or consultancy process, security maturity, regulatory practices
- Security culture – What's the first thing that comes to mind with the words OT security culture?
- Safety and Safety culture - Parallels and Differences between security and safety at various levels
    - Institutional factors and their effect on maturity(e.g., regulation, past incidents)
    - Organisational challenges (e.g., collaboration between functions, management systems)
    - Practices (e.g., risk management)
    - End-user's risk perceptions and behaviours
- OT personnel and cybersecurity
    - Workforce development and awareness efforts for OT personnel
    - OT mindset/mentality? What do OT personnel care about? How does cybersecurity fit into this mindset? How do you get them interested in cybersecurity?
- Concluding remarks & Thanking participants

A.3 Code Examples

We provide some more examples of codes related to the themes described in our results.

Operational needs and values

Availability and Hierarchy: "All they're concentrating on is keeping things running, because if things don't run they'll be told off by the bosses." P_20, OT Cybersecurity Consultant, Various sectors

Availability & SLAs: "The control and instrument engineer is worried about availability and uptime. And we dealt with a power plant, power company that had SLAs that meant they [should] have 99.9999% uptime. If there wasn't, they got fined heavily and their approach was well, 'You're not gonna put any stuff on our systems that could impact on that'." P_10, OT Cybersecurity Consultant, Various sectors

Prioritisation of safety: "We have a kind of mantra which is nothing is so important that it shouldn't do it safely, and a very visible support from everybody at all levels that if you've been asked to do something, or you find yourself in a situation that you feel is unsafe, you should stop immediately under any circumstances. Whether the project gets delayed, whether the service gets turned off. None of that is more important than the safety of the individual and the company." P_43, Chief Information Security Officer, Water sector

Operational Realities

Effects of automation: "The old joke in the 80s was that the yeah, if you went into control room the objective was to have one man and his dog. So maybe for each area of a plant there would be a plant operator who could do each area of his plant or her plant and they understood that area of their plant really to [a] high level. And they took a lot of pride in their area of plant. Now when they went to centralized control rooms, the automation managed a lot of that and they were able to like say if you went from 5 operators like to go down to 3 with the associated people and then the nirvana for businesses at the

time was to get to down to one man and his dog. So why does the operator have a dog? The dog's there to make sure the operator doesn't touch anything. The operator is only supposed to be there if a plant winds into an anomalous condition and they were able to bring it back to normal operating conditions." P_14, OT Cybersecurity Consultant, OEM, Various sectors

Strain due to workload: "If people aren't told to fix a problem, they have other fires to put out, they have other challenges that they are prioritising." P_25, OT Cybersecurity Consultant, Various sectors

Occupational and Professional Development

Lack of security in their careers: "So security is quite a new topic to these guys because no one's really targeted them. It's kind of like that whole head in the sand idea that everyone has about security, but even more so because throughout their career they've been trained that the only thing that matters is uptime and everything is safe." P_46, OT Cybersecurity Consultant, Various sectors

Rising through the ranks: "So the history of the people who have ended up in senior operational roles come from being a junior operational roles. And they they've kind of grown up in the environment of how things are done around here using serial connections and maybe some private wires connections. But what they haven't necessarily had is the exposure to the rest of the world of IT and the problems that come with it." P_43, Chief Information Security Officer, Water sector

Loss of knowledge due to personnel leaving the company: "He had obviously been working here for a long, long time, almost probably 15, 20 years. So yeah the documentation wasn't there. So there is that breakdown of data or knowledge flow. Capturing the knowledge of experienced engineers, it's been tricky to document specifically, what they know in their heads. As a business, obviously we do try and shadow engineers, we have also tried to identify sort of our flight risks and all of that, but it obviously didn't help in this case. [Laughs]" P_68, Engineer, Rail sector

Technological Misperceptions

Security by obscurity: "Historically, the onboard systems have been viewed as entirely an engineering problem, and the IT domain is the kind of operation that the wayside systems, you know, the back office systems. Now with connectivity that's changing. There's always a route to the onboard system generally, yeah. You also get things [like] security by obscurity, we're hearing loss in different ways. It it's, it's just all protocols are secure with no one knows about this. This is so niche, such a such a niche system. No one's gonna bother about this. It's not true." P_37, Head of Business Development, Rail sector

Connectivity Perceptions: "We've seen for every single attack into so-called air gap environments, with the exception of Stuxnet, which was really air gap[ped], everything else was usually enabling the adversary to identify credentials, steal them using common techniques, and then basically use the VPNs to connect to IT and OT and live off the land." P_22, OT Cybersecurity Consultant, Various sectors

Stereotyping of Practices

Differences between practices: "From a cultural perspective, IT thinks about asset inventories. They think about consistency. They think about refresh all the time. You know making sure that everything is the same, following the same

you know, policies, procedures and all that kind of stuff. Everything is very locked very, very consistent. It's a lot easier. … You see this all the time, where a CISO will take on say, the CISO will say 'hey its security, so OT security, IT security, it doesn't matter, it's part of my responsibility'. Then the minute they sort of get dashboards from, however poorly dashboards they are from OT, they begin to go like 'Oh my word. The vulnerabilities are terrible. We gotta go fix all the vulnerabilities.' So there's an immediate like responsible to patch environments. It's like you don't understand what that means. We might not even be able to patch this thing for five years. So, it's an understanding from the IT perspective of again it's that context of what you know understanding what [it] means to go do certain activities. Do these vulnerabilities really matter in certain cases? Maybe not." P_1, OT Cybersecurity Consultant, Various sectors

"So engineering, depends on the company, but is usually relatively local. So if you're in a water company that's not the case, because each pumping station or whatever has very low manning, maybe an operator or two. So these [are] quite centralised. But in manufacturing usually you go to [a] car factory and there will be the line for building Jaguars, a line for building Land Rovers, a paint shop, a warehousing and delivery. And all those have got their own teams, quite insular, their own ways of working in different priorities, different manufacturers, equipment…. And they will have their own skills, policies, procedures, training matrices. IT tends to be more global. More centralised. That means they can often think more strategically. They often have a simpler message. They talk about 4000 laptops. It's the laptop estate. You talk about 4000 PLCs. It's all completely different." P_29, OT Cybersecurity Consultant, Various sectors

Security practitioners' efforts

Different levels of pushback and acceptance:

"And some of them buy into it some of them don't. And then gradually you do see some [of] the ones that don't, start to buy into it when they see you're being reasonable with your recommendation." P_3, OT Cybersecurity Consultant, Various sectors

"But also you've gotta be moving away from the cyber language of IT, which is very much you're all doing it wrong. Because people in the engineering world will go 'Don't care.'" P_21, OT Cybersecurity Consultant, Various sectors