10-9-2023

Social aspects in organisational cyber-security effectiveness - Of British coal mines, resilience and emergence

Tom Fabian Hofmann
Hasso Plattner Institute, tom@wicked.design

Danielly de Paula
Hasso Plattner Institute, danielly.depaula@hpi.de

Falk Uebernickel
Hasso Plattner Institute, falk.uebernickel@hpi.de

Social aspects in organisational cyber-security effectiveness - Of British coal mines, resilience and emergence

Research Paper

Tom Hofmann[1]*, Danielly de Paula[1], Falk Uebernickel[1]

[1]Hasso Plattner Institute, Chair for Design Thinking and Innovation Research, University of Potsdam, Potsdam, Germany
tom@wicked.design,{danielly.depaula, falk.uebernickel}@hpi.de

Abstract. Cyber-security, which plays a key role in all areas of the digital world, from the power grid to healthcare, is mainly addressed from an analytical, engineering perspective. This research looks at social factors impacting real-life cyber-security, and their possible effects, such as resilience and emergence. Semi-structured interviews were conducted with 20 participants from a broad range of international organisations. Their analysis shows that social factors are indeed relevant to cyber-security. Tension within social structures in organisations (e.g., employee-supervisor relationship, and peer pressure within teams) can significantly impact cyber-security effectiveness. The study concludes that cyber-security should be addressed through social-technical system design, in recognition of the fundamental interdependence of social and technical aspects. As a corollary, organisational cyber-security needs to be treated as a so-called wicked problem, for which a reductionist engineering approach is futile. The complexity and ambiguity of cyber-security's socio-technical challenges calls for adequate principles, ways of thinking and methods.

Keywords: Socio-Technical Systems, Complex Adaptive Systems, Cyber-Security, Human-Centred Design, Wicked Problems

1 Introduction

Digital technology provides a trove of new opportunities and advantages. Digitisation, and also cyber-security – the discipline of making the deployment of digital technology secure - are here to stay. Cyber-security has become an essential requirement, affecting business operations, research activities, and critical national infrastructures such as hospitals, power and utilities companies and the military. Cyber-security is commonly seen to be driven by technology and processes, to which people are expected to adapt through initiatives that promote training and awareness [1]. There is a general belief that cyber-security incidents are caused by deficiencies in people interacting with technology [2] and that improved technical understanding derived from training and improved awareness is the key to employee compliance [3].

* First and corresponding author

18th International Conference on Wirtschaftsinformatik
September 2023, Paderborn, Germany

Yet, despite all efforts at training employees, cyber-attacks based on social factors have remained very successful. The success of human-targeted tactics can be traced back more than 10 years, see for example reports from the FBI [4, 5], Verizon [6, 7] and Europol [8, 9]. Recently, the challenge of ensuring employees' compliance with cyber-security policies has been investigated by IS scholars [10, 11]. Research on social factors in cyber-security has increased in the past decade, mostly focusing on the individual, who is considered a risk factor [12] or weakest link [13]. A clear risk that stems from social aspects is the increasing usage of shadow-IT [14]. The availability of easy-to-use technology, such as cloud services and smartphones, enables people to operate their own digital infrastructure, outside of organisational boundaries and without the knowledge and approval of IT-departments. This results in a broadened threat landscape and increased risks [15]. While people seem to be aware of risks, they decide to ignore them in favour of achieving their goals [16]. Recently, the importance of investigating the phenomenon through the lens of Socio-Technical Systems (STS) theory has gained some initial recognition. STS theory [17] traces its origins back to 1949, where it described the role and interaction of technology and social aspects in British coal mines. As such, it has been linked to cyber-security mostly as a tool of analysis and as a framework to develop "better" controls. While STS theory helps assess the influence of such socio-technical factors, it does not provide insights into mechanisms and phenomena such as emergence. As a result, previous research has not given consideration to a number of other social factors, such as social relationships [12, 13]. In recognition of this shortfall, the present study argues that a combination of STS and Complex Adaptive Systems (CAS) theory makes us better equipped to understand both social-technical interactions and underlying social mechanisms affecting employee compliance with cyber-security policies.

The aim of this study is to propose a conceptual model illustrating factors relevant to the design of cyber-security measures and susceptible to affect it. Accordingly, the research questions that guided this study are: What social factors are relevant to cyber-security, and how do they affect it (RQ1)? and What is the impact of knowledge and awareness training on employee compliance with cyber-security measures (RQ2)? In view of the complexity of the research questions, we adopted two different perspectives. First, we interviewed senior managers to obtain insights from operational knowledge. We then obtained insights from the organisational regulatory body. Considering that STS theory is not enough to understand how social factors affect cyber-security, we borrowed concepts from CAS theory. This paper contributes to theory by expanding the knowledge of socio-technical theory through the development of a hybrid model that combines elements from STS and CAS to explain socio-technical interactions and the underlying social mechanisms that affect employee compliance with cyber-security policies. From a managerial perspective, our study is a call for organisations to shift the view from a compliance paradigm to a more human-centric view when creating cyber-security policies.

2 Theoretical Background

We gathered relevant concepts, principles and theories from three main topics: cyber-security, STS and CAS.

2.1 Cyber-security

The term cyber-security is somewhat ambiguous [18], and we therefore address the differences between ICT-, information- and cyber-security. Information and Communication Technology (ICT) security is concerned with the protection of technological assets, which store, process and transmit digital data. Accordingly, ICT-security is considered a subset of information-security since the security of all resources and processes dealing with information is an essential requirement. If this condition is not given, the information itself cannot be deemed secure. Information-security addresses the confidentiality, availability and integrity of information. Therein, the term information includes digital and analogue forms, whether it be for storage, processing or transport. Cyber-security addresses the safety of people, and even societies and nations from risks emerging through the usage of the cyber-space. Their interests - including assets that are not information-based - are to be protected. Examples are the usage of the cyber-space to commit crime, like fraud and extortion, or to threaten people's safety, as in stalking or harassment. In this study, we group ICT-, information- and cyber-security under the umbrella term cyber-security.

A major challenge faced by scholars and practitioners in the field of cyber-security is the growing number of cyber-attacks and data breaches in organisations. According to Dtex Systems, 50% of data breaches are a result from non-compliance with cyber-security policy, with an average cost of some $4 million per event [19]. Unsurprisingly, 40% of businesses reported not trusting their employees to appropriately use IT [10]. Indeed, the top three concerns of organisations related to employee non-compliance are: 1) inappropriate sharing of data via mobile devices; 2) physical loss of mobile devices, exposing organisations to risk; and 3) inappropriate IT resource use by employees [10]. People are seen as the weakest link in cyber-security, and IT executives implement compliance-inducing measures such as education campaigns to persuade employees and users to adopt safer behaviour [10, 20]. However, organisations do not have the resources to ensure that employees comply with cyber-security guidelines or to identify which measures are effective. There is even strong evidence that such compliance-inducing measures are ineffective and harmful [11]. Overall, the studies mentioned above highlight the need to move away from straightforward compliance-inducing measures and to understand how to design more effective strategies. Here, we borrowed concepts from STS and CAS theory to propose how cyber-security should be structured as a challenge in organisational (system) design, with a more human-centric view.

2.2 Socio-technical theory — The promises of technology and British coal mines

Digital technology promises a vast increase in productivity and efficiency, similar to anticipations in post-WWII Great Britain. As new technology changed the way people worked [17], the promise of increased productivity failed [21, 22]. Managers and engineers enforcing the adoption of new technology by workers were not familiar with the working environment. Management saw the source of their problems in the workers' unwillingness to comply with directives about how to exploit the new technology. The local workforce insisted that the new technology could not be operated as directed by the engineers, because of extremely unpredictable underground conditions and resulting

safety issues [23]. Yet, results in one mine, in which management chose the approach of closely collaborating with the workers, were extremely good [22]. They were enabled to adapt new technology to fit their needs, through emergence [17]. The discovery of the positive effect of self-organising teams was considered to "contain dynamite" [24] as it questioned hierarchical management, and the researchers were denied publication of their findings [21]. In cyber-security, we observe a similarly strong focus on hierarchical structures, on top-down commands, on the assumption that technology will fix everything, and on the perception that problems result from people's unwillingness to adapt to technology and follow policies. STS theory was explicitly developed around the notion of *systems* [21]. A system can be defined as "sets of elements standing in interaction" [25], such as teams, organisations or societies. In STS theory, organisations consist of a multitude of elements in constant mutual interaction. Trist and Bamforth divided every organisational system into a social (sub-)system and a technical (sub-)system [23]. The social system includes people, but also their relationships, their professional and personal culture, the management methods in place, and any given experiences of working in the organisation. The technical system as such includes technology, but also the policies regulating actual work. This insight is relevant because the current framework applied in cyber-security only considers (individual) people, processes and technology (PPT) [1], ignoring the social context and its influence on people. Successful or unsuccessful system performance depends on the interactions of social and technical factors. Some of them are intentionally designed, relying on straightforward cause-and-effect relationships. Other interactions are of complex, unpredictable, often unintentional, or even undesirable, and non-linear in nature [26]. People are not machines and cannot be programmed to behave like technical components - a fact few cyber-security researchers and practitioners appear to be aware of. While much work in cyber-security aims at achieving behavioural change, it appears to be remarkably ineffective [27]. Furthermore, optimising just one system – be it only the social system, or only the technical one - will result in a sub-optimal performance of the overall system, i.e., of the organisation as a whole [21, 26, 28]. This holds also for modifications to social and technical systems, which increase the possibility and emergence of unforeseen, undesired and undesigned non-linear relationships [26]. A corollary of this, and the most important objective in the design of STS [26], is the necessity of a *joint optimisation* of social and technical systems [21, 28]. Research on STS should be conducted at three broad levels: the micro (primary work team), meso (organisation) and macro levels (societies) [21]. This is especially important because most studies on humans and cyber-security focus on the individual, rather than including social structures. Cyber-security is very much focused on technological advancements, while STS provides a holistic approach, considering social and technical factors and their interrelationships. This approach has been used to promote systems thinking in cyber-security, designing and supporting education [29, 30], addressing human and cultural factors [31]. STS theory has also been used to develop conceptual models to analyse organisations in the context of cyber-security [32] and corresponding risks [33]. Research showed the importance of STS design towards effective cyber-security [34], yet it lacked information on what social factors are involved and need to be considered. Considering the social factors research narrowed the view and focused on the individual [35]. This led to the belief that knowledge and training

are necessary to adapt people to technology. The research analysed mostly focuses on the individual, neglecting other social factors inside and outside the organisation. An important aspect of STS is the characteristic of complexity [36], which is also true for cyber-security [37]. System phenomena - such as self-organisation, non-linear behaviour, resilience and emergence [36] - lead to tangible effects, like shadow-IT [38], serving thousands of users [15]. Those features are inherent to CAS [39]. We therefore propose to consider STS as a type of CAS, applying a *system of systems* approach in analysing STS [36].

2.3 Complex adaptive systems

Complex adaptive systems are defined as "systems composed of interacting agents described in terms of rules. The agents adapt by changing their rules as experience accumulates" [40]. Scholars have formulated the theory of CAS in various ways, however, three components are consistently mentioned: *agents*, *interactions*, and an *environment* [41]. Agents are individuals actors within a CAS and represent a wide variety of entities such as humans, organisations, objects or concepts. They have the ability to perceive their environment, interact with other agents and the environment in many ways, which can result in complex and unpredictable emergent behaviour (i.e., emergence). Emergence is a bottom-up process that refers to “collective phenomena that are collaboratively created by individuals, yet are not reducible to individual action” [42]. It is an inherent property of CAS, and enables complex systems to adapt, learn and change according to influences of their internal and/or external environment. As an irreducible property of an organisation, it can neither be fully understood nor predicted by examining the parts, such as people or technology, alone. Shadow-IT is irreducible, insofar as it had not existed as a recognised component of the organisation beforehand. Emergent properties often contribute to the resilience of a system. Resilience is the ability of a system [36] or an individual [43] to survive, adapt and learn when facing difficulties or changes in its environment. It is often related to specific risks, hazards, or periods of crisis [44], but also represents the capability to respond to a range of different, less severe, novel disturbances [45]. Overall, CAS has been the subject of a number of studies that address how human actors self-organise in organisational contexts and what behaviours emerge [46, 47]. These studies are part of the “third wave” of systems theory, which primarily seeks to characterise the properties and mechanisms of bottom-up processes [48]. However, as a relatively new stream of thought, CAS theory is still evolving on the topic of emergence in specific. This study extends the third-wave of systems theory through the development of a hybrid model that combines elements from CAS with STS to explain what social factors affect employee compliance with cyber-security measures. It extends current research on the concept of complexity and its impact on cyber security [49–51] .

3 Methodology

We present a qualitative social science study, based on two theories of organisational design, i.e., STS and CAS theories. This study aims to create a conceptual model

that illustrates factors that are relevant to the design of cyber-security measures and susceptible to affect it. To achieve our research goal, we gathered data about operational knowledge from selected organisations and their cyber-security activities. Operational knowledge encompasses insights into the inner workings of an organisation, e.g., how decisions were made, what challenges appeared, what the response was and why [52]. The research of operational knowledge is based on concepts derived from the underlying frameworks of STS and CAS theory. The smallest unit of analysis, at the micro level, are the actual work groups - or teams - in the organisation. This is where conflicts or challenges between cyber-security and daily business possibly arise. As such, our study follows the original research design approach of Trist and Bamforth [21, 26]. We selected two groups of participants, representing distinct levels within the organisation: senior managers and cyber-security experts.

3.1 Sampling strategy and research setting

We used snowball sampling [53] to purposefully select our participants on the basis of the following criteria. First, we targeted a wide range of key organisations from different types of industry sector, size and geographical location. For instance, we included multi-billion US$ financial companies, an international law firm, hospitals, a research institute and a country's military department. The geographical diversity ranges from local businesses in the SME category to international enterprises. It contains 3 SMEs, 1 intermediate enterprise and 10 large enterprises. Second, to gain insights from the perspective of a regulatory body, we targeted organisational-internal senior cyber-security experts (meso level), and to obtain operational knowledge (micro level), we targeted senior managers. The two perspectives allowed us to contrast views and experiences of those who plan and implement cyber-security measures with those who are affected by them as employees. Third, we systematically collected and analysed our empirical data until 'no new data appear[ed]' [54] in line with our research approach [55]. Theoretical saturation was reached with a set of 20 senior experts from 14 leading organisations. An overview of our interviewee's background and their codes can be found in **Tab. 1**. The organisations were chosen to ensure a diverse cross-sector dataset, encompassing a variety of hierarchical and operational organisation models.

3.2 Data collection

We followed well-established guidelines for qualitative research for data collection and analysis [56], i.e., constant comparison, iterative conceptualisation, scaling up, and theoretical integration. We conducted a thorough literature review in 10 different databases: ACM Digital Library, Google Scholar, IEEE Xplore, JSTOR, SAGE Journal, SAGE Knowledge Science, Direct Scopus, Springer and Wiley Online Library. For each database, we designed a search query to combine cyber-security, socio-technical system theory and complex adaptive system theory terms. We reviewed and verified the results to a) address social factors, beyond the individual, in the research and b) mention a combination of STS and CAS in regards to explicitly explaining the internal mechanics and phenomena in an organisation (such as resilience and emergence). Our set of data sources

Table 1. Organisation and interviewee overview.

Organisation	*Interviewees/ID*	*Employees*	*Revenue/ Budget (USD)*	*Area of operations*
Armed forces	Dept. Head/B001	9-12k	70-100B	Europe
Research & education	Researcher/B002	-	-	Europe
Chemicals & process industry	Vice Pres. IT/B003 CISO/S001	15-18k	10-13B	Globally
Finance	Prog. Manager/B004 Chief DLP Officer/S007	72-75k	18-21B	Globally
Finance	Software Eng./B007	48-51k	21-24B	Globally
Power & utilities	Head Consulting & Services/S010 Head of Comms./B010	-	-	Switzerland
Consulting	Cyber-Sec Advisor/B008	135-140k	21-24B	Globally
Logistics & transport	Deputy Editor in Chief/B009 Sr. InfoSec Awareness/S002	96-100k	10-13B	Globally
Luxury goods	CIO/CISO/S003	6-9k	15-18B	Globally
Healthcare	CISO/S004	2-3k	210-240M	Europe
Municipality	Key Acc. Mgr./B005 CISO/S005	18-21k	9-12B	Switzerland
Law firm & legal counselling	CIO/S006	0.1-0.3k	30-33M	Europe
NGO	CISO/S008	6-9k	7-10B	Globally
Foundation	Head of Sec./S009 Prod. Marketing Mgr./B006	0.1-0.3k	30-33M	Switzerland

build on semi-structured interviews that took place in 2021. To achieve two perspectives on the same phenomenon, we created two sets of questions as part of the construction of the interview guideline. The interview guideline was developed according to the underlying theoretical-analytical categories of the two system theories [57], STS and CAS. The questions for the senior managers aimed to understand the needs, challenges, and responses of their particular team concerning cyber-security measures, whereas the questions for the cyber-security experts focused on how and why organisations established those measures. All interviews lasted around 60-90 minutes and were conducted online in either German, Swiss German or English, depending on the interviewee's preference. We developed the interview guide according to the underlying theoretical-analytical categories of the two system theories, STS and CAS. This theory-led approach allows a reciprocal examination of textual interpretation and theoretical knowledge in the phase of analysis [57]. From the 20 interviews, 17 were allowed to be recorded. The answers and comments from the three non-recorded interviews were directly paraphrased after the interview for later analysis. Considering that many participants were aware that their behaviour was non-compliant with the organisation's policies and the cyber-security experts were concerned about disclosing potential cyber risks to an outsider, a challenge during recruitment and when conducting the interviews was earning the participants'

trust. The initial reluctance was mitigated after the interviewing author demonstrated professional business expertise in the field.

3.3 Data analysis and model development

Our research analysis consisted of the three main phases of transcription, coding and network analysis of categories and themes [58]. In the first phase, 17 recorded interviews were fully transcribed, and prosodic and paraverbal utterance features were omitted. 3 interviews without recording were paraphrased during the interview and reviewed afterwards. In the second phase, the transcripts were coded to identify relevant material in the text. Coding was conducted in two main parts: 1) Deductive codes are derived from the pre-formulated, STS and CAS theory-based aspects of analysis. 2) An inductive coding cycle was used for a more detailed analysis of the text concerning the operational knowledge of the interviewee and its relationship to the study. It was also used to identify new and emerging patterns within the statements. The first author developed two corresponding codebooks. The codebooks and results were reviewed by the other authors. In the third phase, categories and themes were developed, based on a codes-to-theory model for qualitative inquiry [58]. A CAQDAS software was used to enable tool-based analysis and networking. Non-English interviews were carefully translated into English by the authors who have advanced English skills. We analysed the data through multiple rounds, balancing the discovery of new insights from the data with structures and principles derived from theoretical models and concepts from STS and CAS. The process led to the development of a hybrid model that extends studies on STS and cyber-security to include theoretical concepts from CAS. We incorporated social and technical subsystems of STS (including social factors and how they extend beyond organisational boundaries) and the CAS aspects of emergence and resilience, as identified in this study. The model was developed iteratively by the first author and reviewed by the other authors. It allows to analyse phenomena such as shadow-IT in a unique way, by enabling to identify internal and external social factors and the potential self-amplification of emergent behaviour.

4 Results

In this study, we identified various social factors capable of influencing and impacting organisational cyber-security, as predicted by STS theory. Furthermore, mechanisms has been observed leading to non-compliant behaviour, which are related to CAS theory. We developed a conceptual model to represent the results and the relationships between various elements and phenomena, shown in **Fig. 1**. The lower part is borrowed from STS theory [59], representing the organisation and their social and technical subsystems. Inside the organisation, the social subsystem consists of the individual people but also of their relationships, hierarchies and social structures. We extended this subsystem beyond organisational boundaries to represent external social factors between and transcending organisations. The lower right part represents the work and technical elements. The latter have been also extended beyond the organisation to represent and show how publicly available technology is integrated in emergent behaviour. The middle part depicts CAS

phenomena - resilience and emergence - and their interaction with organisations. Solutions such as shadow-IT emerge from people's resilience in combination with available technologies. They can lead to positive feedback, as the workaround helps to get a job done, but also to negative one, e.g. when it violates compliance. Therefore, the model allows for a better understanding of the different social factors, e.g. peer pressure, their effects, e.g. fear and insecurity, and the impact through resilience and emergence in terms of information security policy design [60]. The upper part represents the risks stemming from the emergent, non-compliant, behaviour.

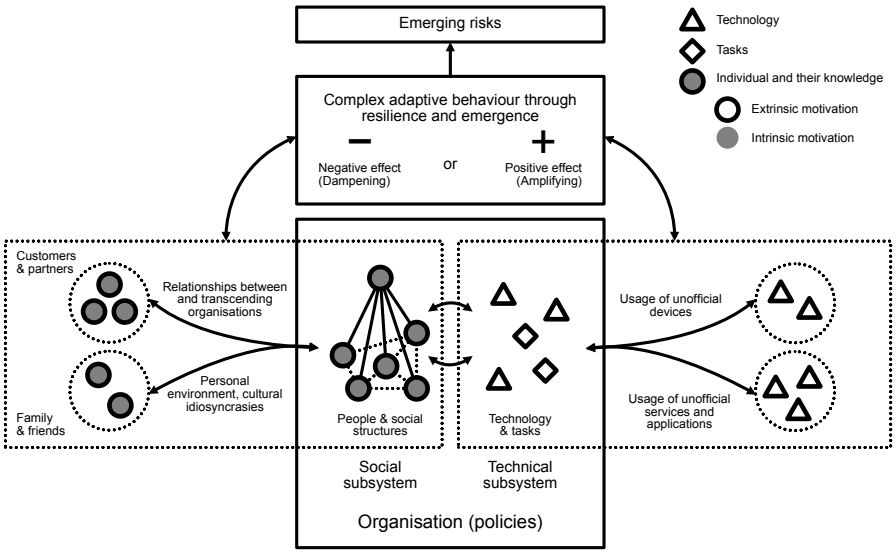

Figure 1. Cyber-security in the context of STS and CAS.

4.1 Social factors that affect cyber-security

This research identified two groups of social factors, one related to the individual, and the other to relationships between people (RQ1). Motivation - both *intrinsic* and *extrinsic* - is a significant factor at the individual level, mentioned by 100% of interviewees. On an individual level, intrinsic and extrinsic motivation has shown to be a significant factor being mentioned by all interviewees. Intrinsically-motivated behaviours are generated by the sense of personal satisfaction that they bring. We identified three sub-factors: *autonomy*, *mastery* and *purpose*. Interviewees reported they want the freedom to design their workplace in order to achieve their goals, do good quality work and get the job done (S002). 16 out of 20 interviewees stated this is an important factor in regard to cyber-security compliance. This was particularly voiced in the healthcare domain, where employees seem to use shadow-IT frequently with justifications relating to mastery,

such as "We save lives, we work with patients. [...] formalism and such comes second" (S005). We found that intrinsic factors are interrelated rather than separated, and can be influenced by extrinsic factors. Extrinsically-motivated behaviours are performed to receive (or avoid receiving) something from others based on three factors: *compensation*, *punishment* and *reward*. Financial incentives as part of a bonus plan (S006) or the fear of being punished for failed goals (B009) are examples of this.

Another strong social factor are *relationships*. They occur within organisations, but also extend beyond their boundaries. Inside organisations, influential relationships appear horizontally in teams and peer groups, and vertically top-down between superiors and employees. External relationships occur between organisations, through customer pressure and peer dynamics, and transcending organisation, through the personal environment and cultural idiosyncrasies. 19 interviewees across 13 organisations reported that relationships contribute to non-compliant behaviour, while 12 interviewees in 10 organisations mentioned group dynamics, e.g., WhatsApp. Despite being non-compliant, it gets used because people need to circumvent technical and organisational restrictions; for example, using WhatsApp for communication (B007). 10 interviewees from 9 organisations reported peer pressure as influencing their cyber-security behaviour. A team under stress will develop locally emergent workarounds to cope with the stress, like WhatsApp for work coordination (S002). Interviewees reported that significant stress is exerted top-down, for example, to achieve financial goals and to avoid punishment. The fear of punishment for failing to achieve business goals is greater than the fear of using non-compliant technology. As one interviewee stated: "you will not go to your manager and say: *"Sorry, I won't deliver results even though I could, because we don't have an approved communication tool like WhatsApp, and WhatsApp is forbidden."* Good luck with finding a manager who tells you that you did a good job for waving the flag for cyber-security." (B008). Another one said: "I'm not being paid to use a tool, but for the output generated" (S003). 16 interviewees from 11 organisation described that they are influenced by external parties, explicitly mentioning customer pressure (5 interviewees in 4 organisations) and external peer pressure (14 interviewees in 10 organisations) towards, e.g., establishing and using shadow-IT. What people use with family and friends is likely to emerge in a business environment. 3 interviewees in 3 organisations described cultural idiosyncrasies, like the usage of WeChat in China (S001).

4.2 Resilience, emergence, and risks

The effects of social factors lead to two CAS phenomena: *resilience* and *emergence*, see **2.3**. People react to stress and disturbances through resilience, in the form of adaption and recovery, as was observed in 100% of the organisations. This led to emerging non-compliant behaviour, such as shadow-IT, which was observed in every organisation. Emergence is not a local, isolated phenomenon; it appears and manifests itself within and among teams, across all hierarchical levels of an organisation, from team leaders to middle and C-level management. Furthermore, it can extend beyond organisational boundaries, e.g., when working with clients and partners.

13 of the interviewed organisations have cyber-security policies and guidelines in place. Yet, 17 interviewees from 12 organisations confirmed that their organisation

was aware of shadow-IT or other workarounds. Interestingly, management did not enforce compliance with organisational guidelines, but rather - implicitly and willingly – condoned shadow-IT as an emergent solution for the sake of business. In one organisation, board members simply overruled policies in order to use actually prohibited tools like Zoom (S001). Others said they had to attend external events hosted on Zoom. As it was forbidden they switched to private devices (B003). The business interviewees and their colleagues were well aware of their risky behaviour, but consciously decided to ignore them, in favour of their business, team or personal goals. All 10 interviewed cyber-security experts were aware of the existence and usage of unofficial tools and services in their organisation. While they are without a doubt knowledgeable and capable of solving complicated - technical - problems, they struggle to address complex ones, like emergence. The interviews showed that the different factors are interrelated, to different degrees. Extrinsic motivation turned out to be the most influential factor, encouraged by organisational design, e.g., through bonus structures. Superiors are widely motivated to achieve monetary gains - an extrinsic motivation - and oftentimes exert pressure onto on their teams to prioritise financial goals over compliance. If in addition a client demands the usage of non-compliant tools, such as Google Drive, employees will give in in order to not to endanger the project, and to satisfy their supervisor's demands.

This behaviour caused substantial risks. The three main contributions towards increasing organisational risks are: usage of unofficial devices; usage of unofficial services/applications; and uncontrollable use and handling of data. This results in three main risk categories: direct risks towards cyber-security controls; data privacy risks; and contractual (legal) risks. The most apparent risks are the ones related to cyber-security objects. The usage of non-compliant, unauthorised and unaudited solutions can compromise the confidentiality, availability and integrity of organisational information. Additional risks are partly a byproduct of emergent behaviour, such as violations of data privacy regulations, e.g., GDPR, or official secrets acts, which can lead to reputational and financial damage. Another risk is the potential violation of contractual agreements. Both can impact organisations, as well as the individual, resulting in legal sanctions for both parties, i.e., liability claims. Many interviewees confirmed that they and their colleagues are generally aware of possible risks.

4.3 Knowledge and awareness in fostering compliance

Our study also explored the role and effect of knowledge and awareness, as they are popular controls in organisations and science. 12 out of 14 organisations conduct cyber-security training, including passive elements - such as blog posts and videos - and active elements - like e-learning and questionnaires. Generally, the assumption is that the problem is due to a lack of knowledge, and that people will adapt if they know more about cyber-security. The aim is to alter employee behaviour to match technical requirements. We found that this assumption is flawed, (RQ2). 15 out of 20 interviewees stated that employees in their organisations are (well) aware of potential cyber-security risks; however, in all 14 organisations unofficial or unauthorised tools and services (shadow-IT) were used. Here, we showed that non-compliant behaviour originates from conscious decisions due to conflicting goals and interests - based on intrinsic and extrinsic

motivation - rather than from a lack of knowledge or awareness, and that organisational and socio-structural influences are neglected in organisations' measures addressing cyber-security.

5 Conclusion

This research confirms the value of systems thinking in cyber-security. It extends existing work in the area of STS and cyber-security [2] by identifying various social factors and their influence, from the individual to supervisor relationships and peer pressure. Those factors are significantly influenced by the organisation design - such as bonus systems or work culture. They even extend beyond organisational boundaries, including clients, partners, families and friends. As such, this study also confirms the approach to conduct STS research at the work group level, rather than the individual [21].

It confirms the two main principles in STS design [26]. Focusing on technical optimisations of cyber-security, while neglecting social factors, leads to unhealthy effects [17, 22]. By applying CAS theory, we provide an explanation for "non-linear" and complex phenomena [26] resulting in effects such as shadow-IT. The notion of "humans as the weakest link" [13] contradicts the findings of this study. The same is true for the assumption that awareness is key [3]. Instead, it is a range of social factors [23] that contribute to safe behaviour. As technology advanced from coal mines to cloud computing, the underlying principles of STS still apply.

The study included multi-national organisations, yet it might be beneficial to extend future research to interviews outside the EU region. Furthermore, a longitudinal study can provide further insights and confirm the findings through a quantitative approach. Future research could usefully explore the relevance of systems thinking in the field of cyber-security. A combined approach of STS and CAS theories also seems to be beneficial for understanding and designing better-performance cyber-security.

From a theoretical perspective, our study makes a timely and necessary contribution to the current debate about employees compliance with cyber-security policies. First, we expand the knowledge of STS theory to combine elements from CAS to explain the underlying social mechanisms affecting cyber-security. Then, we identified relevant factors from industry practices and integrated into the conceptual framework. Furthermore, this paper contributes to practice by recommending policymakers to consider social aspects when designing cyber-security controls. Comprehending cyber-security as a problem which can be addressed by technology alone appears to be the real elephant in the room. Today's focus of cyber-security on technology and processes is necessary, but by no means sufficient. Given the complexity of STS and the effects of CAS, the authors suggest that organisational cyber-security is rather a wicked problem [61, 62] than a complicated one. Furthermore, solutions need to address human desirability, business viability, and technical feasibility [63]. In this context, we recommend researchers and practitioners to look at the current body of knowledge on human-centred design [64, 65] and its potential in designing effective systems [66, 67].

References

1. Amanda Andress. *Surviving security: How to integrate people, process, and technology*. Auerbach Publications, 2nd edition, 2003-12-18. ISBN 978-0-429-21043-3. https://doi.org/10.1201/9780203501405.
2. Gordon Baxter and Ian Sommerville. Socio-technical systems: From design methods to systems engineering. *Interacting with Computers*, 23(1):4–17, 2011-01. https://doi.org/10.1016/j.intcom.2010.07.003.
3. Ling Li, Wu He, Li Xu, Ivan Ash, Mohd Anwar, and Xiaohong Yuan. Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, 45:13–24, 2019-04. https://doi.org/10.1016/j.ijinfomgt.2018.10.017.
4. Federal Bureau of Investigation (FBI). 2020 internet crime report, 2020. URL `https://web.archive.org/web/20220422112606/https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf`.
5. Federal Bureau of Investigation (FBI). 2011 internet crime report, 2011. URL `https://web.archive.org/web/20220422112208/https://www.ic3.gov/Media/PDF/AnnualReport/2011_IC3Report.pdf`.
6. Verizon. 2021 data breach investigations report (DBIR), 2021. URL `https://web.archive.org/web/20220422122253/https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdfx`.
7. Verizon. 2011 data breach investigations report (DBIR), 2011. URL `https://web.archive.org/web/20220122034248/http://www.wired.com/images_blogs/threatlevel/2011/04/Verizon-2011-DBIR_04-13-11.pdf`.
8. European Union Agency for Law Enforcement Cooperation. Internet organised crime threat assessment (IOCTA) 2021, 2021. URL `https://web.archive.org/web/20220422111850/https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf`.
9. European Union Agency for Law Enforcement Cooperation. Internet organised crime threat assessment (IOCTA) 2011, 2011. URL `https://web.archive.org/web/20220422111842/https://www.europol.europa.eu/cms/sites/default/files/documents/octa2011.pdf`.
10. W. Alec Cram, Jeffrey G. Proudfoot, and John D'Arcy. Maximizing employee compliance with cybersecurity policies. *MIS Quarterly Executive*, 19(3), 2020.
11. W. Alec Cram, John D'Arcy, and Jeffrey G. Proudfoot. Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly*, 43(2):525–554, 2019.
12. Devin C. Streeter. The effect of human error on modern security breaches. *Strategic Informer: Student Publication of the Strategic Intelligence Society*, 1(3):2, 2013.

13. Tracey Caldwell. Training – the weakest link. *Computer Fraud & Security*, 2012 (9):8–14, 2012-09. https://doi.org/10.1016/S1361-3723(12)70091-X.
14. Gabriela L. Mallmann, Antonio Carlos Gastaud Maçada, and Mírian Oliveira. The influence of shadow IT usage on knowledge sharing: An exploratory study with IT users. *Business Information Review*, 35(1):17–28, 2018-03. https://doi.org/10.1177/0266382118760143.
15. Symantec. 2018 Symantec shadow data report, 2018. URL `https://web.archive.org/web/20220422115647/https://docs.broadcom.com/doc/2018-shadow-year-report-en`.
16. Andreas Györy, Anne Cleven, Falk Uebernickel, and Walter Brenner. Exploring the shadows: IT governance approaches to user-driven innovation. In *European Conference on Information Systems*, page 13, 2012.
17. Eric L. Trist and Kevin W. Bamforth. Some social and psychological consequences of the longwall method of coal-getting: An examination of the psychological situation and defences of a work group in relation to the social structure and technological content of the work system. *Human Relations*, 4(1):3–38, 1951-02. https://doi.org/10.1177/001872675100400101.
18. Rossouw von Solms and Johan van Niekerk. From information security to cyber security. *Computers & Security*, 38:97–102, 2013-10. https://doi.org/10.1016/j.cose.2013.04.004.
19. Dtex Systems. The 2018 insider threat intelligence report. URL `https://www.dtexsystems.com/resources/white-papers/2018-insider-threat-intelligence-report/`.
20. Mark-David McLaughlin and Janis Gogan. Challenges and best practices in information security management. *MIS Quarterly Executive*, 17(3):12, 2018. URL `https://aisel.aisnet.org/misqe/vol17/iss3/6`.
21. Eric L. Trist. *The evolution of socio-technical systems: A conceptual framework and an action research program*. Ontario Ministry of Labour, Ontario Quality of Working Life Centre, 1981. ISBN 978-0-7743-6286-3. URL `https://web.archive.org/web/20220422115915/https://trove.nla.gov.au/work/18802828`.
22. William Pasmore, Stu Winby, Susan Albers Mohrman, and Rick Vanasse. Reflections: Sociotechnical systems design and organization change. *Journal of Change Management*, 19(2):67–85, 2019-04-03. ISSN 1469-7017, 1479-1811. https://doi.org/10.1080/14697017.2018.1553761.
23. William A. Pasmore and Gurudev S. Khalsa. The contributions of Eric Trist to the social engagement of social science. *Academy of Management Review*, 18(3): 546–569, 1993.
24. Frans M. van Eijnatten. An anthology of the socio-technical systems design (STSD) paradigm: From autonomous work groups to democratic dialogue and integral organizational renewal. 1991.
25. Ludwig von Bertalanffy, Wolfgang Hofkirchner, and David Rousseau. *General System Theory: Foundations, Development, Applications*. 1st edition, 1968.
26. Guy H. Walker, Neville A. Stanton, Paul M. Salmon, and Daniel P. Jenkins. A review of sociotechnical systems theory: A classic concept for new command and control paradigms. *Theoretical Issues in Ergonomics Science*, 9(6):479–499, 2008-11. https://doi.org/10.1080/14639220701635470.

27. Maria Bada, Angela M. Sasse, and Jason R. C. Nurse. Cyber security awareness campaigns: Why do they fail to change behaviour? page 15, 2015. https://doi.org/https://doi.org/10.48550/arXiv.1901.02672.
28. Fred Emery. Characteristics of socio-technical systems. In Eric Trist, Hugh Murray, and Beulah Trist, editors, *The social engagement of social science, Volume 2*. University of Pennsylvania Press, 1993-01-31. ISBN 978-1-5128-1905-2. https://doi.org/10.9783/9781512819052-009.
29. Erjon Zoto, Mazaher Kianpour, Stewart James Kowalski, and Edgar Alonso Lopez-Rojas. A socio-technical systems approach to design and support systems thinking in cybersecurity and risk management education. *Complex Systems Informatics and Modeling Quarterly*, (18):65–75, 2019-04-30. https://doi.org/10.7250/csimq.2019-18.04.
30. Erjon Zoto, Stewart James Kowalski, Edgar Alonso Lopez Rojas, and Mazaher Kianpour. Using a socio-technical systems approach to design and support systems thinking in cyber security education. CEUR Workshop Proceedings, 2018. ISBN 1613-0073.
31. Isabella Corradini and Enrico Nardelli. Building organizational risk culture in cyber security: The role of human factors. In Tareq Z. Ahram and Denise Nicholson, editors, *Advances in human factors in cybersecurity*, volume 782 of *Advances in intelligent systems and computing*, pages 193–202. Springer International Publishing, 2019. ISBN 978-3-319-94781-5 978-3-319-94782-2. https://doi.org/10.1007/978-3-319-94782-2_19.
32. Masike Malatji, Sune Von Solms, and Annlizé Marnewick. Socio-technical systems cybersecurity framework. *Information and Computer Security*, 27(2):233–272, 2019-06-12. https://doi.org/10.1108/ICS-03-2018-0031.
33. Thomas Richard McEvoy and Stewart James Kowalski. Deriving cyber security risks from human and organizational factors – A socio-technical approach. *Complex systems informatics and modeling quarterly*, (18):47–64, 2019-04-30. https://doi.org/10.7250/csimq.2019-18.03.
34. Moufida Sadok, Christine Welch, and Peter Bednar. A socio-technical perspective to counter cyber-enabled industrial espionage. *Security Journal*, 33(1):27–42, 2020-03. https://doi.org/10.1057/s41284-019-00198-2.
35. Grethe Østby, Lars Berg, Mazaher Kianpour, Basel Katt, and Stewart James Kowalski. A socio-technical framework to improve cyber security training: A work in progress. CEUR Workshop Proceedings, 2019. ISBN 1613-0073.
36. Dominique Luzeaux, editor. *Complex systems and systems of systems engineering*. ISTE, 2011. ISBN 978-1-84821-253-4.
37. Wolter Pieters. Defining the weakest link; comparative security in complex systems of systems. In *2013 IEEE 5th International conference on cloud computing technology and science*, pages 39–44. IEEE, 2013-12. ISBN 978-0-7695-5095-4. https://doi.org/10.1109/CloudCom.2013.101.
38. Cecil Eng Huang Chua and Veda C. Storey. Central IT or shadow IT? Factors shaping users' decision to go rogue with IT. page 14, 2014.
39. John H. Holland. Complex adaptive systems and spontaneous emergence. In Alberto Quadrio Curzio and Marco Fortis, editors, *Complexity and industrial clusters*,

Contributions to economics, pages 25–34. Physica-Verlag HD, 2002. ISBN 978-3-7908-1471-2 978-3-642-50007-7. https://doi.org/10.1007/978-3-642-50007-7_3.
40. John H. Holland. *Hidden order: How adaptation builds complexity*. Addison Wesley Longman Publishing Co., Inc., 1996.
41. Murray Gell-Mann. *The quark and the jaguar: Adventures in the simple and the complex*. Macmillan, 1995.
42. R. Keith Sawyer. *Social emergence: Societies as complex systems*. Cambridge University Press, 2005.
43. Tetsuo Sawaragi. Design of resilient socio-technical systems by human-system co-creation. *Artificial Life and Robotics*, 25(2):219–232, 2020-05. https://doi.org/10.1007/s10015-020-00598-3.
44. Gang Wu, Adriana Feder, Hagit Cohen, Joanna J. Kim, Solara Calderon, Dennis S. Charney, and Aleksander A. Mathé. Understanding resilience. *Frontiers in behavioral neuroscience*, 7:10, 2013.
45. Lucy Faulkner, Katrina Brown, and Tara Quinn. Analyzing community resilience as an emergent property of dynamic social-ecological systems. *Ecology and Society*, 23(1), 2018. https://doi.org/10.5751/ES-09784-230124.
46. Ning Nan and Yong Lu. Harnessing the power of self-organization in an online community during organizational crisis. *MIS Quarterly*, 38(4):1135–1158, 2014.
47. Xueyan Dong, Xuan Xiong, Tienan Wang, and Jingjing Ge. Self-organization power: Exploring the synthesis process of self-organization in emergencies - a qualitative study based on COVID-19 epidemic lockdown in China. In *PACIS 2022 Proceedings. 292.*, 2022.
48. Ning Nan. Capturing bottom-up information technology use processes: A complex adaptive systems model. *MIS Quarterly*, pages 505–532, 2011.
49. Michael D. Norman and Matthew T. K. Koehler. Cyber defense as a complex adaptive system: A model-based approach to strategic policy design. In *Proceedings of the 2017 International Conference of The Computational Social Science Society of the Americas*, pages 1–1, 2017.
50. Albert Olagbemiro. Cyberspace as a complex adaptive system and the policy and operational implications for cyberwarfare. In *National Security: Breakthroughs in Research and Practice*, pages 250–264. IGI Global, 2019.
51. Rick Slangen. Understanding cyber-risk by investigating the behaviour of defender and threat agent organisations: Why a complex adaptive systems perspective contributes to further understanding cyber-risk. 2016.
52. Robert Kaiser. *Qualitative Experteninterviews*. Springer Fachmedien Wiesbaden, 2014. ISBN 978-3-658-02478-9 978-3-658-02479-6. https://doi.org/10.1007/978-3-658-02479-6.
53. Michael D. Myers and Michael Newman. The qualitative interview in is research: Examining the craft. *Information and organization*, 17(1):2–26, 2007.
54. Janice M. Morse. The significance of saturation, 1995.
55. Heinz K. Klein and Michael D. Myers. A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly*, pages 67–93, 1999.
56. Dennis A. Gioia, Kevin G. Corley, and Aimee L. Hamilton. Seeking qualitative rigor in inductive research: Notes on the Gioia methodology. *Organizational Research Methods*, 16(1):15–31, 2013-01. https://doi.org/10.1177/1094428112452151.

57. Alexander Bogner, Beate Littig, and Wolfgang Menz. *Das Experteninterview*. Springer, 2002. ISBN 3-531-14447-2. https://doi.org/10.1007/978-3-322-93270-9.
58. Johnny Saldaña. *The coding manual for qualitative researchers*. SAGE, 2nd edition, 2013. ISBN 978-1-4462-4736-5 978-1-4462-4737-2.
59. Robert P. Bostrom and J. Stephen Heinen. MIS problems and failures: A socio-technical perspective. Part I: The causes. *MIS Quarterly*, 1(3):17, 1977-09. https://doi.org/10.2307/248710.
60. Gregory D. Moody, Mikko Siponen, and Seppo Pahnila. Toward a unified model of information security policy compliance. *MIS Quarterly*, 42(1):285–312, 2018. https://doi.org/10.25300/MISQ/2018/13853.
61. Horst W. J. Rittel and Melvin M. Webber. Dilemmas in a general theory of planning. *Policy sciences*, 4(2):155–169, 1973.
62. Horst W. J. Rittel. *The reasoning of designers*. IGP, 1988.
63. Eric Trist, Gurth Higgin, Hugh Murray, and Alex Pollock. *Organizational choice: Capabilities of groups at the coal face under changing technologies: The loss, rediscovery & transformation of a work tradition*. Routledge, 1963. ISBN 0-203-43632-6.
64. Danielly de Paula, Carolin Marx, Ella Wolf, Christian Dremel, Kathryn Cormican, and Falk Uebernickel. A managerial mental model to drive innovation in the context of digital transformation. *Industry and innovation*, 30(1):42–66, 2023.
65. Stefanie Gerken, Falk Uebernickel, and Danielly de Paula. *Design thinking: a global study on implementation practices in organizations: Past-present-future*. Universitätsverlag Potsdam, 2022.
66. Richard Buchanan. Systems thinking and design thinking: The search for principles in the world we are making. *She Ji: The journal of design, economics, and innovation*, 5(2):85–104, 2019-22. https://doi.org/10.1016/j.sheji.2019.04.001.
67. Richard Buchanan. Wicked problems in design thinking. *Design issues*, 8(2):5, 1992-21. https://doi.org/10.2307/1511637.