Complex Systems Informatics and Modeling Quarterly (CSIMQ)
eISSN: 2255-9922
Published online by RTU Press, https://csimq-journals.rtu.lv
Article 105, Issue 18, March/April 2019, Pages 47–64
https://doi.org/10.7250/csimq.2019-18.03

Deriving Cyber Security Risks from Human and Organizational Factors – A Socio-technical Approach

Thomas Richard McEvoy* and Stewart James Kowalski

The Norwegian Cyber Range, Department of Information Security and Communication Technology, NTNU i Gjøvik, postboks 191, NO-2802 Gjøvik, Norway

thomarm@ntnu.no, stewart.kowalski@ntnu.no

Abstract. Cyber security risks are socio-technical in nature. They result not just from technical vulnerabilities but also, more fundamentally, from the degradation of working practices over time – which move an organization across the boundary of secure practice to a place where attacks will not only succeed, but also have a significantly greater impact on the organization. Yet current risk analysis and management methodologies are not designed to detect these kinds of systemic risks. We present an approach, devised in the field, to deriving these risks – using a qualitative research methodology, akin to grounded theory, but based on preset coding descriptors. This allows organizational and individual behavior identified during interviews, observations or document research to be thematically analyzed, collated and mapped to potential risks, linked to poor working practices. The resulting risk factors can be linked together forming "risk narratives", showing how the degradation of working practices in one part of the organization can contribute to undermining its ability to respond to cyber security threats in another part of the organization.

Keywords: Human Factors, Socio-technical, Security Culture, Secure Behavior.

1 Introduction

While cyber attackers have been referred to as "sophisticated" – for instance, in [1] – the capability to cause massive public breaches of organizational security often seems to lie more with the incompetence of the organization attacked than with the cleverness of the attacker. Examples such as Wannacry [2] on the NHS in the UK, the attacks on Sony [3] and the failure of Singhealth [4] all point to fundamental failings in the organizations, not just the capabilities of the attackers, being at the root of the success of the attack.

Analogous to Rasmussen's view of safety in organizations [5] and the work of Leveson [6], we consider cyber security to be an emergent feature of organizational life, which arises from the

* Corresponding author

Reference: T. R. McEvoy and S. J. Kowalski, "Deriving Cyber Security Risks from Human and Organizational Factors – A Socio-technical Approach," Complex Systems Informatics and Modeling Quarterly, CSIMQ, no. 18, pp. 47–64, 2019. Available: https://doi.org/10.7250/csimq.2019-18.03

Additional information. Author ORCID iD: T. R. McEvoy – https://orcid.org/0000-0001-7322-4257, S. J. Kowalski – https://orcid.org/0000-0003-3601-8387. PII S225599221900105X. Received: 30 November 2018. Accepted: 14 March 2019. Available online: 30 April 2019.

integration of control and feedback systems (both human and technological) and which is degraded by pressures to economize on costs and to avoid heavy workloads; to which we would add, failures in organizational learning – such as unwillingness to pay reputational costs [7], [8]. Yet few current risk analysis and management techniques address these issues in a systematic way. They largely focus on the technical aspects of risks.

This is surprising. The security advantages bestowed by strategy and governance form part of a common body of knowledge encapsulated in standards such as CoBIT [9] and ISO27000 [10]. But the effects of failing to incorporate these standards into security governance, management and operations are not addressed by the majority of risk methodologies. Furthermore, there is no lack of material to draw on in terms of economic, cultural, social and cognitive factors leading to increased cyber security risks – for instance, [11]–[14] – however these human factors are almost completely missing in current approaches to risk analysis. Most human-centered risk controls, at best, focus primarily on policy compliance, training and awareness and the need to guard against the malicious insider [15], [16].

To address this gap, we present a practical approach, derived in the field, which incorporates qualitative research techniques with socio-technical and human factor analysis to derive cyber security risks. The goal of the approach is to determine where an organization's working practices either may degrade, or have degraded, to the point where its security boundaries are breached.

The approach widens the consideration of what constitutes secure behavior in organizations to include not just conformance to policy, behavior monitoring, or the institution of regular training and awareness sessions for staff, but also risk communication, emotional engagement in delivering on cyber security goals, ethical commitment, considerations for decision making, planning and investment for cyber security and relational dynamics. It arose out of the challenges raised by consultancy exercises, called *cyber vulnerability investigations*[†], for the healthcare and defense sectors in the UK in the light of recent attacks [2]. On the one hand, the approach had to present a scientifically valid methodology for tacking socio-technical and human factor analysis. On the other hand, it had to be applicable within the short time framework typical of a consultancy engagement.

The investigation methods employed are taken from established approaches to qualitative research [17], [18] making use of semi-structured interviews to capture data about the behavior of the organization and individuals within it.

This data is analyzed using an analytical framework which draws on work on risk communication [19], acceptance of technology (and, by analogy, security processes) [20], cognitive modeling [21], emotional responses [22], ethical engagement [23], [24], as well as recognized industry practice for security strategy, governance, management and operations [25], [26] and project management [27]. We also considered the known effects of economic de-investment in safety engineering [6], [19], which we apply, by analogy, to security. Finally, we considered the role of power structures and the distribution of cultural values in the organization [28]–[31]; including leadership and management and individual and team responses to leadership and management, which are seen as key components in establishing security culture [32].

The risks are derived by mapping a set of *descriptive codes* based on the framework with a set of ideal behaviors we considered an organization should pursue. Any patterns of behavior indicating a deviation from these ideals, detected by the analysis of the interview behavior (and marked using these codes), are predicted to result in one or more negative outcomes, which are likely to cause the organization to breach its own cyber security boundaries, or to make it more vulnerable to the consequences of such a breach.

Subsequently, based on the outcomes of these studies, we are able to make recommendations on risk mitigations which involve bringing behavior throughout the organization more in line with the proposed ideals.

[†] https://www.digitalmarketplace.service.gov.uk/g-cloud/services/535178601350759

Our approach offers an original contribution to the practice of risk analysis and management and provides practitioners with a means to supplement more technical analyses of risks with socio-technical and human factor perspectives on the resilience of the organization to attacks. At this point, we are not claiming that the framework is complete or fully validated. Rather, making use of the principles of design science, we see it as an evolving, but already useful, tool, which can be exploited both by practitioners to provide practical advice to organizations in dealing with risks as well as analyze the causes of incidents; and by scientists to develop their understanding of organizational vulnerability to cyber-attacks.

In *Literature Review* we provide a review of literature in the area. In *Problem Statement*, we set out the challenges which motivate our study. We describe our methodology in *Approach*, covering the background to our work and our assumptions, the risk model we propose and outlining the requirements for delivery in the field. We consider possible challenges to our work in *Discussion*. We draw some initial conclusions and set out our plans for further development in *Conclusions.*

2 Literature Review

Socio-technical systems analysis considers four aspects when analyzing organizations: Culture, Structure, Methods and Machines [29]. Furthermore, research in cyber security incidents has identified various social and economic factors contributing to security breaches by altering work practices, both in individual incidents [2], [33]–[35] and in academic research [11], [36]. But, surprisingly, common risk analysis and management methodologies do not appear to systematically incorporate these factors into their analysis. Instead, they focus on normative management and the application of technical controls [37]. In other words, most risk analysis and management methods are strongly techno-centric and deal primarily with *Machines* in their analysis; and, to some extent, with *Structure*. But their coverage is not complete, since they give little consideration to *Culture* beyond recommending regular training or *Methods*, beyond considering policy conformance [38]. But this approach would fail to identify potential design errors in security procedures or systems [14] – in particular relating to human factors and how people learn in organizations [14].

Parallels with experience in safety engineering are instructive. Complex socio-technical systems break down due to lack of integration and failures to maintain working practices [5], [6]. The design of systems can incorporate the potential for exponentially damaging incidents due to their complex, non-linear and closely coupled nature [39]. In the safety industry, this approach leads to the consideration of a variety of approaches and techniques in relation to complex systems analysis, for instance, [40]: but this appear to be missing, or are, at best, only partially covered by cyber security methodologies for dealing with risk prediction and incident analysis.

This does not mean that socio-technical issues are not addressed in the literature. But simply that this literature appears to be largely ignored in designing or using risk analysis and management methodologies[‡]. The international standard for the creation of such methodologies only considers the components which need to be delivered, not the subject areas which need to be considered [21].

Considering each of the four main aspects of socio-technical analysis – *Culture* has been addressed by several researchers. Schein defines culture in terms of artifacts (e.g. processes), espoused values and shared tacit assumptions; to which Niekerk & Von Solms have added a fourth factor "information security knowledge" [12], [41]. This model is used to design cultural change programs. However, this assumes that senior managers can diagnose the issues correctly and are not part of the problem. Schlienger & Teufel treat information security culture as a problem rooted in processes where the individuals' conformity to security policy determines the

[‡] Consultation with an experienced colleague led to the conclusion that some methods such as NIST (https://www.nist.gov/cyberframework) and IRAM (https://www.securityforum.org/) do make use of socio-technical factors in theory, but not in practice.

maturity of the security culture [15], [38], [42]. But this assumes that the security policy is considered correct when it may have resulted from an incomplete analysis of organizational and technical factors and may, in fact, contribute to security failures[§], introducing both human and technical vulnerabilities simultaneously. Other approaches, more closely related to ours, treat security culture as a multi-factor problem requiring action at different organizational levels [43], or as arising from mental attitudes and models, which could be changed by the context of security questions or the ethnicity of the organization [30]. The most common approaches to security culture and awareness in practice, however, seem to be actively hostile to individual users, regarding them, at best, as lazy and incompetent and, at worst, as a source of threats [13]. This is the approach demonstrated in most risk analysis methods.

We regard culture as an inter-subjective process in which all members of an organization participate and contribute to by reiterating its structures in daily interaction [31], [44]. Cyber security issues therefore arise from these repeating patterns of behavior or *figurations* [45] and these we seek to analyze in our approach.

Methods, in security terms, cover security and operational management, software development, security policy enforcement, and aspects such as data privacy. For risk analysis and management purposes, this topic is usually addressed using control sets in risk analysis to identify security gaps such as concerned in ISO27002 [10], or by reference to compliance frameworks such as PCI-DSS. The area is usually more generally addressed in the discipline of enterprise architecture using methodologies such as SABSA [26] or TOGAF [46], which analyze security at different levels of organization and seek to integrate its provision with business goals in a way which is close to socio-technical approaches. Active research in the area tends to concentrate on issues with standards, or on reconciling approaches – for instance, [47].

Structure is addressed by cyber security strategy and governance with a view to senior management responsibilities. Again, this is addressed in approaches such as SABSA [26] and management frameworks such as CoBIT [9] which seek to establish normative behavior. Research in the area tends to concentrate on the design of suitable governance structures and the need for governance [48]. Most research and practice guidance is more IT focused than specific to security – with some exceptions [10], [25]. It should also be noted that research rarely considers wider factors such as government policy or the development (or failure) of regulatory regimes rarely come into play [6].

Our approach represents an attempt to select factors which can be shown to be immediately relevant to cyber security (either directly or by analogy) from historical experience and which are measurable by a variety of means, allowing for cross validation of interview data. The factors are chosen from a number of fields, including communication techniques, cognition, emotional response, strategy and planning, project management, security investment and power dynamics in organizations. Hence, we cover human and organizational rather than technical factors, not focusing on *Machines*, but on *Methods*, *Structures* and *Culture*, seeking to plug the apparent gap in practice. The approach is, therefore, intended to be complementary to current risk methodologies and aid in identifying underlying causes behind technical or procedural flaws which give rise to security vulnerabilities, directly or indirectly.

Our decision to approach the interviews using social science research techniques was primarily based on maximizing trust between the interviewees and the interviewers – seeking to make the interview as open and friendly as possible to ensure maximum information about potential security flaws. This was naturally underpinned by a strong ethical commitment to confidentiality [17]. This contrasts with more directed interviews usually conducted by consultants auditors [49] which we assumed might cause interviewees to become defensive and hide salient accounts of behavior.

Our technique does not (yet) make use of quantitative analysis – testing hypotheses regarding the organization. This awaits future development. But it should be recognized that both

[§§] http://www.bbc.co.uk/news/technology-40875534

qualitative and quantitative approaches to assessing security culture and organizational behavior are recognized in the literature [42] which have different advantages and disadvantages. In general, questionnaires with scales (e.g. Likert) being subject to statistical analysis allow hypothesis testing, but may miss richer contextual data which qualitative research allows to be gathered [17]. However, the methods are not exclusive; and both could potentially be applied in our approach [50].

Our approach contributes to risk analysis and management as it is a novel approach to deriving risks from both socio-technical and human factor analysis (in combination); but it does not represent a complete methodology – rather it is a complementary approach. ISO27005:2008 is a meta-framework used for guiding the selection of risk analysis processes [21]. It shows the stages for risk analysis and management which can be broken down into several activities (Figure 1). We consider our approach to fall into the category of *risk identification* techniques. It allows various risk factors – threats, vulnerabilities or impacts – to be elicited and built into a more complete analysis in combination with other studies.

3 Problem Statement

The challenge of developing an approach to cyber security risk analysis and management which incorporates socio-technical systems analysis and human factors is twofold.

First, there is a practical need in the field to meet new requirements in the defense sector, where the need has arisen for multi-faceted security assessments of security targets – described as *cyber vulnerability assessments*[**] – and to meet similar requirements, where cyber security has taken priority due to the Wannacry attack.

The second is that no specific risk methodologies exist in the field to carry out this kind of tasks. A review of commonly used methodologies for risk analysis and management [37] showed that, while some methodologies (such as IRAM and SABSA) do address several organizational and cultural concerns (such as the political landscape, balancing business and security goals in designing technologies and procedures, and regulatory requirements), no methods currently consider systems integration, control and feedback loops, and organizational learning, on the one hand, and the potential or actual degradation of working practices to the point of security failure, on the other hand. This contrasts with socio-technical systems analysis approaches in, for instance, safety engineering [6], [40].

This led to the following set of requirements stating that the methodology:

1. Must be deliverable over 10–15 working days.
2. Must address local security concerns about the sensitivity of the data.
3. Must address ethical considerations regarding the anonymity of participants.
4. Must be credible to stakeholders and continue to be credible to stakeholders during ongoing reviews of the work and its outputs.
5. Could incorporate socio-technical or human factors or both.

The fourth requirement could also be interpreted to mean that the approach should be demonstrably scientifically valid as well as make sense in practical business terms.

4 Approach

The approach taken consists of three parts. First, we need to establish a sound theoretical basis for our study which we do in the subsection on *Background and Assumptions.* This meets Requirements 4 and 5 (see Section 3) and forms the foundation of the remainder of the work. Second, in *Risk Model*, we describe how we derived our analytical framework and how it can be used to elicit risks, based on interviews, document analysis and observation exercises. Third, in

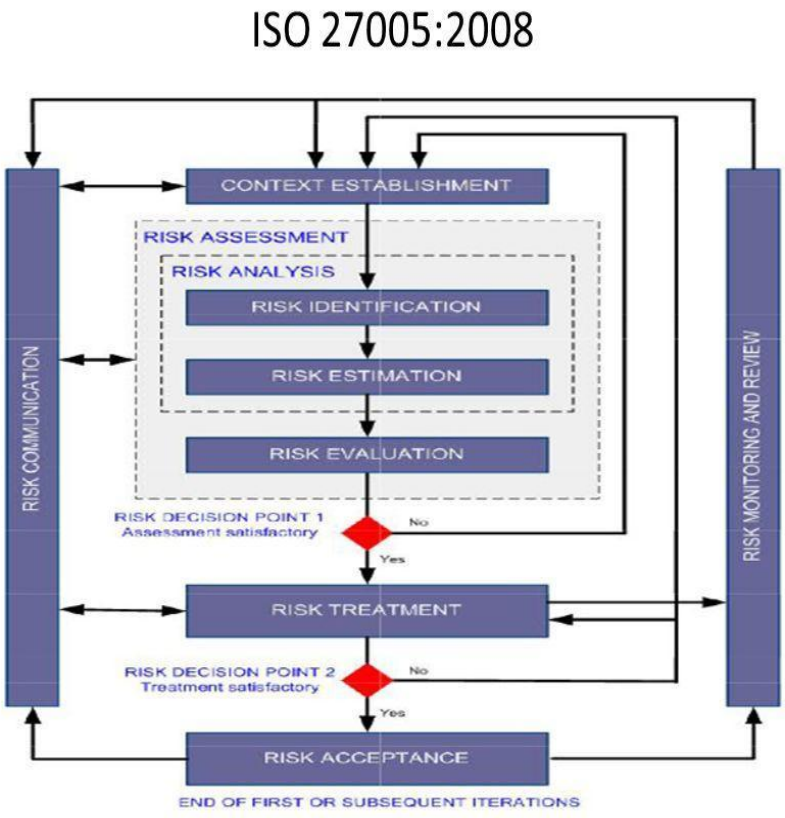
[**] https://www.digitalmarketplace.service.gov.uk/g-cloud/services/535178601350759

Field Delivery, we describe the application of the method in the field and how we met the rest of requirements set out in the *Problem Statement* in Section 3.

4.1 Background and Assumptions

In terms of risk analysis and management, our approach is based on ISO27005 [21] – see Figure 1. In terms of this recognized standard, our approach does not represent a complete methodology at this stage but provides an approach to risk identification and providing recommendations for risk mitigation. In line with the recommendations of this standard, our approach is supported by frequent feedback to the client regarding our methods and our findings – in support of Requirement 4 (see Section 3).

To incorporate the additional steps of risk analysis, evaluation and risk treatment into our approach, we recommend the methods outlined in SABSA [26]. This is not shown but requires additional consideration of the extent to which human factors identified represent increased vulnerability to attacks. In particular, our approach provides useful considerations during the creation of threat scenarios.



.

Figure 1. Risk Analysis Flowchart – based on [21]

In terms of socio-technical systems analysis, we start from the basis provided in Rasmussen [5] for safety engineering, but re-working the concept for cyber security. Hence we regard cyber security as an emergent property of the interaction of all parts of a complex socio-technical system (see Figure 2) underpinned by control and feedback loops between the layers of the system [6].

Working practices in this system provide for its cyber security, protecting it from active threats, but these practices are subject to continual erosion due to changes to working practices at each layer and throughout the system under the dual pressures of cost and labor efficiencies which may result in the cyber security boundary of the organization being breached. To these pressures, we would add barriers to organizational learning [8] such as failures to take account of

threat intelligence, new technologies or paying the reputational costs of admitting the need for cyber security improvements [7] as well as simple organizational inertia.

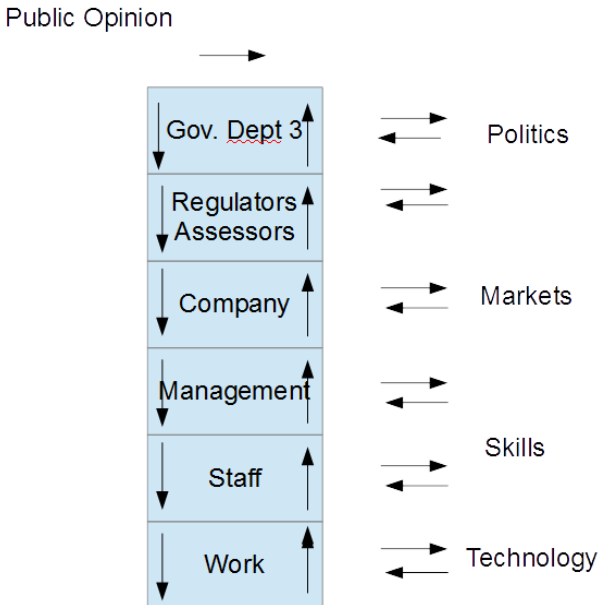


Figure 2. A Complex Socio-technical Organization (adapted from [5])

This leads to the model of cyber security breaches shown in Figure 3 where the degradation in working practices pushes the working practices over its invisible cyber security boundary resulting in potentially catastrophic failures.

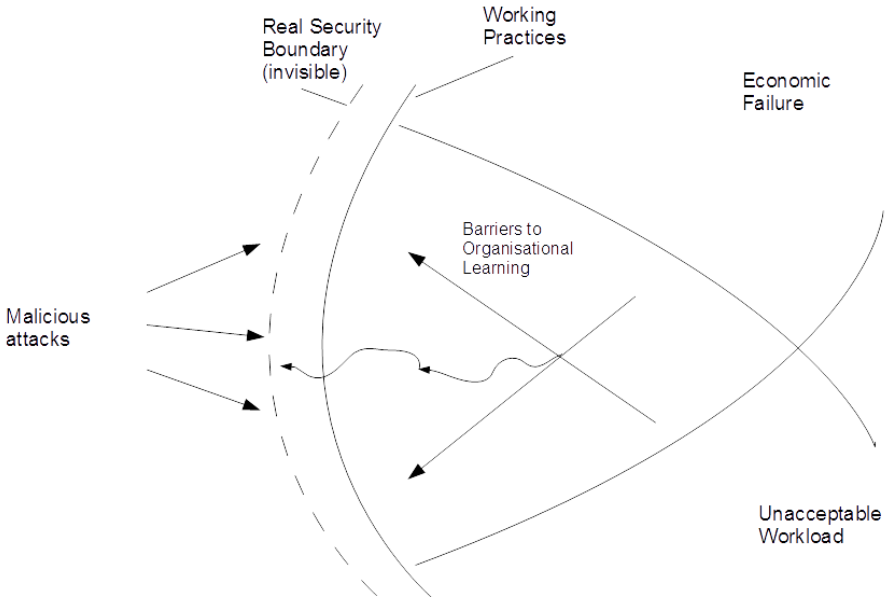


Figure 3. Breaching the Cyber Security Boundary (adapted from [5])

A second consideration is that a socio-technical model should provide coverage of four factors: culture, structures, methods and machines – shown in Figure 4.

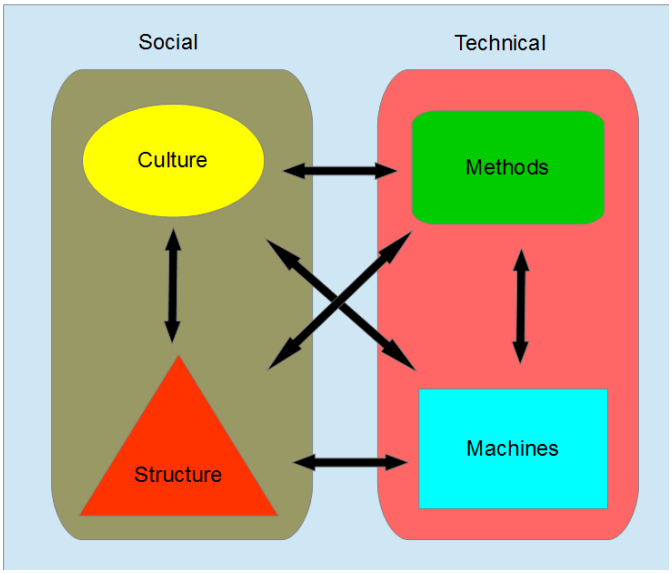


Figure 4. Socio-technical System [51]

Machines refers to the technology employed by the organization; *Methods* to the processes and procedures used in relation to technology, *Structure* to how the organization is arranged – including both formal and informal authority structures – and *Culture* to the behavior of individuals and teams in the organization.

Our risk elicitation approach places the emphasis on the human and organizational aspects of socio-technical systems (i.e. culture, structure and methods) rather than technology (machines). We assume that technical risk analyses will adequately cover the cyber security requirements for technology deployed by organizations. However, we make use of *risk narratives* to allow us to incorporate the human and organizational aspects with technical risk scenarios. For instance, when considering the risk of a distributed denial of service (DDoS) attack, we take account not only of the organization's technical preparedness (deployment of network defenses such as NextGen firewalls and third party DDoS prevention services) but also the preparedness of its management and operational teams to deal with the incident. The use of risk narratives allows us to regard our approach as complete in socio-technical terms.

Additionally, our approach allows us to incorporate human factor analysis into our thinking. For instance, we consider the use of cognitive factors such as effects of security controls on work performance [20] and individuals' mental models of systems [30].

In terms of analysis of culture, we need to make an important distinction between our approach and approaches used by others.

Culture has been addressed by several researchers. But their assumptions seem to be founded in addressing the attitudes and beliefs of individuals (see Section 2). In our approach, we define organizational culture as repeating patterns of thought, feeling and behavior demonstrated by *groups of people* –

> "The way our minds are programmed that will create different patterns of thinking, feeling and actions for providing the security process" [30].

Or, more bluntly,

> "the ways things are done in an organization" [52].

So, we do not regard organizational culture as something reified, which leaders and managers can stand outside of and design in line with Schein's recommendations [31], [41], but as an inter-subjective process in which all members of an organization participate and contribute to by reiterating its structures in daily interactions [31], [44]. This is a key consideration because it

means that culture is then *treated as a pervasive phenomenon which affects performance in every other area under consideration*. It is the patterns of behavior which arise as a result of these interactions which we are primarily interested in observing, analyzing in terms of their effects on the cyber security capability of the organization and, where negative, in predicting the likely cyber security consequences of performance failures.

4.2 Risk Model

Our risk model consists of a *descriptive coding* framework [53] which allows negative organizational and individual behaviors to be identified and mapped to risk factors – including threats, vulnerabilities and impacts – in relation to business goals and recommendations to be made for mitigating the discovered vulnerabilities or impacts. This is combined with technical risks (identified separately) to form risk narratives leading to recommendations for mitigation. The overall approach is shown in Figure 5.

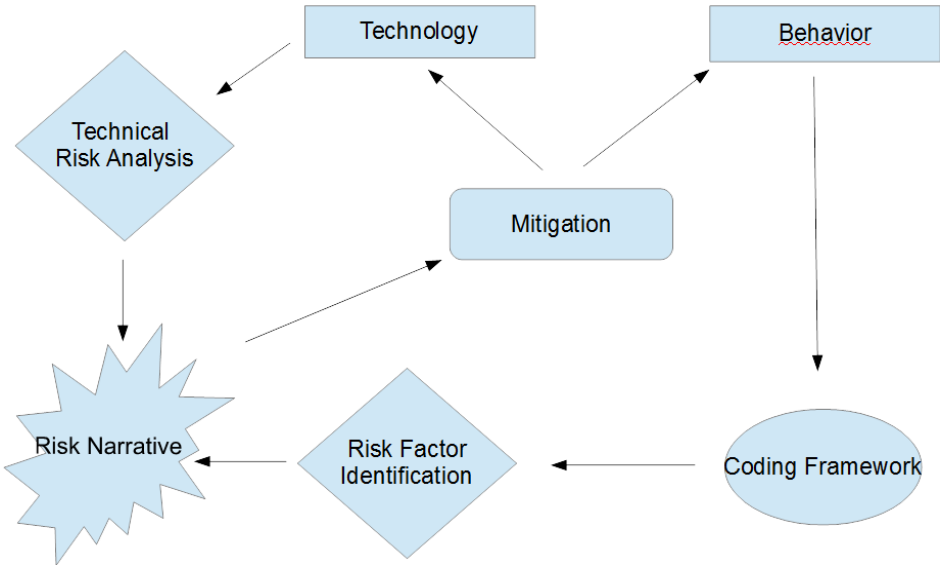


Figure 5. Overall Risk Analysis Approach

The model divides into six areas, shown in Table 1. To create the model, we called on known research frameworks from social science and technology and safety engineering.

We considered the need for IT and security professionals to be trained in technical and professional communication techniques and engage in communication planning in line with lessons learned from safety engineering practice [19]. We also considered lessons learned about the need for completed control and feedback loops from [6].

We incorporated research into technology (in this case, security) adoption (UTAUT) [20] which considers aspects such as perceptions of the effects of security on systems performance and work effort and the social influence of peers, experts and managers. We also used mental models of cyber security and attitudes to risk [30].

Emotional response to security issues was considered important (PAD) [22] as we wanted staff and managers to be engaged seriously with it. A part of this consideration was their ethical engagement [23], [24] with security matters.

Good practice in cyber security management, governance and operations [25] as well as the place of cyber security strategy and enterprise security architecture [26] were regarded as central. But we also focused on how this was implemented in practical terms, considering project management [27] and investment in the provision of cyber security materials and capability by analogy with safety engineering practice [6].

We validated this crossover through considering examples of individual incidents [2], [33], [35], [54][††].

Finally, we considered the role of power structures and the distribution of cultural values in the organization [28], [29], [31]; including leadership and management and individual and team responses to leadership and management, which are seen as key components in establishing security culture – [32]. This resulted in the framework set out in Table 1 which provides an overview of the areas of behavior under consideration: communication, thinking, engagement, investment, planning and processes, and ways of working.

Table 1. Areas of behavior

Area	Description
Communication	The capability of staff to communicate with management about risk, both formally and informally.
Thinking	How people think about security and what influences their thinking.
Engagement	The emotional and ethical responses to acting on cyber security issues.
Investment	The level of resources dedicated to cyber security.
Planning & Processes	What security processes are in place and how well are they executed.
Ways of Working	How employees, teams and managers relate to one another on the subject of cyber security.

4.3 Risk Model Details for Communication Area

To show the risk model applicability, we take one of the areas – communication – and break it down into its component codes (descriptors). Each code is associated with a set of ideal behaviors – see Table 2.

Each code is also associated with a statement of the likely effects of a deviation from the described ideal behavior. We show an example of this in Table 3 for failures to train key staff in technical and professional communication. Where possible, we include real life examples of the effects of deviations from ideal behavior to validate our analysis.

Finally, in Table 4, we give an example of recommendations which could be provided in order to address the poor behavior, although actual recommendations may depend on the context of the organization.

All areas depicted in Table 1 are treated along similar lines.

Our risk model allows risk factors to be identified and is suggestive of potential countermeasures. But the approach does not directly map to threat, vulnerability or impact levels or link to technical risks, allowing risks to be evaluated in terms of their relative priorities or quantitative impacts. Rather the consultant, applying the method, must make an evaluation of how the risk factor affects the organization and its security capability.

Risk narratives are iteratively built up from factors identified during interviews. This is not just a matter of listing the potential risk factors in the model, but translating these into industry, organization and even team, or system, relevant examples and demonstrating systemic links between the factors, based on knowledge of the organization and its technology. Several iterations may be needed as additional links are identified.

These *risk narratives* are built up by demonstrating how behaviors conjoin to reinforce the likelihood of impacts being realized or exposure to specific threats increased. Furthermore, where security breaches are already occurring, such narratives can provide underlying causes which need to be addressed in addition to the actual breaches.

For instance, one organization had clearly invested heavily in ensuring that professional quality online training was in place for the staff. But, without active reinforcement of training by other means (e.g. on the job training, gamification of lessons), the response was one of ennui ("click to pass"). The risk narrative revealed how cyber security measures for training and

[††] https://www.risk3sixty.com/2014/12/19/the-sony-hack-security-failures-and-solutions/

awareness and the actual cyber security culture contradicted each other. This, in turn, increased the likelihood that staff would fall foul of phishing attacks and breach the security barrier by downloading malicious software by clicking on web links where these had not been dealt with effectively by the current web filtering mechanism.

Table 2. Communication: Ideal behaviors

Communication	Ideal Behaviors
Technical & Professional	(1) Organizations should train all key security staff and responsible managers in written, graphical and spoken technical and professional communication techniques. (2) For some forms of communication (e.g. training and awareness materials), organizations should consider employing third party service professionals. (3) Staff with responsibilities as influencers should be able to make use of rhetorical strategies to make their messages both logical and persuasive and geared to the audience. (4) This approach should be backed by quality reviews and audience testing (where feasible). (5) Communication should be multi-channeled to maximize engagement.
Planning	(1) Communication planning ensures the effective communication with relevant parties in a timely fashion. (2) Formal roles and responsibilities should be assigned to ensure that communication channels exist with the key managers and staff. (3) There should be a plan in place for cascading important cyber security communication throughout the organization. (4) There should be a communication plan in place for communicating during cyber security incidents between responders and key stakeholders. (5) Technical means of communication should be tested, and contingency options agreed to deal with any technical breakdowns in normal communication channels. (6) A formal policy framework with associated procedures, standards, guidelines and working practice instructions is a key feature of planned communication. (7) Planning should include communication to partners, suppliers and clients.
Control & Feedback	(1) Managers and operators should have a clear mental model of how the organizational units and systems they are trying to control contribute to business and security goals. (2) The set of instructions and feedback messages to carry out work on systems should be complete and directly informative (e.g. they should not just state that an instruction has been given but that it has been completed and what the result is). (3) Feedback should be lateral to other organizations as well as vertical within the same organization where required.
Common Language	(1) The organization makes the use of an approach to risk analysis and management results of which are commonly understood by both sides. (2) Managers have been trained in a course which provides cyber security awareness targeted specifically to their requirements and provides them with key vocabulary. (3) Senior operational staff have an appreciation for how the management team operates and what information they need to see. (4) Status reports and presentations are in an agreed format where the significance of each item is understood.

Similarly, in another organization, a lack of coordination between different security parties combined with poor communication planning and a narrow mental model of security (excluding many cyber components) resulted in a contingency plan which did not account for ordered response and recovery to a large-scale cyber-attack such as ransomware, or DDoS. These kind of events clearly would cause serious impact to the organization's business operations But the organization had not taken account of either the need to address communication during such attacks, nor was it planning to install technical defenses against these kind of attacks. Both are key to surviving these kinds of threats.

A third example is a regional health body which provided IT services both centrally and within each of the organizations that used the service. This led to a dissipation of resources and efforts which was inefficient on two levels. First, it meant that each IT team repeated work done by other teams. Second, a single larger central spend would have led to more cost-efficient solution provision – even though the central solution would cost more than each of the individual solutions.

Table 3. Impacts of neglecting training in technical and professional communication techniques

Communication	**Deviation**
Technical &Professional	• Failure to make use of technical and professional communication techniques by management may undermine their capability to give clear security messaging to staff. • Failure to train key staff is likely to lead to messages about risk being misunderstood by management.
Impacts	• Decision making by staff may be faulty due to misunderstanding management intentions. Decision-making by management may be faulty or delayed if messages about risk are misunderstood. • Other parties will fail to understand the significance of communications from the organization. • Organizational learning will suffer because work instructions may not be clear and the significance of information about cyber security risks or issues may be missed by managers. • Miscommunication can open gaps in processes to malicious attackers and they may be able to take advantage of unclear instructions during social engineering attacks. • Breakdowns in communication are frequently the cause of conflict within organizations and more so across organizational boundaries. They can have unexpected effects on how organizations respond to information which may negatively affect working practices. • Where vital messages are lost in translation, the security boundary is likely to be breached. • Other organizations may further distort unclear messages through their own poor communication channels, increasing the effects of the deviation.
Real World Example	One of the factors identified in the failure of Sony to protect its confidential data assets was that its policies were unclear about the sensitivity of certain types of data.

Table 4. Communication: Mitigations

Communication	**Recommendations Regarding Failures in Technical and Professional Communication**
Mitigations	• Train key security and technical staff in technical and professional communication techniques and ensure their continued use through quality reviews and recipient testing. • Review all current documentation (e.g., policies, procedures, standards and guidance) and ensure that it meets guidelines for clear communication such as use of natural language and document design. • Ensure that key messages are communicated using multiple channels e.g. follow up emails with phone calls or phone calls with face to face meetings. • Include rhetorical training for managers who are expected to present key security messages to the board.

5 Delivery in the Field

Our proposals for the delivery of the methodology are based on our experience of the early trials in UK defense and health sectors.

5.1 Interview Approach

Returning to the study requirements (see *Problem Statement*, Section 3), the approach outlined satisfied the requirements in terms of scientific and business credibility – drawing on known research or practice forming part of the common body of knowledge for cyber security and incorporating both socio-technical and human factors. The credibility of the approach was underlined by holding preparatory meetings with the stakeholders and presenting the approach as well as providing interim reports on progress and findings.

The selection of a qualitative research approach was based, in part, on the requirements to deliver the project within the tight timescales (10–15 days) which we were given. Given a longer period of time, it might have been possible to fully factorize the risk framework and provide a quantitative rather than a qualitative analysis of risks – although it might have been useful to precede the quantitative analysis with a qualitative phase of study in order to form hypotheses about the cyber security posture of the organization – similar to the approach used in [50].

The second reason for selecting a qualitative research approach was the nature of the interviews. Normally, in consultancy and audit work, a diagnostic interview approach is used where the interviewer starts from an open question and then delves into the detail of the response with a series of follow up questions [49]. However, we wanted to steer away from this approach because we assumed that the sense of being "audited" would cause interviewees' defensive attitude and thus might close off some lines of enquiry. Instead, we chose to make use of semi-structured interviews. This changes the power dynamics of the interview, making it more friendly, open and free flowing [17]. Underpinned by a strong ethical commitment not to reveal the sources of our information about the organization, we expected this approach would elicit more information than a traditional consultancy style of interviewing. This approach is also congruent with classic qualitative analysis research techniques, which further underlined the credibility of our interviewing method.

Security concerns were addressed by ensuring the laptops we used for note taking, analysis and reporting were encrypted and secured against theft; and by carrying out investigations face to face rather than using telecommunications. We also agreed not to record interviews – although this would be normal practice in social science research – and instead substituted the use of two consultants to ensure that the transcription of the interviews was as close to verbatim as possible.

The interview process followed the practice set out in [18]:

1. "The interviewees are selected in line with the criteria which match the research purpose" – in this case, selecting at least three interviewees from senior management, from operational management and from staff roles.
2. "The interviews are conducted, if appropriate, using the coding framework." We made use of Saldana [53] to help us create a coding framework guiding for the structure of the interview but avoiding set questions.
3. "The interviewers conduct the interviews in a friendly and open fashion to encourage the elicitation of facts."
4. "Ideally, the interviews are recorded." (This step may be omitted for security reasons).
5. "Where the interviews are recorded, they are transcribed." (Or two interviewers may recreate the interview from notes).
6. "Following transcription or note-taking, the interviews are coded, and analytical notes are taken."
7. "The coding and analytical notes are subject to secondary (or even tertiary) analysis to draw out the themes."
8. "Once the thematic analysis is completed, the researchers seek to draw conclusions from the data."
9. "On the basis of the findings (and other sources of information) make recommendations to the company based on the conclusions."

Once risks have been identified using the thematic analysis of the interview material, further evidence can also be sought through observation exercises or by reviewing documentation – including policy, procedures, standards and guidance, emails, reports and financial data.

In addition, as stated above, other technical risk analysis approaches can supplement the human factors study providing further evidence of damaging effects or examples of deviations from ideal behavior.

These supplementary sources of evidence mitigate the potential criticism that the material produced is purely the result of subjective opinion on the part of the researcher or the interviewees. This approach allows the method to compensate for the lack of quantitative evidence to support hypotheses.

5.2 Coding Method

There are various ways of labeling interview and other data from qualitative studies in accordance with the themes found in them (known as *coding*). The coding methods vary by the experience and purpose of researchers [53].

In our method, the consultants doing the work, while experienced in cyber security, were not trained in social science research techniques (though they were familiarity with various interviewing techniques). In addition, the codes along with the analytical notes had to be mapped to a more or less fixed set of deviations and associated risk factors.

These considerations narrowed the selection of coding methods down to a single candidate, *descriptive coding*, which makes use of an agreed set of codes and is suitable for the use by novice researchers.

The chosen approach allows the consultants to focus on analyzing the interview transcriptions to uncover behaviors which it has already been agreed are negative and to focus on the mapping exercise and the risk identification and management processes. Starting from principles e.g. using grounded theory [53], would otherwise add considerable time to the process and still might produce inconsistent results.

6 Discussion

In this article our primary contribution is to provide a novel qualitative approach to investigating and mapping behavioral patterns to socio-technical risk factors and to use these to build cumulative and systemic risk narratives, showing how specific behaviors have the potential to push organization's working practices across its security boundary, leaving it exposed to malicious attacks.

The approach is solidly rooted in social science research methods, but does not require extensive training in social science, to be put into practice. This makes it easy for organizations with consultants skilled in information security, which are unlikely to have training in the social sciences, to adopt these methods. The approach draws on a long history of validated social science research as well as a common body of cyber security knowledge built up on commercial and industrial experience.

The method is not intended to be a complete risk analysis and management methodology but to be used in conjunction with other compliance frameworks and technical studies. It provides a potential basis for understanding why gaps revealed by other approaches exist in the organization, allowing underlying causes to be addressed.

There are some potential challenges to the approach. Using qualitative investigation techniques could be seen as subjective. But it is easy to validate any claims made from interview findings, using other evidence. For instance, even a small sample of documents shows how prevalent good technical and professional communication is. Cyber security spending commitment can be demonstrated from accounting records. The only constraint is the time given to conduct the analysis.

Another challenge is the number of interviews is not "representative", i.e. that insufficient data points have been taken. This challenge arises from a category error, seeking quantitative validation of the data. Qualitative interviews seek to build a "rich" picture of the organization from multiple layers [17]. The aim is to derive "meaning", i.e. the underlying beliefs and attitudes of the organization, rather than testing a statistical hypothesis [18]. This fits to the cultural nature of our study in the sense we defined it in *Background and Assumptions* (Section 4.1). Furthermore, it is possible, if requested, to follow up the initial investigation with a quantitative analysis, based on the same analytical framework, of the organization's security posture [50].

It could also be asked why we did not consider ergonomic studies during our work. Such studies might be recommended. Furthermore, it would be possible to expand the framework to include additional factors such as ergonomic considerations, if required.

A further challenge to the method is that the "ideal" behavioral profiles and associated codes and risk mappings are not fully validated. Our primary response is that our approach is based in design science [55] – that is, we are seeking through practical trials to develop a suitable artifact for deriving socio-technical and human factor risks. But we also consider that the research areas we have drawn on in forming our framework – the disciplines of safety engineering, organizational theory and information systems research as well as the common body of knowledge regarding cyber security practice – provide a firm theoretical foundation for our research. Further work in the area will allow us to refine and, if necessary, augment our model to support our purpose.

In terms of delivery techniques, it could be asked if we selected the appropriate methods. To some extent, of course, any choices are driven by stakeholder requirements, which are likely to include budgetary and resource constraints. Where these are tight, the social science research approach we propose would seem most appropriate, allowing 7 to 15 interviews to be conducted over the period of 10 to 15 days with full analysis and reporting. But other customers may prefer a quantitative approach or a different approach to deriving the qualitative data such as the use of auto-ethnography by selected staff.

We should also consider whether a semi-structured interview does provide the best interview format. A diagnostic interview may be more culturally appropriate to the situation, where a semi-structured approach may put some interviewees outside of their "comfort zone".

7 Conclusions

It is taken as a truism that cyber security attacks are growing in capability and sophistication, but even the most cursory assessment of successful attacks is more an indicator of incompetence of defending organizations.

We have described a practical approach which allows poor working practices in organizations to be mapped to cyber security risk factors using an ethnographic approach based on qualitative research methods. The method consists of a small set of investigative interviews, supplemented by desktop research, which are analyzed thematically using a descriptive coding framework.

Each of the codes maps to an ideal cyber security behavior and any deviations from this behavior are considered to result in increasing exposure to threats in terms of either vulnerability or impact on the organization and its business goals. Concrete examples of the potential effects of deviations are provided as an inspiration to the risk analyst.

Each of the risk factors identified is considered individually and cumulatively, allowing the risk analyst to build up a chain of potential consequences, linking them where possible to technical risks, which we label a 'risk narrative', out of which the analyst can develop a practical set of mitigations to reduce the human and organizational aspects of risk.

The approach was developed in the field as a practical response to the challenges raised by 'cyber vulnerability investigations' in the defense and health sectors. As such, it is designed to be used by cyber security consultants who do not have training or exposure in social science

research methods, drawing on approaches which have been found to be useful with novice researchers. The method is also cost-effective because it can be carried out in a short period of time by a small number of consultants.

Future work will focus on the following areas:

- Validating the selection of factors,
- Developing archetypal risk narratives,
- Gamification,
- Trialing different forms of delivery.

The combination of factors, although each of them are selected from validated frameworks or fields of knowledge, may not be fully correct. So, we need to consider not only experiences from ongoing studies to determine whether the factors used are relevant to work practices, but also consider refining the approach using theoretical models of risk exposure and by hypothesis testing, using quantitative approaches.

The risk narratives, which we "discovered" during the investigations we carried out, seem to be a common feature of socio-technical investigations – for instance, [14] – and reflect the discovery of archetypal system dynamics [56]. We would like to investigate these further and enrich our picture of risk exposure beyond considering risk factors in isolation or pursuing the intuitions of risk analysts to a systematic approach to predicting risk figurations [45] in organizations.

We also wish to experiment with different delivery formats. For instance, the use of diagnostic interview techniques, using recording equipment (where feasible) and transcribing interviews, and making use of auto-ethnographic sources of data about the cyber security posture of organizations.

Finally, we believe that our approach can be adapted to training consultants and managers to consider and address socio-technical factors during cyber-attacks. So, we hope to incorporate our work into ongoing research into gamification of cyber security risk training as part of developing the Norwegian Cyber Range[‡‡].

References

[1] N. Virvilis, B. Vanautgaerden, and O. S. Serrano, "Changing the game: The art of deceiving sophisticated attackers," *Cyber Conflict Proceedings (CyCon), 2014 6th International Conference* IEEE, pp. 87–97, 2014. Available: https://doi.org/10.1109/CYCON.2014.6916397

[2] J. M. Ehrenfeld, "WannaCry, Cybersecurity and Health Information Technology: A Time to Act," *Journal of Medical Systems*, vol. 41, pp. 104, 2017. Available: https://doi.org/10.1007/s10916-017-0752-1

[3] H. Berghel, "Cyber chutzpah: The sony hack and the celebration of hyperbole," *Computer*, vol. 48, no.2, pp. 77–80, 2015. Available: https://doi.org/10.1109/MC.2015.41

[4] K. Ramakrishna, "The Advent of "CyWar": Are We Ready?" RSIS Commentary, 2019.

[5] J. Rasmussen, "Risk management in a dynamic society: a modelling problem," *Safety science*, vol. 27, no. 2–3, pp. 183–213, 1997. Available: https://doi.org/10.1016/S0925-7535(97)00052-0

[6] N. Leveson, *Engineering a safer world: Systems thinking applied to safety*, MIT press, 2012. Available: https://doi.org/10.7551/mitpress/8179.001.0001

[7] A. Cassano-Piché, K. J. Vicente, and G. A. Jamieson, "A sociotechnical systems analysis of the BSE epidemic in the UK through case study," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, SAGE Publications, pp. 386–390, 2006. Available: https://doi.org/10.1177/154193120605000337

[8] B. H. Kleiner and W. A. Corrigan, "Understanding organisational change," *Leadership & Organization Development Journal*, vol. 10, no. 3, pp. 25–31, 1989. Available: https://doi.org/10.1108/EUM0000000001137

[9] J. W. Lainhart IV, "COBIT™: A methodology for managing and controlling information and information technology risks and vulnerabilities," *Journal of Information Systems*, vol. 14, no. s–1, pp. 21–25, 2000. Available: https://doi.org/10.2308/jis.2000.14.s-1.21

[10] A. Calder and S. G. Watkins, "Information security risk management for ISO27001/ISO27002," It Governance Ltd, 2010.

‡‡ https://www.ntnu.no/ncr

[11] R. Anderson and T. Moore, “Information security economics – and beyond,” *Advances in Cryptology – CRYPTO 2007. Lecture Notes in Computer Science*, vol. 4622, Springer, pp. 68–91, 2007. Available: https://doi.org/10.1007/978-3-540-74143-5_5
[12] J. Van Niekerk and R. Von Solms, “Information security culture: A management perspective,” *Computers & Security*, vol. 29, no. 4, pp. 476–486, 2010. Available: https://doi.org/10.1016/j.cose.2009.10.005
[13] A. Adams and M. A. Sasse, “Users are not the enemy,” *Communications of the ACM*, vol. 42, no. 12, pp. 40–46, 1999. Available: https://doi.org/10.1145/322796.322806
[14] D. Botta, K. Muldner, K. Hawkey, and K. Beznosov, “Toward understanding distributed cognition in IT security management: the role of cues and norms,” *Cognition, Technology & Work*, vol. 13, no. 2, pp. 121–134, 2011. Available: https://doi.org/10.1007/s10111-010-0159-y
[15] T. Schlienger and S. Teufel, “Analyzing information security culture: increased trust by an appropriate information security culture,” *Proceedings of the 14th International Workshop on Database and Expert Systems Applications*, IEEE, pp. 405–409, 2003. Available: https://doi.org/10.1109/dexa.2003.1232055
[16] C. W. Probst, J. Hunker, M. Bishop, and D. Gollmann, *Insider threats in cyber security*, Springer, 2010. Available: https://doi.org/10.1007/978-1-4419-7133-3
[17] S. Kvale and S. Brinkmann, *Interviews: Learning the craft of qualitative research*, California, Thousand Oaks, CA: Sage, 354 p., 2009.
[18] S. Ladner, *Practical ethnography: A guide to doing ethnography in the private sector*, Routledge, 2016.. Available: https://doi.org/10.4324/9781315422251
[19] C. Boiarsky, *Risk Communication and Miscommunication: Case Studies in Science, Technology, Engineering, Government, and Community Organizations*, University Press of Colorado, 2016. Available: https://doi.org/10.5876/9781607324676
[20] L. Oshlyansky, P. Cairns, and H. Thimbleby, “Validating the Unified Theory of Acceptance and Use of Technology (UTAUT) tool cross-culturally,” *Proceedings of the 21st British HCI Group Annual Conference on People and Computers: HCI...but not as we know it*, vol. 2 , pp. 83–86, 2007.
[21] G. Wahlgren, K. Bencherifa, and S. Kowalski, “A framework for selecting IT security risk management methods based on ISO27005,” *Conference paper, 6th International Conference on Communications, Propagation and Electronics*, 2013.
[22] S. A. Eroglu, K. A., Machleit, and L. M. Davis, “Empirical testing of a model of online store atmospherics and shopper responses,” *Psychology & marketing*, vol. 20, no. 2, pp. 139–150, 2003. Available: https://doi.org/10.1002/mar.10064
[23] J. M. Kizza, *Computer network security and cyber ethics*, McFarland, 2001.
[24] L. Floridi, *The Cambridge handbook of information and computer ethics*, Cambridge University Press, 2010. Available: https://doi.org/10.1017/CBO9780511845239
[25] D. Alexander, A. Finch, D. Sutton, and A. Taylor, *Information security management principles*, BCS, 2013.
[26] J. Sherwood, A. Clark, and D. Lynas, “Enterprise Security Architecture – SABSA,” *Information Systems Security*, vol. 6, no. 4, pp. 1–27, 2004.
[27] D. White and J. Fortune, “Current practice in project management—An empirical study,” *International journal of project management*, vol. 20, no. 1, pp. 1–11, 2002. Available: https://doi.org/10.1016/S0263-7863(00)00029-6
[28] S. Bălan, “M. Foucault's view on power relations,” *Cogito-Multidisciplinary Research Journal*, vol. 2, pp. 55–61, 2010.
[29] B. Al Sabbagh and S. Kowalski, “A socio-technical framework for threat modeling a software supply chain,” *IEEE Security & Privacy*, vol. 13, no. 4, pp. 30–39, 2015. Available: https://doi.org/10.1109/MSP.2015.72
[30] B. Al Sabbagh and S. Kowalski, “Developing social metrics for security modeling the security culture of it workers individuals (case study),” *Proceedings of the 5th International Conference on Communications, Computers and Applications (MIC-CCA2012)*, IEEE, pp. 112–118, 2012.
[31] C. Mowles, *Rethinking management: Radical insights from the complexity sciences*, Routledge, 2016. Available: https://doi.org/10.4324/9781315606125
[32] M. T. Siponen, “A conceptual foundation for organizational information security awareness,” *Information Management & Computer Security*, vol. 8, no. 1, pp. 31–41, 2000. Available: https://doi.org/10.1108/09685220010371394
[33] Cyber Attack on the NHS, Thirty-Second Report of Session 2017–19, House of Commons Committee of Public Accounts, 2018. Available: https://publications.parliament.uk/pa/cm201719/cmselect/cmpubacc/787/787.pdf
[34] T. A. Mattei, “Privacy, Confidentiality, and Security of Health Care Information: Lessons from the Recent WannaCry Cyberattack,” *World neurosurgery*, vol. 104, pp. 972–974, 2017. Available: https://doi.org/10.1016/j.wneu.2017.06.104

[35] J. Collmann and T. Cooper, “Breaching the security of the Kaiser Permanente Internet patient portal: the organizational foundations of information security,” *Journal of the American Medical Informatics Association*, vol. 14, no. 2, pp. 239–243, 2007. Available: https://doi.org/10.1197/jamia.M2195
[36] 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, 2001. Available: https://doi.org/10.1023/A:1011902718709
[37] D. Ionita, “Current established risk assessment methodologies and tools,” M.S. thesis, University of Twente, 2013
[38] T. Schlienger and S.Teufel, “Analyzing information security culture: increased trust by an appropriate information security culture,” *Proceedings of the 14th International Workshop on Database and Expert Systems Applications*, pp. 405–409, 2003. Available: https://doi.org/10.1109/dexa.2003.1232055
[39] C. Perrow, *Normal Accidents: Living with High Risk Technologies*, Princeton university press, 2011. Available: https://doi.org/10.2307/j.ctt7srgf
[40] P. M. Salmon, N. A. Stanton, M. Lenné, D. P. Jenkins, L. Rafferty, and G. H. Walker, *Human Factors Methods and Accident Analysis: Practical Guidance and Case Study Applications*, CRC Press, 2017. Available: https://doi.org/10.1201/9781315587400
[41] I. Okere, J. Van Niekerk, and M. Carroll, “Assessing information security culture: A critical analysis of current approaches,” *Information Security for South Africa*, IEEE, pp. 1–8, 2012. Available: https://doi.org/10.1109/ISSA.2012.6320442
[42] T. Schlienger and S. Teufel, “Information security culture – from analysis to change,” *South African Computer Journal*, vol. 2003, no. 31, pp. 46–52, 2003.
[43] A. Martins and J. Elofe, “Information security culture,” *Security in the information society*, Springer, pp. 203–214, 2002. Available: https://doi.org/10.1007/978-0-387-35586-3_16
[44] D. Boden, *The Business of Talk. Organizations in Action*, Organization Studies, Sage, 1997. Available: https://doi.org/10.1177/017084069701800315
[45] T. Quintaneiro, “The concept of figuration or configuration in Norbert Elias' sociological theory,” *Teoria & Sociedade*, vol. 2, 2006.
[46] V. Haren, TOGAF Version 9.1, 2011
[47] M. Siponen and R. Willison, “Information security management standards: Problems and solutions,” *Information & Management*, vol. 46, no 5, pp. 267–270, 2009. Available: https://doi.org/10.1016/j.im.2008.12.007
[48] A. E. Brown and G. G. Grant, “Framing the frameworks: A review of IT governance research,” *Communications of the Association for Information Systems*, vol. 15, no. 1, 2005. Available: https://doi.org/10.17705/1CAIS.01538
[49] R. W. Perkins, “Diagnostic Interviewing for Consultants and Auditors: A Collaborative Approach to Problem Solving,” *Consulting to Management*, vol. 8, no. 3, pp. 70, 1995.
[50] M. Heerink, B. Kröse, V. Evers, and B. Wielinga, “Assessing acceptance of assistive social agent technology by older adults: the almere model,” *International Journal of Social Robotics*, vol. 2, no. 4, pp. 361–375, 2010. Available: https://doi.org/10.1007/s12369-010-0068-5
[51] S. Kowalski, “IT insecurity: a multi-discipline inquiry,” Department of Computer and System Sciences, University of Stockholm and Royal Institute of Technology, Sweden, 1994.
[52] M. Lundy, *Strategic human resource management*, 1993
[53] J. Saldaña, *The coding manual for qualitative researchers*, Sage, 2015.
[54] W. Ashford, “Sony hack exposes poor security practices,” *Computer Weekly*, 2014. Available: http://www.computerweekly.com/news/2240236006/Sony-hack-exposes-poor-security-practices
[55] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, “A design science research methodology for information systems research,” *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45–77, 2007. Available: https://doi.org/10.2753/MIS0742-1222240302
[56] E. F. Wolstenholme, “Towards the definition and use of a core set of archetypal structures in system dynamics,” *System Dynamics Review*, vol. 19, no. 1, pp. 7–26, 2003. Available: https://doi.org/10.1002/sdr.259