Beyond Training and Awareness: From Security Culture to Security Risk Management

Richard McEvoy[1, 2] and Stewart Kowalski[1]

[1] NTNU, Gjovik, Norway
[2] DXC Technology, Royal Pavilion, Aldershot, UK
richard.mcevoy@dxc.com

Abstract. DXC Technology were asked to participate in a Cyber Vulnerability Investigation into organizations in the Defense sector in the UK. Part of this work was to examine the influence of socio-technical and/or human factors on cyber security – where possible linking factors to specific technical risks. Initial research into the area showed that (commercially, at least) most approaches to developing security culture in organisations focus on end users and deal solely with training and awareness regarding identifying and avoiding social engineering attacks and following security procedures. The only question asked and answered is how to ensure individuals conform to security policy and avoid such attacks. But experience of recent attacks (e.g., Wannacry, Sony hacks) show that responses to cyber security requirements are not just determined by the end users' level of training and awareness, but grow out of the wider organizational culture – with failures at different levels of the organization. This is a known feature of socio-technical research. As a result, we have sought to develop and apply a different approach to measuring security culture, based on discovering the distribution of beliefs and values (and resulting patterns of behavior) throughout the organization. Based on our experience, we show a way we can investigate these patterns of behavior and use them to identify socio-technical vulnerabilities by comparing current and 'ideal' behaviors. In doing so, we also discuss how this approach can be further developed and successfully incorporated into commercial practice, while retaining scientific validity.

Keywords: security, culture, risk, human factors, socio-technical

1 Introduction

When considering "security culture" in relation to individuals, there is an understandable focus on countermeasures such as training and awareness. This is because many attacks either aim to trick individuals into downloading malicious software, or take advantage of security flaws that result from human error. But a narrow focus on entraining individual behavior fails to take into account organizational, cultural and social factors. These can also have a direct bearing on individual behavior; and thus on security outcomes.

To give a real life example, during an IT failure in a hospital system, pressure by managers on engineering staff to roll out a fix without conducting normal testing procedures resulted in a more severe incident, including the release of personal data [1]. The hospital culture, in effect, gave the managers too much authority to trump technical decision-making and processes during incident response.

If the culture of the organization as a whole can counteract investment in the security education and training of individuals; this points to the need for a more integrated approach to the assessment of organizational security within its cultural and social context. Such an assessment, of course, also needs to take into account the nature and risk appetite of the organisation. For example, a start-up company may be prepared to take more risks than a large enterprise; or may be in a position where it has to do so because internal processes are still immature.

DXC Technology were recently asked to participate in a Cyber Vulnerability Investigation – which is a socio-technical analysis of security vulnerabilities in the Defense sector in the UK[1]. As part of this, we were asked to develop and/or apply techniques for analyzing human and socio-technical factors which could contribute to security risks.

For the reasons outlined above, rather than focusing on individual factors, we took the approach of defining 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” [2].

Or, more bluntly,

> “the ways things are done in an organisation”[3].

This definition is ethno-methodological in intent. 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[4, 5], but as an inter-subjective process in which all members of an organization participate and contribute to by reiterating its structures in daily interaction[5, 6].

We set out how beliefs and values can be linked to patterns of behavior which, in turn, can be described, categorized and mapped to specific cyber security risks at both human and technical levels, providing the integrated view we require. Our approach was applied to the immediate project requirement and is intended to be developed as a practical consultancy tool, which is demonstrably valid and repeatable in scientific terms, while cost-effective to deliver in the commercial arena.

[1] https://www.gov.uk/government/case-studies/helping-mod-improve-its-defences-against-cyber-attack

In section 2 (Literature Review), we provide background reading on security culture and our methodology. Section 3 (Problem) describes the problem of investigating security culture and the requirements and constraints on our approach in the context of the CVI requirements. Section 4 (Approach) gives our overall approach to the work and the construction of our model. Section 5 (Model) provides an account of the theoretical framework we use and its validation. In section 6 (Additional Lessons), we further discuss the experience of applying our method – although, for obvious reasons, avoiding the specifics of the systems investigated. We discuss our approach in section 7 (Discussion). Finally, we draw our conclusions and outline future work in section 8 (Conclusions).

2 Literature Review

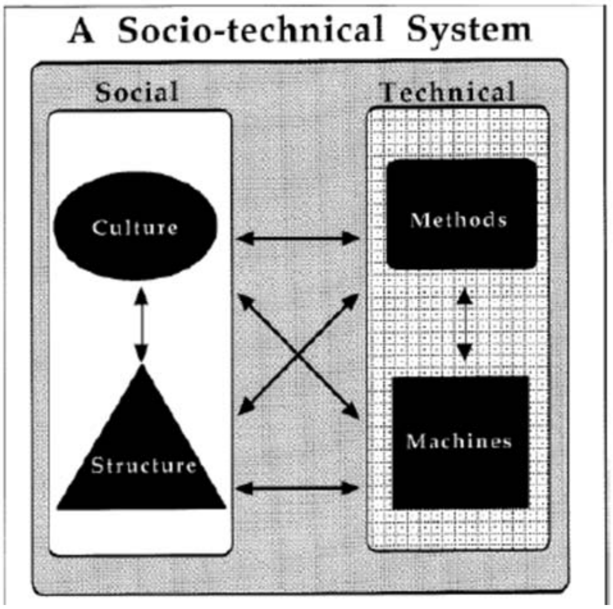
Security culture can be measured at various levels: regional, national and governmental, organizational and individual[2]. Our focus is chiefly on the interplay between organizational and individual factors and on local interactions which reflexively re-iterate the culture and institutions of an organization[5]; but, in line with Rasmussen’s analysis of socio-technical frameworks, other levels at regulatory or governmental levels may come into play[7].

Culture may initially seem to stand outside of the framework of socio-technical analysis, but, given our ethno-methodological assumption (see Introduction), we make the assumption that it touches on all actions and interactions taken by individuals and teams within an organization at each level. This assumption is illustrated in Figure 1, based on previous research by one of the authors.

Culture may be defined in different ways. 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”[4, 9]. This approach may be used to justify a change management program led by senior management who alter the culture of the organization to meet business requirements. However, this approach assumes that senior managers can objectively stand outside the culture, diagnose it and prescribe a solution; when, in fact, their organizational involvement could be part of the problem. For example, the Executive Director of Information Security at Sony clearly contributed to the repeated breaches in his organization in recent years[10].

Schlienger & Teufel treat information security culture as a problem rooted in processes where the individuals’ conformity to security policy determines the maturity of the security culture[11]. But this assumes that the security policy is necessarily correct when it may, in fact, have resulted from an incomplete analysis of organizational and technical factors and may, in fact, contribute to local issues with work performance, or even defeat the purpose of the policy’s implementation. A recent example is a common password complexity policy which is now admitted to be wrong (despite near universal acceptance) because it fails to make passwords complex enough to be unguessable by machines but too complex to be remembered by human beings[12], introducing both human and technical vulnerabilities simultaneously.

Figure 1 – A Socio-technical System[8]



Other approaches, more closely related to ours, treat security culture as a multi-factor problem requiring action at different organizational levels[13], or as arising from mental attitudes and models, which could be changed by the context of security questions[2]. Our approach is to attempt to select factors which can be shown to be immediately relevant to security (and safety) from historical experience and which are measurable by a variety of means, allowing for cross validation.

Both qualitative and quantitative approaches to assessing security culture are recognized in the literature [14] to have different advantages and disadvantages. In general, questionnaires with scales (e.g., Likert) subject to statistical analysis allow hypothesis testing, but may miss richer contextual data which qualitative research allows to be gathered[15]. However, the methods are not exclusive; and both could potentially applied in our approach.

To create our model, we called on known research frameworks or knowledge areas from research into the social science of technological development – technical and professional communication [16], research into technology adoption (UTAUT) [17], mental models of cyber security [18], emotional response to environments (PAD) [19], as well as aspects of good cyber security governance [20] and enterprise security architecture [21]. We also considered the known effects of economic de-investment in safety engineering [16], which we apply, by analogy, to security. We validated this crossover through examples. Finally, we considered the role of power structures and the distribution of cultural values in the organisation[8]; including leadership and management and individual and team responses to leadership and management, which are seen as key components in establishing security culture – for example [22].

3 Problem

The CVI projects presented us with a twofold problem. First, and obviously, to create a socio-technical approach to cyber security risk analysis and management, based on security culture assessment, which can identify vulnerabilities and associated risks at both organizational and individual level. Clearly, also the approach had to be scientifically and ethically valid to meet with predicted customer concerns. It also had to adhere to local security concerns, which, given the defense context, were understandably fraught.

At the same time, the nature of such projects requires that the approach be or, at least, appear to be strictly limited in terms of time and resources with 10 to 15 man days being allowed for the socio-technical aspects of the engagement. Although it should be added that such requirements often have a strong ritualistic element to them[23] which does not necessarily play out in practice. The key to success is to maintain the stakeholders' level of engagement with the process, rather than keeping strictly to initial time and resource limitations. In fact, this opening ritual is part of ensuring such engagement and other ritualistic practices – such as regular reporting – retain and repair engagement throughout the project without necessarily being related or contributing meaningfully to progress.

A final constraint was that the approach must be usable by information security consultants, who normally have engineering backgrounds and are not necessarily (or ever) trained in social science research techniques.

4 Methodology

4.1 Model Construction

On the basis of the research areas outlined in Section 2, we created a model of models which divided behaviors into six categories: communication, cognition, emotion, process, economic investment and structural (power relationships).

To meet with the requirement to achieve scientific validity, we adhered to frameworks or areas of knowledge which were well attested in the literature. We analyzed each category further; characterizing it into behavioral sub-categories.

For example, under cognition, we used the UTAUT framework which is considered a reliable way of measuring the adoption of technology, including security technology[17]. We also used, from previous research, the concept of security "mental models". These examine the breadth of individuals' understanding of security measures[2], which we argue could also influence their decision to adopt those measures.

As another example; for the “process” category we used frameworks from SABSA and IT Governance [20, 21]. There were used to identify “action areas” such as “security strategy” and “policy”. Table 1, below shows the actions areas identified for each of the six categories.

Table 1 – Action Areas

Communication	**Cognitive**	**Emotion**	**Process**	**Economic**	**Structural**
Technical & Professional Communication	Mental Model	Pleasure - Arousal - Dominance “Emotion”	Strategic Planning	Financial Spend	Conformance
Communication Planning	Risk Attitude		Architecture & Design	Human Resources	Autonomy
Control & Feedback	Performance Expectancy		Delivery	Time Given	Resistance
	Effort Expectancy		Testing	Timeliness	Negotiation
	Facilitation Expectancy		Implementation	Quality Criteria	Conflict
	Social Influences		Support & Maintenance	Priority	Blocking
	Problem Solving		Training (P)	Materials & Capability	Subversion
			End use	Roles & Responsibilities	
				Training (E)	

For each action area, we identified ideal behavioral patterns and recorded examples of vulnerabilities and associated risks which we considered, from experience, could arise from deviating from those patterns. Where possible, we associated these with real-life security (and, in some cases, safety) incidents.

For example, under the category of “economic investment”, we identified an action area called “financial commitment”. A vulnerability associated with this action area is the de-prioritization of security investment. An illustration of how this behavioral vulnerability can increase security risk is provided by the experience of the UK National

Health Service (NHS). The decision by the UK Health Secretary to discontinue a service contract legacy systems resulted in the inability of NHS IT staff to patch a vulnerability associated with the *Wannacry* attack [24].

4.2 Investigation Technique

We selected to use a qualitative approach to the investigation, using interviews and local observations. We presented an approach to the interview which reflected best practice in terms of carrying out such interviews. That is, we would record the interviews verbatim, transcribe them and subsequently code the results and analyze them using our framework. However, the proposal to record the interviews met with some objections, so we elected to have two consultants carry out the interviews with one focusing on note taking to capture the information in as much detail as possible.

Qualitative interviews of this nature enquire into the day to day life of the organization and the individuals' experience in making decisions relating to cyber security or carrying out cyber security processes and actions.

Set codes were associated with each of the action areas, described above, and used to analyze the interview data (effectively, acting as summaries of the emergent themes). The approach of using pre-set codes to represent themes is known as *descriptive multi-coding* and lends itself to use by novice researchers[25], matching the requirement that consultants with little experience of social science research methods should be able to use the approach.

The methodology also allows the inclusion of informal observations, or desktop research, where appropriate. It could also be supplemented with a quantitative analysis, based on a suitably designed questionnaire. However, this depends on the time allowed for the study and, given the time and resources constraints we were initially provided with, the approach of solely using qualitative interviews were considered the best match in terms of time and effort.

4.3 Number of Interviews

There was a discussion with the client organisations over the number of interviews. One of the systems under investigation was relatively small (a warehousing system). The other was a large HR (human resources) operation.

It should be noted here that the validity of qualitative research is not measured by the number of interviews carried out. The aim of the research is not statistical, but rather hermeneutical validity. Three interviews are considered the minimum number required for an investigation [15], but we considered that five interviews at different levels of the organisation and for different roles – senior manager, middle manager, front line staff, IT support, information security - would give a better picture of organizational life.

But this approach met with some objections. Some of these objections arose from the error of confusing quantitative and qualitative validity, which we have already discussed. Other aspects arose from changes to the nature of the investigation. For the smaller system, we were investigating (a warehousing system with around 40 staff), this number was probably adequate but it was felt that to deal with the interfaces to other organisations, more interviews would be needed.

The most interesting change occurred in the larger organisation (consisting of 780 seats) where, despite some initial concerns from trade unions, the approach was accepted and led to a call for volunteers. The consultant carrying out that investigation felt obliged to interview all 15 staff members who volunteered to show good faith. This number is actually the maximum number of such interviews recommended in the literature [15, 23] and proved both exhausting and, more interestingly, following the seventh interview, very repetitive in terms of findings. This number of interviews also exceeded the time and resource constraints, but demonstrated the point that stakeholder engagement is key, rather than strict adherence to a ritually induced plan.

4.4 Vulnerability and Risk Identification

Vulnerability and risk identification is initially a mechanical process of associating codes, interview data and analytical notes, with potentially risky behavior. But, at later stages, it became a more imaginative exercise as vulnerabilities and risks were correlated, or linked causatively with technical artefacts, and made more concrete and detailed in relation to the technical and business goals of the organization and its informational and technological assets.

We refer to these inter-linkings as *risk narratives* and they demonstrate how the themes we identified can be linked to demonstrate systemic or institutionalized risks, which would be an expected result from any socio-technical analysis of risk.

This process appears to consume around 3 man days, leaving 3 man days to complete a summary report – the actual vulnerabilities and risks can be recorded in a spreadsheet, or database, as the analysis proceeds. The overall time duration is about a week and a half to two weeks, more or less conforming with the time and resource constraints set out for the engagement.

5 Model: Mapping Security Culture to Security Risk

In this section, we further outline the reasons for selecting the categories used. We also take one category, for illustration, and show how we can divide it down into action areas, create an ideal behavioral profile for each action area, associated codes and potential risks. Finally, we demonstrate how we would develop risk and vulnerability narratives from identified risks and issues.

5.1 Category Selection

The underlying theme behind the category selection is predicting the adoption or non-adoption (including maintenance) of security measures by organizations. Failures to adopt security measures, arising from deviations from the "ideal" behavioral patterns, have been associated with each area in historical incidents, based on experience in both security and the closely related area of safety engineering. The six categories: communication, cognition, emotion, process, economic investment and structural (power relations) were selected with the following reasoning given below.

Communication: Failures to inculcate good practice in the area of technical and professional communication have led to warnings being ignored, poor decision making and poor incident response, including managers blocking actions which might have redeemed the situation (e.g., during the Columbia disaster)[16].

Cognition: UTAUT[17] is a cognitive framework used to predict the adoption or non-adoption of technology. Predictions are based on the expectancies of technical performance, effort and support (facilitation) for the new technology and the social influence of colleagues, seniors and the IT department. We adapted the framework to include the concept of security expectancy based on individuals' *mental model*[2] of security – whether they included all aspects (physical, personnel, cyber) and whether they considered "defense in depth" (deterrence, detection, prevention, response, recovery). Clearly, failures to adopt appropriate technical measures and security procedures, such as two-factor authentication[26], can leave an organization exposed to attack.

Emotion: Extreme emotional responses to an environment have been shown to predict non-adoption behaviors [19]. Apathy regarding security is an obvious cause. But, paradoxically, cyber security paranoia[27] can also be linked to blocking innovation, including security innovation. This can fundamentally undermine the achievement of business goals. Our case study (section 6) uncovered an example where the use of wireless technology would have greatly increased information integrity, but this was banned on confidentiality grounds, even though the information being communicated was not security sensitive.

Process: It is obvious that failure to put in place security processes at strategic, tactical and procedural levels will negatively affect security outcomes [20, 21]. One example from the *Wannacry* incident where missing software lifecycle planning processes left the organization in a situation where 5 % of systems, including some key medical equipment, were no longer in full support [28].

Economic Investment: A failure to invest in security, like failure to invest in safety[7], has the potential for catastrophe. Again, using the *Wannacry* example, the decision to remove funding from support contracts was a contributor to the length of the outage [28].

Structural: Defective power structures may lead, for example, to leadership failures or employees resisting change. The Sony hack demonstrated a leadership failure by the Direction of Information Security Operations which was not effectively countered by other board members or subordinates [22]. On the other hand, local changes to procedures autonomously instigated by operators can alter operating parameters for control systems with disastrous results[29].

5.2 Mapping Categories to Risks

For each category, it is possible to subdivide the category into action areas, as described in Section 4. A code was associated with each area and these were mapped to "ideal" behavioral profiles. Deviations from a profile resulted in vulnerabilities leading to risks.

Some degree of customization is required to fit the risks to specific organizations. Risk priorities and mitigation strategies are also organizationally dependent.

For reasons of space, we cannot reproduce the complete framework here[2], so we give a partial mapping of the category of economic investment to illustrate the mapping process – see Table 2 – and to demonstrate that the cultural behaviors we select result in direct risks at the user and operator level.

Table 2 – Mapping Actions Areas (Codes) to Risks – Economic Investment

Category: *Economic Investment*		
Code	*Ideal Behavioral Profile*	*Risks of Deviation*
Financial Spend	Organizations should commit to continued spend on necessary cyber security hygiene activities. Cyber security budgets should be prioritized for, at least, the next five years. Ring fencing cyber security budgets should be considered.	Failure to commit to spending on hygiene activities may result in operators or users being unable to carry out necessary security activities. Failure to invest in new security technology may lead to exposure to novel attacks which operators or users are unable to counter. Failure to invest in new policy and processes to deal with new legislation on privacy and security may in result in fines or prison sentences.

[2] The full model is available on request to the authors.

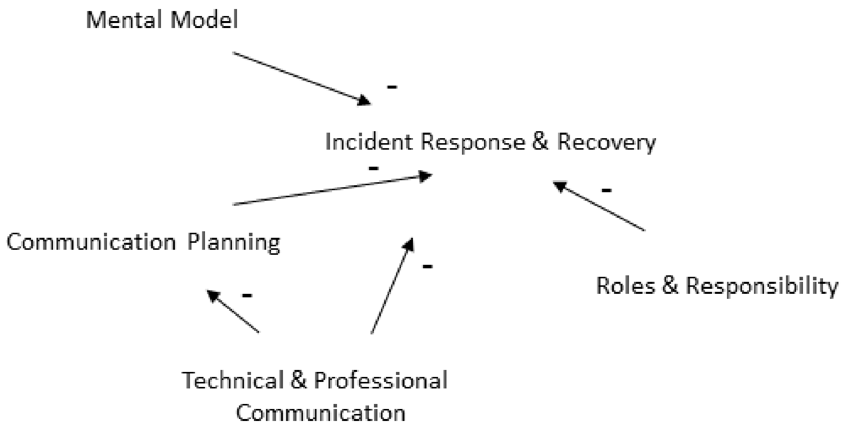
Code	*Ideal Behavioral Profile*	*Risks of Deviation*
Human Resources	Organizations should employ appropriate levels of staff with cyber security skills in different areas, e.g., software engineering, risk management, incident response	Failure to employ suitably skilled individuals across the organization results in an inability to act effectively on cyber security issues (e.g., asking individuals with security governance skills to carry out technical reviews)
Time Given	Time should be given in projects and during system maintenance lifecycles to address cyber security issues.	Failure to give time to cyber security issues during conception, design, implementation, testing and roll out may lead to last minute and inadequate fixes, exposing systems to attack Failure to give time to security maintenance activities directly exposes systems to new vulnerabilities (e.g., no patching windows). This prevents operators from making systems secure.
Timeliness	Technical and human resources should be supplied in a timely fashion during projects or support activities. Security decision making should chime with other project decision making timetables.	Failure to supply technology on time may lead to users employing local solutions such as use of unauthorized media. Failure to supply security vetted human resources may lead to un-vetted resources being used.
Materials & Capability	Technology and materials (such as computer media) should be supplied from authorized resources. Technology should have the capability to support operations efficiently and effectively.	Failure to supply authorized or suitable resources may lead to unauthorized or unsuitable resources being substituted by users or operators. Users resort to local solutions which may be insecure.

Code	*Ideal Behavioral Profile*	*Risks of Deviation*
Quality Criteria	Quality acceptance criteria should be specified for all security actions to assure security goals.	Failure to specify security quality acceptance criteria may result insecure settings.

5.3 Building Risk Narratives

The third step in the model is iterative – as part of the analysis. This is to build *risk narratives* (see Approach) up from factors identified during interviews. So we do not simply mechanically list risks but link them using system dynamics to organizational decisions, or practices, and to technical artefacts and associated behaviors.

Figure 2 – Diagram of a Risk Narrative


Mental Model
-
Incident Response & Recovery
-
-
Communication Planning
-
-
Roles & Responsibility
-
Technical & Professional Communication

Risk narratives are built up by demonstrating how behaviors conjoin to reinforce the likelihood of risks being realized; or to undermine security measures. Furthermore, where security breaches are already occurring, such narratives provide underlying causes which need to be addressed in addition to the actual breach.

For example, in an early trial, one organization had clearly invested heavily in ensuring that professional quality online training was in place for staff. But, without active reinforcement of the 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 security measures and security culture contradicted each other.

Similarly, a lack of coordination of roles between different security parties in another organization combined with poor communication planning, a lack of training in professional communication techniques, and a narrow mental model of security (one which excluded 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 a distributed denial of service and would initially be in serious disarray due to poor communication practices. Figure 2 shows a diagrammatic view of this risk narrative, with different factors contributing to a poor incident response outcome.

Furthermore, the " open and friendly" nature of the interview[15], the voluntary nature of participation as well as the strong ethical stance on interview confidentiality created an environment for the admission of issues which might not otherwise have come to the surface, e.g., use of unauthorized media.

6 Additional Lessons

We have already discussed the number of interviews and, following the experience, now consider that, unless the organization is very small, 7 interviews should be considered with representatives of the organization at different levels and in different roles. But, for very large or distributed organizations, a higher number up to 15 may be needed. One might also consider modifying the approach to include small workshops with several representatives, provided this is not considered inhibiting.

During this initial foray, the interviewer teams consisted of a human factors expert and an experienced cyber security practitioner. The latter did not have a background in social science research. The cyber security practitioners found the method conceptually easy to understand, but stated they would have preferred more time to become familiar with the coding process and the framework and associated risks than had been allowed during preparation. This suggests the need for a practice interview and analysis session.

It was also suggested by the consultants that the materials used for training and preparation could be improved by a better layout and by including an initial set of questions to help novice interviewers structure the risk assessment – not necessarily as part of the interview itself, but to ask themselves during the analysis and review of materials.

7 Discussion

In response to a commercial requirement in the Defense sector in the UK, we undertook to develop an approach to socio-technical research, which was trialed successfully with two organisations.

To meet with potential objections from clients, our method relied on well-known research techniques and frameworks (Section 2). The only original contribution was to map using multi-coding techniques behavioral patterns to specific risks and vulnerabilities and to use these patterns to build systemic risk narratives. These mappings can be validated in terms of previous experience in both security and safety engineering as being precursors to serious incidents.

We believe our approach allowed us to uncover risks where human factors could contradict apparently successful security initiatives; and issues where human factors reinforced the likelihood of risks being realized.

Using qualitative investigation techniques can be, and sometimes was, seen as subjective. But it is easy to validate the claims made by our approach, if necessary. For example, 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. Delays in decision-making due to poor management can be illustrated from email correspondence or from meeting minutes. The only constraint on our analysis is the time given to conduct it. The reason for selecting the interview approach was that it lent itself to meeting project time and resource constraints.

We consider that a final challenge to the method is that the "ideal" behavioral profiles and associated codes and risk mappings are difficult to fully validate without further engagements. But we have shown how historical incidents can be used to refine, augment and validate the framework. We also accept that social science researchers should continually re-visit their thinking.

8 Conclusion

We have described our experience with developing an approach which allows security culture in organizations to be mapped to security risks which directly affect individuals and operators.

Future work will consider a full case study, using both qualitative and quantitative methods within the framework to further validate our approach. We would welcome feedback from other researchers and industry specialists. We also believe the same framework could also be applied to health and safety and to post-incident analysis as well as cyber security risk management.

References

1 Collmann, J., and Cooper, T.: 'Breaching the security of the Kaiser Permanente Internet patient portal: the organizational foundations of information security', Journal of the American Medical Informatics Association, 2007, 14, (2), pp. 239-243

2 Al Sabbagh, B., and Kowalski, S.: 'Developing social metrics for security modeling the security culture of it workers individuals (case study)', in Editor (Ed.)^(Eds.): 'Book Developing social metrics for security modeling the security culture of it workers individuals (case study)' (IEEE, 2012, edn.), pp. 112-118

3 Lundy, M.: 'Strategic human resource management', 1993

4 Okere, I., Van Niekerk, J., and Carroll, M.: 'Assessing information security culture: A critical analysis of current approaches', in Editor (Ed.)^(Eds.): 'Book Assessing information security culture: A critical analysis of current approaches' (IEEE, 2012, edn.), pp. 1-8

5 Mowles, C.: 'Rethinking management: Radical insights from the complexity sciences' (Routledge, 2016. 2016)

6 Boden, D.: 'The Business of Talk. Organizations in Action', ORGANIZATION STUDIES-BERLIN-EUROPEAN GROUP FOR ORGANIZATIONAL STUDIES-, 1997, 18, pp. 544-544

7 Leveson, N.: ‘Engineering a safer world: Systems thinking applied to safety’ (MIT press, 2011. 2011)
8 Al Sabbagh, B., and Kowalski, S.: ‘A socio-technical framework for threat modeling a software supply chain’, IEEE Security & Privacy, 2015, 13, (4), pp. 30-39
9 Van Niekerk, J., and Von Solms, R.: ‘Information security culture: A management perspective’, Computers & Security, 2010, 29, (4), pp. 476-486
10 ‘https://www.risk3sixty.com/2014/12/19/the-sony-hack-security-failures-and-solutions/’
11 Schlienger, T., and Teufel, S.: ‘Information security culture-from analysis to change’, South African Computer Journal, 2003, 2003, (31), pp. 46-52
12 BBC: ‘http://www.bbc.co.uk/news/technology-40875534’, 2017
13 Martins, A., and Elofe, J.: ‘Information security culture’: ‘Security in the information society’ (Springer, 2002), pp. 203-214
14 Teufel, T.S.a.S.: ‘Analyzing information security culture: increased trust by an appropriate information security culture’, in Editor (Ed.)^(Eds.): ‘Book Analyzing information security culture: increased trust by an appropriate information security culture’ (2003, edn.), pp. 405-409
15 Kvale, S., and Brinkmann, S.: ‘Interviews: Learning the craft of qualitative research’, California, US: SAGE, 2009, pp. 230-243
16 Boiarsky, C.: ‘Risk Communication and Miscommunication: Case Studies in Science, Technology, Engineering, Government, and Community Organizations’ (University Press of Colorado, 2016. 2016)
17 Oshlyansky, L., Cairns, P., and Thimbleby, H.: ‘Validating the Unified Theory of Acceptance and Use of Technology (UTAUT) tool cross-culturally’, in Editor (Ed.)^(Eds.): ‘Book Validating the Unified Theory of Acceptance and Use of Technology (UTAUT) tool cross-culturally’ (BCS Learning & Development Ltd., 2007, edn.), pp. 83-86
18 Wahlgren, G., Bencherifa, K., and Kowalski, S.: ‘A framework for selecting IT security risk management methods based on ISO27005’, in Editor (Ed.)^(Eds.): ‘Book A framework for selecting IT security risk management methods based on ISO27005’ (2013, edn.), pp.
19 Eroglu, S.A., Machleit, K.A., and Davis, L.M.: ‘Empirical testing of a model of online store atmospherics and shopper responses’, Psychology & marketing, 2003, 20, (2), pp. 139-150
20 Alexander, D., Finch, A., and Sutton, D.: ‘Information security management principles’, in Editor (Ed.)^(Eds.): ‘Book Information security management principles’ (BCS, 2013, edn.), pp.
21 Sherwood, J., Clark, A., and Lynas, D.: ‘Enterprise Security Architecture-SABSA’, Information Systems Security, 2004, 6, (4), pp. 1-27
22 Siponen, M.T.: ‘A conceptual foundation for organizational information security awareness’, Information Management & Computer Security, 2000, 8, (1), pp. 31-41
23 Ladner, S.: ‘Practical ethnography: A guide to doing ethnography in the private sector’ (Routledge, 2016. 2016)
24 Mattei, T.A.: ‘Privacy, Confidentiality, and Security of Health Care Information: Lessons from the Recent WannaCry Cyberattack’, World neurosurgery, 2017, 104, pp. 972-974
25 Saldaña, J.: ‘The coding manual for qualitative researchers’ (Sage, 2015. 2015)
26 ‘http://www.computerweekly.com/news/2240236006/Sony-hack-exposes-poor-security-practices’
27 Mason OJ, S.C., Freedman F: ‘Ever-present threats from information technology: the Cyber-Paranoia and Fear Scale’, Frontiers in Psychology, 2014, 5

28 Ehrenfeld, J.M.: ‘WannaCry, Cybersecurity and Health Information Technology: A Time to Act’, Journal of Medical Systems, 2017, 41, (7), pp. 104

29 Wynne, B.: ‘Unruly technology: Practical rules, impractical discourses and public understanding’, Social studies of Science, 1988, 18, (1), pp. 147-167