Cassandra's Calling Card: Socio-technical Risk Analysis and Management in Cyber Security Systems

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

[1] NTNU i Gjøvik, Teknologivegen 22, 2815 Gjøvik, Norway
[2] DXC Technology, Royal Pavilion Wellesley Road Aldershot Hampshire GU11 1PZ
www.ntnu.no

Abstract. Current methodologies for cyber security risk analysis are largely focused on process and technology. They do not systematically incorporate socio-technical thinking. We argue this reduces their predictive power in determining the risks of cyber threats to organizations and hence limits the range of responses. A remedy is to augment such systems using suitable socio-technical models. As an example, we propose a re-working of Rasmussen's model for safety in systems, applying it to cyber security. The updated model gives rise to a set of predictors and boundary conditions which can be used to determine an organization's resilience in the face of external and internal cyber threats, enabling analysts to propose an extended range of countermeasures. We propose using this approach as a basis to include socio-technical analysis in risk assessment. As an example, we provide a critique of the risk methodology used in SABSA against this model. We discuss practical applications of the approach and some associated issues. Future work will focus on incorporating this approach into a variety of risk methodologies and the creation of novel techniques that can be tested in the simulated cyber security environment of a cyber range or in the field.

Keywords: socio-technical systems analysis, cyber security, risk analysis, risk management

1 Introduction

Current methodologies used for cyber security risk analysis and management largely focus on technical and process requirements. Evidence from incidents such as the Sony hacks and failures at SingHealth (see section 3) point to social failures as much as technical or procedural weaknesses as reasons for the occurrence of security incidents. Threats and vulnerabilities in organizations are also not simply technical or procedural in nature but result from complex systemic factors arising in modern organizations and societies. We argue that the lack of socio-technical systems analysis in commonly used risk analysis methodologies leaves organizations more vulnerable to cyber security risk than they should be. As one possible means of addressing this, we show how Rasmussen's model of a complex socio-technical systems for safety engineering can be adapted for cyber security purposes. This adaptation, in turn, provides a basis for enhancing current approaches to risk analysis and management. We give an example of applying

our approach to the risk methodology SABSA, outlining the current weaknesses in the approach and making recommendations for its improvement. Future work will focus both on enhancing current approaches in other methodologies and developing new ones. Verification and validation of our techniques will be aided not only by case studies in real life, but also the use of simulated studies in the Norwegian Cyber Range.

Section 2, "Literature Review", puts our approach in the context of current research. In section 3, "A Socio-technical Risk Vacuum?", we provide evidence of the current techno-centric nature of cyber security risk analysis methodologies. Following on in Section 4, "4 Cyber Systems as Complex Socio-Technical Systems", we model the socio-technical nature of cyber security risk to organizations in terms of Rasmussen's model of complex socio-technical systems(Rasmussen 1997); and we augment the boundary conditions and predictors provided in the model(Cassano-Piché, Vicente et al. 2006), incorporating barriers to organizational learning(Kleiner and Corrigan 1989), such as failure to pay reputational costs(Cassano-Piché, Vicente et al. 2006). Section 5, "Developing Socio-Technical Techniques for Cyber Security Risk Analysis", states the predictive properties cyber security risk analysis techniques should have in order to be able to address risks on a socio-technical basis. These factors can be used as criteria to develop and assess proposed techniques. In section 6 ,"Example Assessment – SABSA", we provide an example assessment of a commonly used risk methodology – SABSA (Sherwood, Clark et al. 2004) – against our criteria. We make some practical recommendations for its enhancement using our approach. We conclude in section 8, "Conclusions and Future Work", where we set out our proposals for developing both current and novel techniques for risk analysis on the basis of our approach, their verification and validation.

2 Literature Review

Socio-technical systems analysis is an established part of safety engineering practice for over fifty years(Leveson 2011, Salmon, Stanton et al. 2017). But despite strident efforts by – for example – Kowalski(Al Sabbagh and Kowalski 2012, Al Sabbagh and Kowalski 2015), Sasse (Adams and Sasse 1999, Sasse, Brostoff et al. 2001) and Anderson (Anderson and Moore 2007), cyber security risk analysis and management techniques commonly in use do not address socio-technical, economic or human factors based analysis in any depth (see Section 3).

Where socio-technical or human factors are addressed, generally, the treatment is superficial. Users are treated as hostile, lazy, or ignorant – and the highest standard is conformance to cyber security policy, which may be out-of-step with actual security requirements, or place an unacceptable burden on costs or workloads -leading to their "shadow" abandonment (McEvoy and Kowalski , Schlienger and Teufel 2003, Schlienger and Teufel 2003, Teufel 2003, Okere, Van Niekerk et al. 2012) or even be directly mistaken(BBC 2017). A faulty epistemological standpoint can also undermine the effectiveness of approaches – for example, the assumption that managers can stand objectively outside the system and manipulate other agents within it (Mowles 2016).

This shortcoming is starting to be addressed in academia where there is a recognition that cyber security requires approaches including human and organizational factors and that technical solutions no longer provide satisfactory answers – see, for example, (Soomro, Shah et al. 2016) for a review of the relevant literature.

This paper attempts to bridge this gap by showing how socio-technical models can be adapted to create practical set of criteria for judging risk analysis and management techniques from a socio-technical viewpoint as a basis for the assessment and development of current techniques to make them more complete. As an example of this approach, it draws on and adapts Rasmussen's model of a complex socio-technical system(Rasmussen 1997) and brings it up to date by including some additional predictors drawn from a real-world scenario(Cassano-Piché, Vicente et al. 2006) and by considering the increasing complex intermediation of the supply of cyber services (Section 4). We use the risk methodology SABSA (Sherwood, Clark et al. 2004) as a well-known and accessible example of a commercial risk analysis and management methodology to demonstrate our approach.

Ultimately, we propose to validate the plausibility of these models through action research on real-world systems and realistic simulations (Checkland and Holwell 1998).

3 A Socio-Technical Risk Vacuum?

We argue that most current approaches to cyber security risk analysis center on technology and procedures, reflecting their origins in engineering practice (Saleh and Alfantookh 2011). Others reflect a more business-oriented approach considering different parts of the organization. But almost none systematically incorporate socio-technical aspects which leads to risks being underestimated (see below and section 4).

We carried out a brief review, based on a survey of major cyber security risk analysis methodologies in the marketplace (Ionita 2013). We define socio-technical thinking as the consideration of a combination of factors - *Culture* (for example, human factors, behavior, ethnicity, organizational culture), *Structure* (for example, economics, social structures, politics, regulation, policy, procedure management and governance), *Methods* (policies and procedures, working practices) and *Machines* (technology) and their *Interaction* – see Figure 1.

The criterion used was that, during the *risk discovery* phase (according to ISO27005(Wahlgren, Bencherifa et al. 2013)), the methods used mentioned the factors directly and dealt with them systematically. For example, if *culture* was mentioned in relation to users' knowledge and awareness of cyber security, this scored a 1. If it was examined at different levels, such as worker, manager, senior manager and other aspects such as group (as well as individual) learning, behavior and ethics were examined, it would score a 2. Finally, *Interaction* was considered, at the basic level, to be building risks from links between different factors and components, rather than considering them in isolation and, more fundamentally, the identification of underlying patterns in the social, economic and political life of the organisation which contributed to its overall risk.

The results of the review are shown in Table 1. The total score (out of 10) shows the completeness of the methodology in socio-technical terms in our interpretation. Although not exhaustive, the list shows that most common methods in the marketplace have a shortfall in terms of socio-technical systems analysis. We have also been informed by experienced colleagues in industry that even where an approach is theoretically more complete (e.g., NIST(Saleh and Alfantookh 2011)), in practice, these aspects are seldom addressed[1].

To demonstrate how scores were assigned, we use SABSA (Sherwood, Clark et al. 2004) and OCTAVE Allegro as example methodologies. SABSA scores quite highly because it takes a layered approach to risk analysis, based on soft systems methodologies, , considering threats in terms of four domains (people, processes, systems and external). The assets of the organization are considered its business goals and threats are categorized in relation to these goals – for example, threats to health and safety, threats to information security, business failures in terms of mis-selling systems capabilities and so forth. Threats themselves are analyzed using scenarios and the capability and motivation of threat actors considered. The scenarios also allow some consideration of the interaction of different factors (under the labels of catalysts and inhibitors).

Having said this, the SABSA approach is business-oriented, rather than socio-technically oriented. Underlying factors which lead to the kinds of vulnerabilities identified in the approach are not addressed – for example, aspects such as power relations between groups(Bălan 2010), social and economic pressures which militate against process maintenance, the results of changes over time (Rasmussen 1997), or group/individual cognitive perceptions of security measures (Oshlyansky, Cairns et al. 2007) are not considered. Hence, we perceive this approach as only partially meeting with the socio-technical criteria proposed. Similar remarks can be made about NIST and IRAM (see also remarks on how these factors are ignored - above).

OCTAVE Allegro, in contrast, takes an information centric approach to risk analysis where the organization's information assets represent the organizing principle. Information moves between various "containers" in a system which can include people as well as technical objects which store and transmit information assets. Each type of container is associated with a set of questions about potential vulnerabilities and various counter-measures are proposed at container level. From a socio-technical point of view, this model focuses on technology and procedures. For example, it does not address social or human reasons why vulnerabilities might occur and does not consider interaction between system components or aspects such as change over time. Similar remarks can be made about CRAMM, other OCTAVE methodologies, FAIR, Infosec Standard 1, attack path analysis and MEHARI. In essence, all these approaches focus on technical, physical and procedural security control measures and do not consider social factors leading to technical vulnerabilities or poor behavior.

We believe this socio-technical deficit represents a serious gap in thinking about cyber security risk which affects all aspects of risk analysis from gathering threat intelligence to contingency planning, since almost all threats have a strong socio-technical element to them, both in terms of how and where the threat originates, who implements

[1] In conversation.

it, what organizations are affected, how they are impacted, their resilience and their ability to recover from the attack.

Examples of threats with marked socio-technical elements include[2] -

1. Hostilities between nation-states
2. Political protestors engaging with social media to launch attacks
3. Insider attacks
4. Malware attacks making use of (ultimately disposable) human agents
5. Hardware and software backdoors
6. Insider trading
7. State-sponsored espionage

Where organizations do not take account of socio-technical factors, they fail to defend themselves effectively or respond appropriately to threats because they do not understand the full extent of the risks they face, the vulnerabilities they have or the potential impacts of such attacks on them, not just at the technological level, but at the organizational level.

For example, the "Wannacry" attack(Hillier April 2018) on the NHS (National Health Service) in the UK proved more devastating than it should have been due to a failure to appreciate the weaknesses of the organization from a socio-technical point of view. Central governing bodies were not aware of shortcomings in technical defenses – demonstrating weaknesses in control and feedback within the organization and a resultant weakness in the vertical integration of its working practices. The close-coupled and complex nature of NHS systems (where, for example, medical equipment, patient management systems, IoT and ICS devices and office systems reside on the same unsegmented network) ensured a non-linear impact of any successful attacks (Perrow 2011, Ehrenfeld 2017, Mattei 2017, Mohurle and Patil 2017, Sütterlin, Dyrkolbotn et al. 2018). Furthermore, the organization's priorities during the attack were skewed in terms of dealing with the attack and its costs rather than addressing the more vital issue of patient safety – a serious cultural shortcoming where central government cost concerns took priority over patients' lives.

Other attacks show similar patterns. The Sony attacks represented a set of internal management failings as much as they did the work of sophisticated attackers(Berghel 2015) including the willingness of the director of IT to cover up audit failings. Similar statements can be made about the failures at SingHealth[3].

These real-world examples show that socio-technical considerations are vital during risk analysis. This is further emphasized by the complex nature of modern cyber systems which we consider in Section 4.

[2] https://www.forbes.com/sites/firewall/2010/04/29/seven-cyber-scenarios-to-keep-you-awake-at-night/#2e701f576f7d

[3] https://www.straitstimes.com/singapore/probe-report-on-singhealth-data-breach-points-to-basic-failings?utm_medium=Social&utm_campaign=STFB&utm_source=Facebook&fbclid=IwAR0HHFtADeIC5jLquA3bZuMGUgBAxnnPK96NzmHRAXvkf6rwc7Ml-K9yhs8#Echobox=1547076196

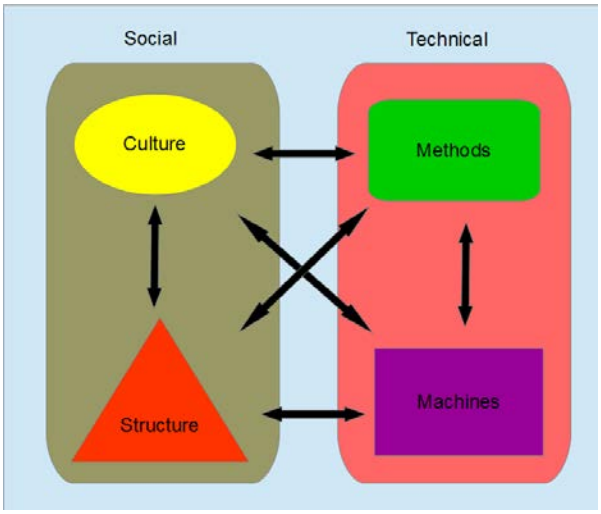

Figure 1: Socio-technical System(Kowalski 1994)

4 Cyber Systems as Complex Socio-Technical Systems

Rasmussen's model (Rasmussen 1997) demonstrates how organizations need to think socially and systemically in addressing risk – considering the vertical integration of systems, both managerial, operational and technical and how pressures on systems – on the one hand, to economize on cost and, on the other, to reduce work load – can push systems to a point where they are vulnerable to a triggering event, whether exogenous or endogenous, which creates a catastrophic incident.

These models are useful because they allow us not just to analyze incidents but also to derive incident predictors and determine boundary conditions (Cassano-Piché, Vicente et al. 2006). But these predictors are currently written with a view to preventing accidents which threaten health and safety, rather than specifically cyber security incidents – that is, triggering events are normally endogenous rather than exogenous. They also do not take account of reputational costs and their influence on security decisions, nor of failures in organizational learning due to organizational inertia(Kleiner and Corrigan 1989) – which specifically includes organizational response to threat intelligence and to the introduction of new technologies in the cyber security context.

Furthermore, although possibly unintentionally, the current version of the model might lead analysts to the belief that primary focus should be on a single organization and its integration. However, most critical systems are now provided on a multi-party basis, which induces a requirement for lateral as well as vertical integration. This leads us to propose two extensions to the model, shown in Figures 1 and 2.

Risk Analysis & Management Methodology	Culture	Structure	Methods	Machines	Interaction	Socio-Technical Score
CRAMM	1	0	1	2	0	4
OCTAVE Allegro	0	0	1	2	0	4
NIST	1	1	1	2	1	6
Infosec Standard 1	0	0	1	2	0	3
FAIR	0	0	1	2	0	3
MEHARI	0	0	1	2	0	3
STRIDE	0	0	0	2	0	2
SABSA (Risk)	1	1	1	2	1	6
Attack Path Analysis	0	0	0	2	0	2
IRAM	1	1	2	2	1	7

0 – Not present
1 – Partially present
2 – Systematically addressed
N/A – Not applicable

Table 1 – Socio-Technical Components in Cyber Security Risk Analysis

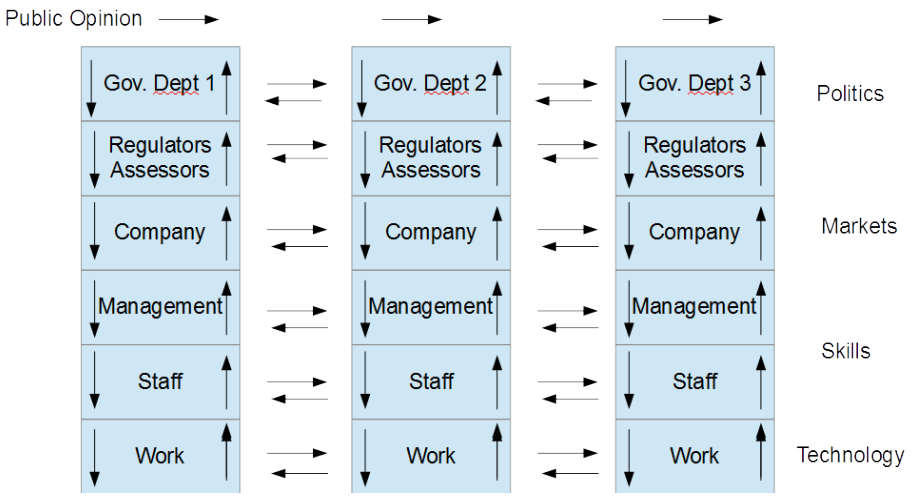

Figure 1 – Rasmussen's Model - Adapted for Cyber Organizations

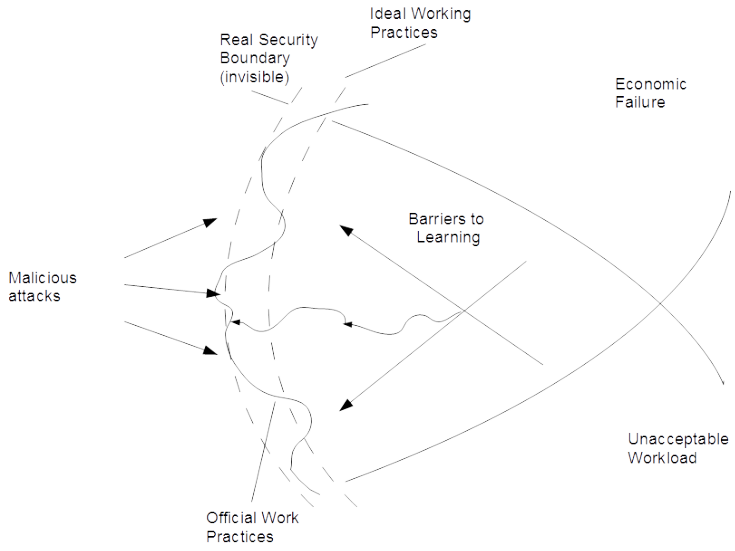

Figure 2 – Adapted View of Rasmussen Boundary Model for Cyber Security

Original Predictors	Updated Cyber Security Predictors
Safety is an emergent property of a complex socio-technical system. It is impacted by the decisions of all the actors.	Security is an emergent property of a complex cyber system. It is impacted by the decisions of all the actors.
Threats to safety are usually caused by multiple contributing factors, not just a single catastrophic decision or action.	Threats to security are usually caused by multiple malicious actors, vulnerabilities in organisations by multiple contributing factors: not just a single catastrophic threat, decision or action.
Threats to safety or accidents usually result from a lack of vertical integration across all levels of a complex socio-technical system, not just from deficiencies at any one level alone.	Security incidents or vulnerabilities usually result from a lack of vertical and lateral integration across all levels of a complex cyber system, not just from deficiencies at any one level alone.
The lack of vertical integration is caused, in part, by a lack of feedback across levels of a complex socio-technical system. Actors at each level cannot see how their decisions interact with those made by actors at other levels, so the threats to safety are far from obvious before an accident.	The lack of integration is caused, in part, by a lack of feedback across and between levels of a complex cyber system. Actors at each level cannot see how their decisions interact with those of others so the threats to security are far from obvious before an incident.
Work practices in a complex socio-technical system are not static. They will migrate over time under the influence of a cost gradient driven by financial pressures in an aggressive competitive environment and under the influence of an effort gradient driven by the psychological pressure to follow the path of least resistance.	Work practices in a complex cyber system are not static. They will migrate over time under the influence of a cost gradient driven by financial pressures in an aggressive competitive environment and under the influence of an effort gradient driven by the psychological pressure to follow the path of least resistance. Organizations may resist change for a number of other cultural reasons.
The migration of work practices can occur at multiple levels of a complex socio-technical system, not just one level alone.	The migration of work practices can occur at and across multiple levels of a complex cyber system, not just one level or in one organisation alone.
Migration of work practices causes the system's defenses to degrade and erode gradually over time, not all at once. Accidents are released by a combination of this systematically-induced migration in work practices and a triggering event, not by an unusual action or an entirely new, one-time threat to safety.	Migration of work practices causes the system's defences to degrade and erode gradually over time, not all at once. Incidents occur due to a combination of changes in malicious action and this systemically-induced migration in work practices – not by a single unusual action or an entirely new, one-time threat to security.

Table 3 – Proposed Extension to Predictive Statements for Cyber Systems

In Figure 1, we extend the view of cyber systems to encompass other organizations in the service and supply chain.

In Figure 2, we include two additional features to the conventional Rasmussen model. We add the label "Barriers to Learning" to show that social and cultural factors can impede the pace of organizational change in working practices in response to threats (i.e., social cognition). We also display the barrier posed by working practices as a jagged edge to show that such practices can degrade to the point they cross the security boundary which – due to the constant nature of attacks – can lead to catastrophic failure.

In Table 3, we re-write and extend the predictors which can be derived from Rasmussen's model(Cassano-Piché, Vicente et al. 2006), both to make the wording match the vocabulary of cyber security, and also to take into account the extensions we have proposed. The major changes are the dual factor cause of cyber security incidents (both malicious acts and a breakdown in work practices; the incorporation of the need for lateral as well as horizontal integration; and the consideration of cultural barriers to organizational learning.

5 Developing and Assessing Techniques for Cyber Security Risk Analysis

The predictive model proposed in Section 4 thus provides us with one possible basis for assessing and improving cyber security risk analysis and management methods using socio-technical analysis. We summarize the assessment criteria in Table 4.

Factor	Criteria
Decision-making	Provide a view of the nature of organizational decision-making.
Threat Actors	Identify all threat actors and external agents creating pressure on the organizations
Integration	Identify where working practices mismatch.
Control & Feedback	Uncover weaknesses in control & feedback mechanisms
Work Practices	Uncover (historical) changes in work practices
Security Boundaries	Determine if the security boundaries have already been breached by changes to work practices
Identify New Security Working Practices	Identify if new working practices are required in response to threats or to other environmental/working practice changes.
Dynamic Modelling	Provide a model of the system which allows weaknesses to be identified/described and captures change over time

Table 4 - Using the Predictors as Assessment Criteria for Analyzing Risk Methodologies

Note, the requirement for *dynamic modelling* leads to the use of techniques such as *risk narratives* as a sense-making account of cyber security behavioral patterns (the term 'figuration' (configuration) (Quintaneiro 2006) or 'construct' (Taylor and Lerner 1996) may be preferred). This is arguably a natural mode for expressing socio-technical risks, exampled in (McEvoy and Kowalski , Botta, Muldner et al. 2011) - which can also be captured using techniques such as systems dynamics diagrams (Wolstenholme 2003).

6 Example Assessment - SABSA

SABSA (Sherwood, Clark et al. 2004) is an open-source methodology for creating an enterprise security architecture.

SABSA Layer	**Description**
Contextual	Business planning and decision-making, e.g., business risk assessment, business requirements, organizational and cultural development
Conceptual	Business operations, e.g., process development, audit and reviews, standards and procedures
Logical	Security governance, e.g., security policymaking, information classification, service management, audit trails
Physical	Security administration, e.g., development and execution of security rules, access list maintenance, event log file management
Component	Technical capability, e.g., products, tools, project management, operation of individual systems

Table 5 – SABSA Layers

This not the same as a technical architecture. Rather it is a layered organizational blueprint for ensuring cyber security is maintained throughout all parts of the organisation. The layers are described in Table 5.

SABSA makes use of soft systems methodology(Sherwood, Clark et al. 2004) to analyze and represent requirements and solutions at each level, leading to an integrated approach to creating secure organizations.

Based on our review above, SABSA does refer to socio-technical factors, but the coverage is not complete as the methodology is business-oriented – making it ultimately policy and procedurally driven, rather than sociologically motivated.

In Table 6, we provide our assessment the strengths and weaknesses of SABSA risk methodology in relation to our predictive criteria and its dynamic modelling capability.

Predictive Capability	Strengths	Recommendations
Decision-making	SABSA is quite strong in terms of gathering decision-making criteria (business requirements) from all parts of the business.	SABSA focuses too narrowly on a single organisation and should consider vertical or horizontal integration of requirements.
Threat Actors	SABSA identifies multiple threat actors both internal and external at different layers.	The analysis would need to also consider issues raised by changes in external actors and external pressures over time as well as the potential degradation in working practices.
Integration	SABSA does not use methods to promote intra-organizational integration.	Lateral integration should be considered.
Control & Feedback	SABSA's approach is likely to promote feedback on poor decision-making.	There should be a focus on the completeness of feedback mechanisms, either vertically or laterally.
Work Practices	SABSA does consider business requirements changing over time	SABSA should consider historical or current changes to work practices, particularly in other organizations.
Security Boundaries	SABSA is likely to uncover where work practices have violated security policy.	SABSA should seek to uncover underlying reasons for the violation such as pressure on costs or workloads or other cultural or human factors as well as breaches in the security boundary
Identify New Security Working Practices	SABSA is likely to identify the need for new or updated security working practices.	Barriers to the adoption of new practice may not be identified in SABSA. It also needs to incorporate responses to threat intelligence and new technology into consideration.
Dynamic Modelling	The use of threat scenarios goes part way to capturing risk narratives. But accounts of countermeasures are not connective.	SABSA should seek to capture dynamic aspects of the narrative and avoid a static ontology of threat capabilities/motivations. Countermeasures should be related to one another to form both defense-in-depth and defense-in-breadth.

Table 6 - Current Deficiencies in the Socio-Technical Capabilities of SABSA

In practical terms, many of these issues are easy to address in the SABSA methodology by incorporating some additional layers of analysis in the risk approach. For example, by considering the *disintegrating* effect of organizational issues at different layers in the model and providing additional means to carry out analysis of change over time.

It would be much harder to address the same issues in a methodology such as OCTAVE Allegro where the solution would appear to be to carry out a supplementary risk analysis from a socio-technical viewpoint in order to capture additional risks. This kind of multi-standpoint risk assessment approach is starting to become common in industry, suggesting that the deficiencies in purely technical and procedural approaches are being recognized and organizations are seeking to deal with them – see (McEvoy and Kowalski) for an example in the defense sector in the UK.

7 Conclusions and Future Work

We believe that current approaches to cybersecurity risk analysis and management, are, for the most part, inadequate due to the omission of socio-technical systems analysis.

We propose using socio-technical models to enhance these methodologies, using a variant on Rasmussen's model in relation to SABSA and OCTAVE Allegro as an example.

In future, these factors also lead us onto to a deeper discussion of how and why organizations identify risks, what we are trying to protect and what is regarded as a threat and why. These point to issues of identity and survival which would be difficult to address in the scope of this paper but lead us to believe that a model which unifies social learning and socio-technical factors might provide deeper insights into the nature of risk. We are aware that the very act of augmenting risk models in this manner could change how we think about risk in such systems, pointing us to underlying factors that are not addressed in systems design methodologies or even perceived as relevant(Checkland and Holwell 1998).

Future work will focus on developing and assessing novel approaches to both risk identification and risk evaluation and management in line with our findings. We also intend to develop and improve techniques for the dynamic modelling of socio-technical risks. In this, we will make use of the simulation of socio-technical systems (Hettinger, Kirlik et al. 2015) and their management on the Norwegian cyber range[4].

Bibliography

Adams, A. and M. A. Sasse (1999). "Users are not the enemy." Communications of the ACM **42**(12): 40-46.

Al Sabbagh, B. and S. Kowalski (2012). Developing social metrics for security modeling the security culture of it workers individuals (case study). Communications,

[4] Norwegian Cyber Range https://www.ntnu.no/ncr

Computers and Applications (MIC-CCA), 2012 Mosharaka International Conference on, IEEE.

Al Sabbagh, B. and S. Kowalski (2015). "A socio-technical framework for threat modeling a software supply chain." IEEE Security & Privacy **13**(4): 30-39.

Anderson, R. and T. Moore (2007). Information security economics–and beyond. Annual International Cryptology Conference, Springer.

Bălan, S. (2010). "M. Foucault's view on power relations." Cogito-Multidisciplinary Research Journal **2**: 55-61.

BBC (2017). "http://www.bbc.co.uk/news/technology-40875534."

Berghel, H. (2015). "Cyber chutzpah: The sony hack and the celebration of hyperbole." Computer **48**(2): 77-80.

Botta, D., et al. (2011). "Toward understanding distributed cognition in IT security management: the role of cues and norms." Cognition, Technology & Work **13**(2): 121-134.

Cassano-Piché, A., et al. (2006). 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 Sage CA: Los Angeles, CA.

Checkland, P. and S. Holwell (1998). "Action research: its nature and validity." Systemic practice and action research **11**(1): 9-21.

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

Hettinger, L. J., et al. (2015). "Modelling and simulation of complex sociotechnical systems: Envisioning and analysing work environments." Ergonomics **58**(4): 600-614.

Hillier (April 2018). Cyber Attack on the NHS. HC 787. H. o. C. C. o. P. Accounts. House of Commons, Public Accounts Committee, House of Commons.

Ionita, D. (2013). Current established risk assessment methodologies and tools, University of Twente.

Kleiner, B. H. and W. A. Corrigan (1989). "Understanding organisational change." Leadership & Organization Development Journal **10**(3): 25-31.

Kowalski, S. (1994). "IT insecurity: a multi-discipline inquiry." Department of Computer and System Sciences, University of Stockholm and Royal Institute of Technology, Sweden.

Leveson, N. (2011). Engineering a safer world: Systems thinking applied to safety, MIT press.

Mattei, T. A. (2017). "Privacy, Confidentiality, and Security of Health Care Information: Lessons from the Recent WannaCry Cyberattack." World neurosurgery **104**: 972-974.

McEvoy, R. and S. Kowalski "Beyond Training and Awareness: From Security Culture to Security Risk Management."

Mohurle, S. and M. Patil (2017). "A brief study of wannacry threat: Ransomware attack 2017." International Journal **8**(5).

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

Okere, I., et al. (2012). Assessing information security culture: A critical analysis of current approaches. Information Security for South Africa (ISSA), 2012, IEEE.

Oshlyansky, L., et al. (2007). 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-Volume 2, BCS Learning & Development Ltd.

Perrow, C. (2011). Normal Accidents: Living with High Risk Technologies-Updated Edition, Princeton university press.

Quintaneiro, T. (2006). "The concept of figuration or configuration in Norbert Elias' sociological theory." Teoria & Sociedade **2**(SE): 0-0.

Rasmussen, J. (1997). "Risk management in a dynamic society: a modelling problem." Safety science **27**(2-3): 183-213.

Saleh, M. S. and A. Alfantookh (2011). "A new comprehensive framework for enterprise information security risk management." Applied computing and informatics **9**(2): 107-118.

Salmon, P. M., et al. (2017). Human Factors Methods for Accident Analysis. Human Factors Methods and Accident Analysis, CRC Press**:** 29-104.

Sasse, M. A., et al. (2001). "Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security." BT technology journal **19**(3): 122-131.

Schlienger, T. and S. Teufel (2003). Analyzing information security culture: increased trust by an appropriate information security culture. Database and Expert Systems Applications, 2003. Proceedings. 14th International Workshop on, IEEE.

Schlienger, T. and S. Teufel (2003). "Information security culture-from analysis to change." South African Computer Journal **2003**(31): 46-52.

Sherwood, J., et al. (2004). "Enterprise Security Architecture-SABSA." Information Systems Security **6**(4): 1-27.

Soomro, Z. A., et al. (2016). "Information security management needs more holistic approach: A literature review." International Journal of Information Management **36**(2): 215-225.

Sütterlin, S., et al. (2018). Supporting the Human in Cyber Defence. Computer Security: ESORICS 2017 International Workshops, CyberICPS 2017 and SECPRE 2017, Oslo, Norway, September 14-15, 2017, Revised Selected Papers, Springer.

Taylor, J. R. and L. Lerner (1996). "Making sense of sensemaking: How managers construct their organisation through their talk." Studies in Cultures, Organizations and Societies **2**(2): 257-286.

Teufel, T. S. a. S. (2003). Analyzing information security culture: increased trust by an appropriate information security culture. 14th International Workshop on Database and Expert Systems Applications.

Wahlgren, G., et al. (2013). A framework for selecting IT security risk management methods based on ISO27005. 6th International Conference on Communications, Propagation and Electronics, Kenitra, Morocco. Academy Publisher.

Wolstenholme, E. F. (2003). "Towards the definition and use of a core set of archetypal structures in system dynamics." System Dynamics Review **19**(1): 7-26.

