Consulting the Oracle at Delphi – Combining Risk I and Risk in Cyber Security

Richard McEvoy [1] and Stewart Kowalski[1]

[1] *NTNU, Teknologivegen 22, 2815 Gjøvik, Norway*

Abstract

Risk may be analyzed implicitly or explicitly. From industrial experience, the former is less commonly used than the latter on a day-to-day basis, even though the former makes up the primary content of most commercially available risk analysis and management methodologies. Paradoxically, the latter is also more commonly baked into the process and technology used by organizations and its culture of risk management. Hence this represents a sociotechnical issue which requires the resolution of both conflict of methods and ambiguity in the interpretation and application of risk analysis. We propose an approach for resolving these issues, based on experience "in the wild", and creating a Delphic convergence between the results of both approaches. Ultimately, we would aim to create a methodology for this purpose and propose some criteria for its creation.

Keywords

cyber security, risk, sociotechnical, analysis

1. Introduction

Explicit risk management is an approach where risks are defined by a tuple of factors (asset, threat, likelihood, impact) over which function is performed to derive a risk value, e.g., high, medium, low or $ 1m. This valuation is subsequently used to determine risk management strategy or tactics (treat, accept, transfer, avoid). Two issues may exist with risk analysis conducted in this fashion. The first is disagreement (which may be unrecognized) over the valuation of ordinal labels (i.e., qualitative risk analysis), where utilized. The second is that organizational membership, outside of subject matter experts, often struggle to understand this kind of analysis as they think in terms of concrete issues to be fixed (that is, implicit risk analysis terms).

Implicit risk analysis states risk in terms of issues which may contribute to organizational exposure, e.g., "the lack of patching", "poor network segmentation", "the risk of vulnerability X" "the risk of loss of confidentiality". Implicit risk statements conflate risks, with issues which contribute to exposure, with impacts and so forth. Hence the risks are not stated in these terms, but implicitly, in definitionally imprecise terms(Freund and Jones 2014). Paradoxically, risk is often still valued, in terms which are superficially like those used in explicit risk analysis. Labels such as "high", "medium", "low" may be utilized to categorize issues or $ values and the strategy choices of treat, transfer, accept or avoid applied. But with no formal function, the valuation is even more intuitive and highly subjective than even the use of qualitative methods in explicit risk analysis and may result in (often unrecognized) conflict and ambiguity over results and subsequent strategic or tactical choices.

The solution proposed by adherents of explicit risk analysis is to displace implicit risk analysis in the organization's thinking. But this has a potential for adversarial outcomes where members of an organization seek to introduce explicit risk analysis approaches since the power structure, leadership values, language, culture, processes and technology of the organization are often geared primarily to

7th International Workshop on Socio-Technical Perspective in IS development (STPIS 2021) 11-12 October 2021, Trento, Italy
EMAIL: thomarm@ntnu.no; stewart.kowalski@ntnu.no
ORCID: 0000-0001-7322-4257 (Thomas Richard McEvoy); 0000-0003-3601-8387 (Stewart Kowalski);


implicit risk thinking. So, risk analysis experts can become caught in a power struggle when they seek to introduce explicit, more formal and less subjective, approaches.

This last issue, we believe, points to a more fundamental sociotechnical issue underlying the divergence between explicit and implicit risk management and, indeed, human and organizational response to risk. Explicit risk management is, we believe, highly process and technology focused and normative in its results. Risk analysis results in recommending changes to process, policy and technology while ignoring organizational and cultural issues. It also tends to be design oriented rather than oriented to resolving day to day issues. Implicit risk analysis, on the other hand, because it is issue-centric and deals with ongoing problems and blockages, makes such issues concrete for management and employees and, despite gaps in the utility of outcomes, offers (or, at least, appears to offer) better chances for resolution. It is also closer to how results are presented in GRC systems and to auditors, where the focus is often compliance with control frameworks, not managing explicitly stated risks.

Based on practical experience, we offer a novel approach to risk elicitation and analysis which may form a basis for reconciling these approaches. In essence, we use a set of categories to draw out assumptions about assets, risks, threats and impacts and the costs of addressing these in business terms. Applying ordinal valuations to these allows for a reduction in ambiguity (and potential for unexpressed disagreement). Furthermore, it becomes easy to introduce explicit risk valuations into this approach as a contributing factor in the discussion. We believe our approach could form the basis for a Delphic convergence between explicit and implicit risk analysis - with resulting managerial improvements and reduction in conflict and ambiguity.

This paper makes the following contributions. First, while the issues of explicit versus implicit risk management are known, we identify sociotechnical factors which contribute to this divergence. Second, we outline an original technique which has been used "in the wild" which may provide a basis for reconciling these approaches. Third, we provide criteria for the development of a more formal methodology to achieve this goal – with the further aim of drawing sociotechnical thinking into risk analysis and management.

Risk I in the title, therefore, refers to the current approaches to risk analysis and Risk II to proposed approaches which include sociotechnical thinking in and sociotechnical solutions to issues in risk analysis and management. The inspiration is taken from Hollnagel's definitions of Safety I and Safety II (Hollnagel 2018)

In section 2, we review the relevant literature. Section 3 discusses the issues raised by the conflict and conflation of explicit and implicit risk approaches in more detail. Section 4 describes our approach as a counter proposal which addresses limitations we identify with both techniques. Section 5 discusses the requirements for creating a more formal methodology to incorporate sociotechnical thinking in risk analysis and management methodologies. Section 6 concludes and describes future work.

2. Literature Review

The gold standard of risk analysis and management is often taken to be ISO27005 (Wahlgren, Bencherifa et al. 2013) which sets out a framework for such analysis. The framework sets out how a risk analysis and management process should take place and be re-iterated by an organization. The process begins with establishing the business context of the organization, followed by a risk discovery and subsequent analysis, leading to recommended solutions, whose implementation is monitored. At the same time, there should be ongoing communication with management about the results of the analysis and progress towards reducing risk to acceptable levels.

The problem with this becomes clear from a review of current risk analysis and management methods which start from the assumption that a new system is being developed(Ionita 2013), but do not explicitly address how iterations of the process or blockages to it should be dealt with. Indeed, repeating the process would seem likely to repeat the solution, yet if the solution has not been applied in the context of the organization for reasons which exist outside the scope of these methods, this suggests either that it may not be appropriate and that alternatives should be sought or that other

problems exist which are not addressed by process and technological centric risk analysis and management methods and need a wider (we propose, sociotechnical) lens.

Work by Wangen et al. (Wangen, Hallstensen et al. 2018) suggests that ISO27005 is not complete as a framework, while the creators of SABSA, a security enterprise architecture methodology, show that poor definition of business context, especially future proofing solutions, can lead to serious organizational mismatches (Sherwood, Clark et al. 2004). Furthermore, work by the authors shows that sociotechnical considerations are missing from risk analysis and management methodologies(McEvoy and Kowalski 2019, McEvoy and Kowalski 2019).

Other authors have commented on the lack of maturity in cyber security risk analysis and management. The creators of the FAIR methodology have identified that risk is dealt with implicitly rather than explicitly by many organizations with consequent poor definitions of what constitutes risk or how to assess it. They also highlight issues with qualitative approaches to risk which use ordinal values, which are often interpreted in different ways without these differences being recognized. They propose a formal definition of the derivation of risk (using an ontology) and a quantitative methodology for analyzing risk as a cure(Freund and Jones 2014).

With the notable exception of SABSA(Sherwood, Clark et al. 2004), we would argue that most risk analysis methods, while they may formally take account of the nature of the business and management goals, offer an approach which is "context-free" in business and operational terms. Indeed, in some cases, methodologies recommend that any current countermeasures be discounted in the initial analysis of risk (e.g., CRAMM(Yazar 2002)) and that subsequent comparison is used only to discount measures already taken rather than consider operational or other (e.g., business, economic, cultural, social, cognitive) issues which may block the imposition of security controls. Furthermore, in general, measures are drawn from frameworks such as ISO27001 or NIST CSF(Calder and Watkins 2010, Teodoro, Gonçalves et al. 2015) which focus on technical and process requirements and largely ignore other sociotechnical factors such as culture and organization(McEvoy and Kowalski 2019).

A very different approach is proposed by Langner, particularly with regards to control systems security, where he shows that risk management can be regarded as a matter of system stability and resilience rather than the absence of breaches – a concept he borrows from financial risk management(Langner 2011). This is similar in some respects to proposals regarding the management of safety risk by (Rasmussen 1997) where control and feedbacks are proposed for controlling risk which is seen as a sociotechnical problem and systemic in nature. The latter also highlights economic pressures which are often missing in risk analysis and sociotechnical thinking.

Finally, research in the related safety industry points to analyzing risk using systemic methods and a risk management approach which should be human rather than technology centric, e.g., (Hollnagel 2018).

In our approach, following Hollnagel (ibid.), we seek to reconcile explicit and implicit risk management and offer a channel for introducing sociotechnical thinking into risk analysis. We do this by analyzing risk in additional categories, whose priorities are agreed with leadership and employees. The use of ordinal values for sorting priorities represents an agreement with management on current business goals, but also allows a scaled vector to be used to determine the degree and seriousness of the sociotechnical gap(Al Sabbagh and Kowalski 2011). We believe this approach allows us to go beyond pure technical or process considerations, leading to more flexible risk strategies that take account of business and operational actualities rather than simply normative security requirements. We also believe this approach allows to introduce explicit risk considerations alongside implicit ones without initiating a power struggle. This kind of conflict resolution which furthers business ends while creating a more humanistic approach to work is very much a part of the origin of sociotechnical approaches(Trist 1981).

3. A Conflict of Methods?

In the introduction, we summarized the divide between explicit and implicit risk analysis and touched on the differences between quantitative and qualitative analysis. The authors of the FAIR method identify these issues as arising from the immaturity of cyber security risk analysis methods (Freund and Jones 2014) and it can also be seen in the creation of multiple risk methods with differing

approaches to risk elicitation, understanding of risk factors, risk calculation and risk communication, though there are some commonalities between them (Ionita 2013).

While we agree that the industry would benefit from a precise and agreed ontology of risk and from a cost/benefit analysis based on quantitative techniques rather than qualitative (ordinal) valuations, we consider that risk analysis approaches have more fundamental issues than a conflict of methods, ambiguity in results or a lack of definitional precision. The divergence between explicit and implicit risk approaches is a symptom of these underlying issues. Nor is this simply a matter of cognitive biases(Acciarini, Brunetta et al. 2020) at the individual level. They are sociotechnical in nature.

Commercial and government cyber security risk analysis methodologies are generally process and technology oriented and do not take into account sociotechnical or human factors in their analysis(McEvoy and Kowalski 2019). They also start from the premise of "blank slate" which allows technical and process controls to be applied without regard to the organizational environment. This tends to normative solutions which may not match local requirements, but lacking the toolset to analyze human, organizational or cultural factors leads to the imposition of measures which create issues that lead either to failure to apply the recommended risk controls or to "shadow" practices as policy and process fail to match circumstance (Fürstenau and Rothe 2014) – a failing which is also common in the safety industry under the label of process drift (Berman and Ackroyd 2006). These blockages and shadow practices create issues which are subsequently identified by implicit risk thinking by managers and experts working on operational systems and seeking to address problems rather than being engaged in system design or redesign.

The creators of FAIR have also mapped out a history of the development of risk management methods(Freund and Jones 2014) which developed over time in the absence of economic analysis from the use of FUD[2] to control frameworks and maturity analyses. Each of these approaches has left a mark on how organizations view risk and what mechanisms and processes they have in place to manage them. The primary tendency has been a move towards compliance rather than risk. For example, GRC systems are oriented towards applying relevant control frameworks such as NIST or ISO27002. This leads to a situation where management, experts, auditors and staff focus on identifying control gaps and raising these as security issues (while mislabeling them as risks as described – see Introduction and Literature Review). Again, these solutions tend to be normative, process and technology driven, perhaps more strongly than the risk methodologies. They fail to move away from technical and process -centric approaches.

We argue that, having identified issues and blockages, the risk analysis technique is foreshortened, likely due to work pressures and lack of economic resources undermining the risk management process (Rasmussen 1997) and well as a lack of risk management training and awareness. Hence, as described (Introduction) issues are analyzed as risks, labeled "high", "medium", "low" and treated or accepted. It should be noted that this also represents a reduction in the solution space as it not possible to avoid or transfer issues or control failures.

Hence, we believe that the divergence between implicit and explicit risk management is not simply a result of immaturity, or lack of awareness, but arises from sociotechnical issues. First, an over-focus on technical and process solutions which are context-free, normative and claim "objective" validity, but create local issues. Second, a heavy emphasis on control frameworks and maturity requirements, with a similar focus on process and technology, not only recreating the same issues but also emphasizing their identification and resolution as a security goal – free of both the context of economic risk and human and organizational requirements. Third, work pressures and a lack of organizational expertise leads issues being analyzed in a way which is superficially similar to formal explicit risk analysis but lacks the formal mechanisms, leading to subjective resolutions which are likely based on political rather than utilitarian considerations. Often economic pressures lead to the "risks" (i.e., the issues) being "accepted", left with no resolution, because they are perceived as being too expensive to fix (but with no comparison with the cost of not doing so). Clearly, this drift over time in working practices leads to precisely the breaches warned about in (Rasmussen 1997) in the safety context, but here are equally applicable to security.

[2] Fear, uncertainty and doubt

4. Industry Experience

Based on industry experience, we propose a different approach which seeks to reconcile both implicit and explicit risk analysis approaches and introduce a sociotechnical element to risk elicitation and risk analysis which works with organizations rather than proposing context free, technocentric solutions. The approach has been applied to two health organizations in the UK and also to a defense establishment – as well as being adopted by a major UK government office, but we only present one of the cases. Some of the issues have been fictionalized but are based on real examples in the authors' experience.

A regional NHS body in the UK requested an assessment of their current security posture as part of preparing to gain ISO27001 status and to contribute to creating an overall IT strategy. They expressed a willingness to engage not only with technical and procedural aspects of the assessment, but also to consider sociotechnical aspects such as security culture and organizational arrangements as part of their consideration of the overall strategy. They also requested the creation of a methodology to allow them to repeat further such assessments in future with other consultancy practices.

To achieve this, one of the authors, prepared an approach which took security issues identified during the investigation and analyzed them using the following factors, which were agreed with senior management.

Each of the factors was further divided into subcategories – see Table 4.1 – and assigned ordinal values between 1 and 5 to represent increasing complexity and cost for resolving the issues, taking account of both social and technical elements.

Table 4.1
Qualitative Analysis of Cost and Complexity of Resolving Cyber Security Issues

	5	4	3	2	1
Threat Type	Multiple	Cyber	Human	Technical	Force Maj.
Impact	Organization	Division	Team	Service	Individual
Vulnerability	Structural	Operational	Design Fault	HMI	Technical
Business Goal	Multiple	Patient Safety	Compliance	Availability	Other

The categories and subcategories were defined as follows:

1. Threat Type – various types of attack
    a. Multiple – an attack which combined multiple other factors such as social engineering and malware
    b. Cyber – a malware or penetration type attack
    c. Human – social engineering or another human agent attack such as tailgating
    d. Technical – a technical event which caused an outage
    e. Force Majeure – a natural event which caused an outage
2. Impact – likely impacts on achieving business goals at different organizational levels
    a. Organization – the whole organization would be affected by the outcome
    b. Division – a division of the organization would be affected by the outcome
    c. Team – a team would be affected
    d. Service – a service offered by the team would be affected
    e. Individual – only an individual would be affected
3. Vulnerability – the exposure to attack
    a. Structure – the vulnerability was part of how the organization as a whole function, e.g., a faulty policy or a management gap
    b. Operational – an exposure in IT or security operations, e.g., a lack of a SIEM
    c. Design Fault – a hardware or software design issue
    d. HMI – a poorly designed system-human interaction leading to, e.g., shadow practice
    e. Technical – for example, a faulty configuration

4. Business Goal – these are interpreted as being the organizational assets – see (Sherwood, Clark et al. 2004)
    a. Multiple – multiple goals would be affected by the impact
    b. Patient safety – a high priority goal in a health organization
    c. Compliance – regulatory compliance was identified as a key secondary goal
    d. Availability – the most common priority in the CIA triad in information security
    e. Other – allowed miscellaneous, e.g., local, goals to be identified as well

The assessment was carried out through a series of interviews with staff and management at different levels of the organization. This included review meetings with managers to agree on categorizations and subcategorizations of issues and their priorities and to gain perspective on whether other parts of the organization might also be affected (changing impact levels). This also provided an opportunity for early reflection on findings and potential solutions.

The analysis started with the identification of issues which the organization believed were relevant to its cyber security posture. This is the normal starting place for an implicit risk analysis. But the subsequent analysis by categories and subcategories meant that the issue was analyzed in two directions. The first direction, represented by the categories, was in the direction of a formal explicit representation of risk, The risk vector of threat, impact, vulnerability and asset (business goal) is clearly present in the definition of the categories. While an ordinal analysis was used, it should be obvious that financial figures could also be introduced to enhance the analysis and remove any ambiguities over priorities.

The second direction, represented by the subcategories, was in the direction of sociotechnical issues. The subcategories were intended to give a starting place to understanding the origin of the issues and to provide the beginnings of a qualitatively rich description of the organizations's problems while being able to associate these back with explicit risks.

For example, – say a security problem (fictionalized, in this case) was described as follows: "Passwords may be accidentally revealed by staff in a small research division keeping informal records of passwords for multiple [40 +] databases leading to data leaks, possible compromise of confidential subject information, and regulatory notices or fines". This would be evaluated as a "human/compliance failure" potentially leading to regulatory penalties, in a "team" due to poor "HMI" design (expecting staff to remember multiple complex passwords by themselves) and affecting the business goal of "regulatory compliance". A vector of ordinal values $i=(3,3,2,3)$ would result from the analysis.

The resulting vectors can be prioritized by sorting on their ordinal values. Furthermore, an advantage of the approach is that the sort order does not have to be fixed. For different business purposes, different orderings could be selected of the categories and different businesses may select and order some of the subcategories differently. What these priorities where can be agreed with the business.

For example, Table 4.2 shows different issues, referred to by a short descriptive label, which yield different risk orders depending on which categories are given greater weighting in the sort order.

The different sort orders effectively represent different strategies for resolving the issues and the underlying theme is their difficulty of resolution. For example, if all factors were sorted "low to high", with the exception of business goals (high to low) to give an overall rank order, this represented the strategy of undertaking "effective quick wins". If the same sort were carried out "high to low" across all factors, it represents approximately where the greatest level of time and resources would be needed to resolve key business issues.

Adding, or removing, categories from the sort – an obvious addition being costs - or changing the sort order, therefore, allows the risk analysis to have more flexible goals than simple prioritization of risk by cost[3]. This more flexible approach crosses the bridge from implicit to explicit expressions of risk by allowing sociotechnical considerations to be included in risk reasoning and to be part of the risk resolution.

Finally, each of the security issues analyzed was defined in such a way that a deeper analysis of sociotechnical factors was enabled by being able to discuss why particular issues were recalcitrant of solution. The approach also allowed for analysis of any patterns arising from individual factors such as

[3] Or qualitative impact assessment.

a preponderance of design vulnerabilities, or issues affecting patient safety. Basic statistical analysis of the identified factors and their weights could therefore point to areas of further investigation with regard to underlying (systemic) causes of security failures – see (McEvoy , McEvoy and Kowalski 2019) for potential candidates.

The technique applied across the regional body was used to identify organizational factors such as a need to unify information security provision across the Trusts. This arose because the subcategorization of security issues allowed for a wider discussion than the imposition of "normative" security measures. In other words, the discussion was not just about technical, or process solutions based on normative control frameworks, but allowed the risk analysts to open the discussion out to aspects such as organizational structure, the nature of local blockages and issues, design issues and the contribution of shadow IT and security practices to either supplement or undermine security. Yet this expansion of the terms of reference of the risk analysis beyond explicit risk factors or control frameworks did not result in an extension of the normal timeframe to carry out a standard risk analysis process.

Table 4.2
Example Security Issues

Issue	Threat Type	Impact	Vulnerability	Business Goal
Patching Failure	4	2	3	2
Password weakness	3	3	2	3
No power backup	1	4	4	3
No MFA on Remote Access	5	5	3	2

5. Discussion

We are not claiming at this point that the method illustrated represents a complete solution to the fundamental issues we have identified in the section 3 (A Conflict of Methods?). But our experience shows that it is possible to start to disentangle these issues by, initially, at least, accepting them in the form presented and determining their nature, based on a set of agreed categories, and their priority, in terms of difficulty to resolve. It is important, however, not to misapply the approach used in explicit risk methodologies to determine impact or to decide whether to treat/accept/avoid or transfer a "risk" which is really a security issue that could relate to multiple risks. Instead, we need a formal approach to breaking down these issues and relating them to their potential business impact and the cost of imposing countermeasures, while also resolving additional sociotechnical barriers.

To borrow inspiration from Hollnagel (Hollnagel 2018), we need to move away from Risk I (technology and process oriented, normative, context-free) risk analysis and move towards Risk II (human and sociotechnically oriented). As part of this, we believe the issues thrown up by implicit risk analysis are a stronger starting place for such a risk analysis but need both explicit adduction of risk and sociotechnical analysis of causes to be able to move towards cost-effective resolutions.

Hence, we propose the following criteria for the creation of a formal risk methodology which comprises both directions of analysis.

1. The risk methodology should start with issue elicitation at different levels of the organization.
2. A well-defined and agreed explicit risk ontology should be used for explicit risk analysis derived from the issues raised (Freund and Jones 2014)
3. Economic analysis of risk should be used to remove ambiguity caused by ordinal labelling (Ibid.)
4. Factorial analysis of sociotechnical aspects of issues should be incorporated into the approach (McEvoy , McEvoy and Kowalski 2019)
5. Risk prioritization should be flexible to allow different prioritization strategies to be used at different parts of the organization's timeline or for different purposes. A pure cost or impact prioritization is not a sufficient basis for decision making.

6. Countermeasures should not be simply process and technology oriented but encompass sociotechnical aspects as well.

We believe that this approach will organizations to more accurately prioritize cyber security issues and as well as identifying explicit risks, also identify underlying sociotechnical causes and hence result in a more flexible and more rounded approach to cyber security risk.

The other advantage of this approach is that it does not require switching the organization from considering implicit risk to considering explicit risk, setting up a potential cultural conflict, but rather by starting with issues which are already under peoples' focus and consideration and expanding the analysis in two different directions with communication and consensus on the shape the analysis takes leads the organization to a better acceptance of the analysis and its results.

6. Conclusion and Future Work

In this paper, we described how formal methods of cyber security risk analysis focus on developing an explicit view of risks, while commonly practiced informal approaches use an implicit view of risks. Many of the weaknesses associated with both methods have been described elsewhere. But we believe these approaches are tied to one another by a view of risk which is focused on technology and process and does not recognize sociotechnical aspects of security exposure. In turn, pressures on the organization foreshorten analysis and lead to a reduced solution space and often a failure to properly address issues, hence increasing the exposure of the organization to security risk over time.

We believe the solution lies in formally incorporating both approaches to risk analysis and management and enhancing these with a sociotechnical element. We outline criteria for creating such an approach and we contrast the earlier process and technically oriented approaches which we designate Risk I and our convergence of sociotechnical, explicit and implicit approaches which we call Risk II. We seek to ensure that this is done in full communication with management and staff leading to consensus on the approach and outcomes. A Delphic convergence should hence be achievable both in theory and in practice by our approach.

Future work will focus on developing this methodology and a suitable software architecture to support its implementation as a practical business tool.

7. References

Acciarini, C., et al. (2020). "Cognitive biases and decision-making strategies in times of change: a systematic literature review." Management Decision.

Al Sabbagh, B. and S. Kowalski (2011). A Cultural Adaption Model for Global Cyber Security Warning Systems (A socio-technical proposal). 5th Mosharaka International Conference on Communications, Networking and Information Technology (MIC-CNIT 2011), Mosharaka for Research and Studies.

Berman, J. and P. Ackroyd (2006). Organisational drift-a challenge for enduring safety performance. INSTITUTION OF CHEMICAL ENGINEERS SYMPOSIUM SERIES, Institution of Chemical Engineers; 1999.

Calder, A. and S. G. Watkins (2010). Information security risk management for ISO27001/ISO27002, It Governance Ltd.

Freund, J. and J. Jones (2014). Measuring and managing information risk: a FAIR approach, Butterworth-Heinemann.

Fürstenau, D. and H. Rothe (2014). "Shadow IT systems: Discerning the good and the evil."

Hollnagel, E. (2018). Safety-I and safety-II: the past and future of safety management, CRC press.

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

Langner, R. (2011). Robust control system networks: How to achieve reliable control after Stuxnet, Momentum Press.

McEvoy, R. and S. Kowalski (2019). Cassandra's Calling Card: Socio-technical Risk Analysis and Management in Cyber Security Systems. STPIS@ ECIS.

McEvoy, T. R. "An Accimap Waiting to Happen: Using Multi-coding Frameworks to Accelerate Risk Analysis and Management."

McEvoy, T. R. and S. J. Kowalski (2019). "Deriving Cyber Security Risks from Human and Organizational Factors–A Socio-technical Approach." Complex Systems Informatics and Modeling Quarterly(18): 47-64.

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

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

Teodoro, N., et al. (2015). Nist cybersecurity framework compliance: A generic model for dynamic assessment and predictive requirements. 2015 IEEE Trustcom/BigDataSE/ISPA, IEEE.

Trist, E. L. (1981). The evolution of socio-technical systems, Ontario Quality of Working Life Centre Toronto.

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.

Wangen, G., et al. (2018). "A framework for estimating information security risk assessment method completeness." International Journal of Information Security **17**(6): 681-699.

Yazar, Z. (2002). "A qualitative risk analysis and management tool–CRAMM." SANS InfoSec Reading Room White Paper **11**: 12-32.