An Accimap Waiting to Happen: Using Multi-coding Frameworks to Accelerate Risk Analysis and Management

Thomas Richard McEvoy

NTNU, Norway

Abstract

We present a proposed framework for conducting data analysis and gathering for the Accimap methodology, a sociotechnical analysis method, for a given domain area (in this case, cybersecurity) which we believe will help address the acknowledged defects of the method when applied to predictive risk analysis and management. The approach combines a generic framework for Accimap with an enhanced version of Rasmussen's original model of complex sociotechnical systems on which the Accimap approach is based, reflecting 'known good' cybersecurity principles as well as common factors underlying system breakdowns in other areas of safety and security. As well as its immediate application to risk analysis and management, we believe the framework may have value as a teaching and research tool.

Keywords

Accimap, qualitative interviews, qualitative coding, sociotechnical, security incident analysis

1. Introduction

Safety research has shown that human and organizational factors are implicated in over 50 percent of accidents[1], pointing to the requirement to analyze such incidents using sociotechnical systems methods [2]. We believe that similar findings will be evident in the field of cybersecurity and highlight the need for adopting sociotechnical approaches to cybersecurity[3, 1]. This approach of using artifacts from safety analysis in security also has precedent. For example, fault tree analysis has been adopted in the form of attack trees [4] and Accimap has been used to analyze security incidents [5].

But predictive risk analysis rather than post-hoc accident analysis is regarded as the primary technique of cybersecurity practice in communicating security requirements to management[6]. Accident analysis techniques such as Accimap are usually applied after the fact and require considerable investment in time and resources (which is, of course, justified by the seriousness of the accident) and this factor, along with others, undermines their use as techniques for predictive risk analysis[7].

By combining domain knowledge ('common body of knowledge') [8] from cybersecurity with common factors underlying accidents in other domains (based on a literature search – see section 2), we believe that these weaknesses can be overcome in the case of Accimap.

STPIS'20: 6th International Workshop on Socio-Technical Perspective in IS development, Online

richard.mcevoy@dxc.com (T.R. McEvoy)

The propsosed approach uses a multi-coding framework which combines a generic Accimap coding framework[9] with a domain-specific framework which has previously been used for analyzing weaknesses resulting from human and organizational factors in cybersecurity[3]. The framework is supplied in the form of a wiki[1].

It should be applied by undertaking and analyzing the results of a series of semi-structured qualitative interviews (similar to those which might be used in a cybersecurity capability maturity review [10]). The results can be underpinned by documentary evidence and quantitative surveys. This makes it possible carry out the data gathering, reporting and analysis in the same period of time and using similar human resources to a normal cybersecurity maturity review – rendering the technique commercially feasible – but the end result is not a set of scores but a 'rich picture' of potentially negative behaviors by the organization which could represent potential underlying weaknesses exposing the organization to the possibility of a serious cybersecurity breach and can be addressed in cultural change programs and organizational and work design.

This makes it possible to communicate with the management of the organization in an intuitive fashion which allows them to "join the dots" in terms of understanding how organizational failings can contribute to an incident and to its impact. It allows them not just to prioritize addressing threats at the technical level, but similarly address vulnerabilities within the organization at higher levels, tackling cultural and structural issues as well as process and technical aspects [11]. In short, to adopt a sociotechnical approach to cybersecurity risk analysis and management.

The end result is that recommendations for risk treatment at the technical level can be enriched by the proposal of additional organizational and cultural measures to address the underlying causes which lead to such control failings in the first place.

We believe the approach also has value for pedagogical and research purposes. It could be used as the basis for simulating cybersecurity incidents during training or study in the context of a poorly prepared organization[12] highlighting the role organizational failings could play in exacerbating the effects of a cybersecurity incident, or be used as a springboard for analysis of the interaction of specific factors by researchers.

Future work will involve undertaking full studies with the framework, treating it as an artifact of design science [13], seeking to refine and improve it and considering ways to semi-automate the derivation of findings.

Section 2 provides related literature on the area. Section 3 lists the current failings of Accimap in terms of predictive risk analysis and management. Section 4 summarizes the overall approach. Section 5 describes the multi-coding framework, its contents, construction and use. Section 7 shows how it should be applied within organizations. We discuss our approach in section 8 and we conclude and outline future work in section 9.

2. Related Work

The use of Accimap for accident investigation in various contexts, including information systems security, is well attested in the literature [9, 5] and its strengths as well as its flaws are recognized [7].

The concept of improving on the capability to use Accimap more readily comes from [7], based on identifying generic factors. However, we argue in this paper that for specific do-

[1] https://github.com/thomasrichardmcevoy/FASST

mains and in the context of specific organizations, we can make use of specialist domain knowledge to further accelerate this process. The domain knowledge is derived from our research into sociotechnical factors in information security failures [1, 3] combined with known technical countermeasures [14] and a simplified threat model which covers common forms of breaches that have had devestating effects at organizational level[1].

Both the generic Accimap framework and the FASST framework we employ are modeled on Rasmussen's model of complex sociotechnical systems[15]. The difference between them is that the generic Accimap approach divides the organization into levels and then considers factors, whereas the FASST framework takes the factors which Rasmussen identified – cost evasion, work evasion and control and feedback (further divided into workflow, learning and external monitoring) – and maps potential organizational and human factors which contribute to security failure as potential subfactors. The mapping between the two frameworks hence allows the analyst to consider potential cause and effect across levels.

The overall aim of the exercise is to improve the communication of risk in the organization by not only being able to justify technical or procedural countermeasures on a business case basis [6], but also to encourage business managers to take a humanistic approach to their security decision-making in line with the philosophy of sociotechnical design [16]. Such an approach would represent a joint optimization of security and human aims. For example, poor design of security procedures can be shown to represent a security weakness rather than a strength [17]. Our approach allows these kinds of weaknesses to be detected.

The methodology for applying the system is carried out in a way which is similar to a capability maturity exercise, but rather than being completed with a scoring of the organization's capabilities [10], the approach ends with a clear communication of potential risky scenarios where human and organizational factors are already creating exposures in the organization's security posture.

The overall approach is based on design science where the multicoding framework acts as the artifact which will be developed recursively and reflexively over a set of research studies into the effectiveness of its application to the problem of incorporating sociotechnical systems thinking into cyber security risk analysis and management [13, 1].

Finally, we believe our approach should allow the further development of pedagogical efforts to teach security skills by allowing organizational and human failings to be incorporated into training in cybersecurity ranges to create more realistic scenarios [12].

3. Problem

Accimap offers several advantages which explains its popularity as a method [7] –

1. It offers an approach to identifying failures at the sharp and across the entire organization.
2. It is simple to learn but has a strong theoretical underpinning.
3. It allows system failures and inadequacies to be identified.
4. It offers and exhaustive description of accidents.
5. The output is visual and easily interpreted.
6. It is a generic approach which can be applied to any domain.
7. It removes apportioning of blame to individuals and promotes the development of systematic countermeasures.

Its disadvantages are [7] –

1. It can be time consuming (and hence costly)
2. It suffers from problems of hindsight analysis and may lead to oversimplified causality and counterfactual reasoning.
3. The quality of the analysis is dependent on the quality of the data
4. The output does not explicitly generate remedial measures or countermeasures
5. There is an absence of taxonomies of failure types which raises questions over its reliability
6. The approach can only be applied retrospectively
7. The accident analysis can become large and unwieldy

Our task is to seek to overcome some, or all, of these disadvantages to make Accimap useable as a predictive risk analysis method which tackles sociotechnical aspects of risk exposure.

4. Approach

The approach combines a generic coding framework for Accimap which addresses various aspects of accidents occurring across different levels of the organization [9] – already being used to accelerate analysis – with a coding framework (now extended and augmented) for addressing organizational and human factors underlying cybersecurity risk exposure [3] and technical elements (security countermeasures) and risks (potential security incidents).

The mapping between the two frameworks, first, allows human and organizational factors to be considered from the perspective of different levels of the organization and, second, helps to identify causal dependencies and effects between levels, including how such failings can undermine the provision of procedural and technical countermeasures. The framework has a strong theoretical underpinning based on on an adapted version of Rasmussen's model of complex sociotechnical systems (see section 5).

The method for applying the technique is based on the approach used with the original human and organizational factors framework in [3], using as primary input a set of qualitative interviews with individuals from different parts and levels of the organization. The only different is that the analysis technique uses multi-coding [18] to create an enriched picture of organizational dynamics.

The approach potentially addresses some of the flaws in using Accimap –

1. It should reduce the time to complete a study
2. It avoids hindsight bias – the approach can be used predictively
3. The use of the framework means that a more structured approach is taken to data gathering which can contribute to a higher quality of data or, at least, better identification of gaps
4. The approach explicitly generates countermeasures and remedial actions which can form part of security program
5. The associated risk model gives an initial taxonomy of failure types which can augmented as required
6. The scope of the analysis is contained in the framework - though this may be a disadvantage in some cases (see section 8).

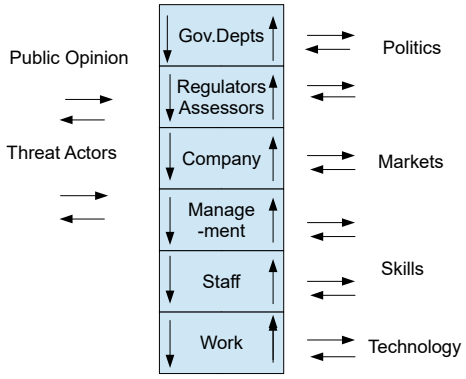

Figure 1: Control and Feedback in Complex Sociotechnical Systems [15]

5. Underlying Model and Coding Structure

5.1. Model

Accimap is based on Rasmussen's model of complex sociotechnical systems [15]. This was used as the basis for the generic Accimap coding framework [9]. Based on an adaptation of this model specifically for the purposes of cybersecurity [1], we created a coding framework which looked at the factors Rasmussen identified in his model – cost evasion, work evasion and breakdowns in various control and feedback processes.

For the purposes of this analysis, we specifically identified three types of breakdown – loss of control and feedback (over the security workflows), weaknesses in learning culture and lack of monitoring external circumstances which could be significant in cybersecurity terms. This is not the only possible categorization, but suits our purpose. The model is summarized in Figures 1 and 2. Furthermore, we increased the granularity of our analysis by considering a further categorization, using these factors, of behaviors we had previously identified in [3]. We call the resulting model FASST,standing for 'factorial analysis - sociotechnical security thinking'.

We created a mapping between the two frameworks which means that a category on one framework will have one or more corresponding categories in other framework and vice versa. This mapping reflects intuitions concerning relevance and causality between the frameworks.

For example, the category 'Culture' appears several times in the Generic Accimap framework and is linked to aspects such as 'Communication', 'Mental Models' and 'Ethics' in the FASST framework. In turn, each of those categories points back to other organizational layers

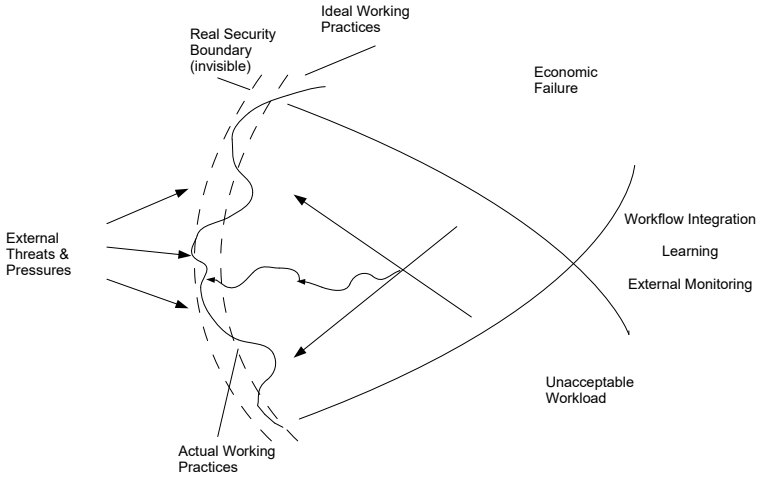

Figure 2: A Factorial View of Rasmussen's Model of Work Practice Breakdown[1]

of the Generic Accimap model and should allow the analyst to consider possible causal links or associations both within and between layers of the organization.

The FASST framework not only identifies potential underlying causes which expose an organization to security incidents occurring but also possible countermeasures which could be instituted by the organization to address these underlying weaknesses.

Finally, we can associate potential failures with a simple threat model to identify risks. This risk selection creates the 'Accident (Security Incident)' category in the generic Accimap. For example, the threats of a cybersecurity attack leading to data theft, a denial of service attack, a malicious action by an insider,*force majeure* and regulatory breaches can serve as an initial set of risk categories allowing potential underlying exposures to such attacks and subsequent failings in security working practice to contribute to probability assessments that attacks may succeed. Combined with a quantitative analysis of risk, this can justify expenditure on cultural and other initiatives to address these problems [6].

6. Wiki Structure

The Wiki structure is headed by two files 'HeadsBySTCategory' and 'GenAccimap'. All files are written in Markdown.

The 'HeadsBySTCategory' file contains the codes and basic definitions for different patterns of behavior or activity in an organization. For example, 'PJM' is the code for project management. The code heading is given in URL form and points to '***Define' file in the structure – here 'PJMDefine' which contains a more detailed definition of the capability or behavior and of the potential consequences of any deficits. For example, weak project management

could lead to security requirements being omitted or delays in delivering such requirements, increasing the risk exposure of the organization.

In turn, the '***Define' files have URLs pointing to categories in the 'GenericAccimap' structure which allow the researcher to link deficits in capabilities or behaviors to different levels of the organization and to consider further effects on other behaviors. Again, to give an example, poor project management may lead to security resources being delivered late. This relates to an area coded 'MAT' for technical capability and materials. Deficits in this area will point to other category levels in the 'GenericAccimap'.

Countermeasures for improving areas are provided in turn [2], e.g., training project managers, having a structured project management methodology and so forth.

It is also possible to start with the 'GenAccimap' file and read across all possible behaviors or capabilities in the model which might affect this area. This kind of approach might be used when building a set of interview questions – see section 7.

7. Proposed Application

The overall structure is intended to promote an exploration of how the organization functions as well as identifying possible countermeasures. The researcher is encouraged to use the initial coding as a basis for further coding and interpretation of the organization's behavior and to revisit interviews or other evidence where appropriate.

The end result of the exploration will be a 'rich picture' of organizational issues which are interlinked and may entail risk exposure. This becomes the basis for building representative Accimaps of the organization for each of the major risks.

The multi-coding framework can be used in several ways. As has already been discussed in section 2, the initial analysis is based on qualitative semi-structured interviews, which can subsequently be backed up by quantitative analysis (based on testing hypotheses derived from the qualitative analysis) and other evidence such as documentation, emails, discussion boards and so forth.

The framework provides a structure for developing leading questions in the semi-structured interviews. It could be potentially used interactively during the interview to follow up on topics. If a more formal approach to interviews is preferred, for example, when using novice interviewers, the same structure can be used to create diagnostic interview sets [19].

The coding process will itself create connections across the framework which may spring further queries in the security experts mind and guide the search for evidence as well as hypotheses relating to potential failures built into patterns of behavior in the organization.

Ultimately, of course, the aim of the process is to produce several hypothetical Accimaps showing how human and management failures as well as weaknesses in process and technology may be contributing directly or indirectly to one or more potential security incidents and to use these as the basis for managing risk in the organization by determining on a set of feasible countermeasures which not only addresses immediate technical flaws but also underlying failings in organization and culture. This process could also be extended to examining the organization's ability to respond to or recover from security incidents [5].

Obviously, the approach can also be applied to security incident analysis and we consider that it may be possible to apply it as a pedagogical and research framework covering the

[2]These are currently in draft, but further detail is being added along with literature references which may prove useful.

human and organizational issues we have identified.

8. Discussion

At this stage, there is no claim that the framework is 'complete' or 'correct'. It is a proposed way of working with an organization, using the Accimap method predictively. As an artefact of design science, the approach is likely to be refined over several studies [13].. What we do argue is that the framework combines extensive experience with the use of Accimap with a coding approach based on specific knowledge and experience in the information systems domain and, as such, it addresses many of the flaws in Accimap, particularly addressing the predictive element which was missing.

It could be argued that the framework may limit the scope of inquiry. It specifies a search for certain patterns of behavior and proposes specific countermeasures. Arguably, additional categories of behavior will be present outside the scope of the framework and some countermeasures may not be suitable for some kinds of organization, or fail to deal with the identified patterns of behavior. But qualitative coding techniques allow for additional 'in vivo' coding if required to cover novel patterns of experience outside those potentially expected [18]. At the same time, the results of the exercise should be open to discussion with experts, management and staff on the ground, if novel solutions are required. As with any sociotechnical approach, the aim is to conjoint optimization of desirable outcomes.

A final consideration is that different sectors of information security (such as telecomms or industrial control systems) may require additional work on the coding frameworks to draw in additional domain specific knowledge. This may ultimately result in creating either an expanded framework or specific frameworks for each subdomain area.

9. Conclusion and Future Work

This paper presents a proposed approach to sociotechnical analysis of cybersecurity risks using the Accimap methodology. The original Accimap approach is seen as flawed for cybersecurity risk analysis due to cost and time considerations and because it does not lend itself to predictive risk assessments.

We address these issues by combining a generic Accimap coding framework with an encoding of specific domain knowledge applicable to negative patterns of human and organizational behavior in information systems and those which are generically applicable to risk management such as good communication.

Data gathering and analysis is done on the basis of several qualitative interviews in the same format, with the same time and resource usage, as a cybersecurity maturity interview, making the approach commercially feasible. The findings in the qualitative interviews can be confirmed through follow up quantitative studies or using documentary evidence in various formats.

Future work will require applying and refining the approach as an artifact of design science to several organizations, preferably in different sub-domains of information systems such as telecomms, banking systems or industrial control systems. The resulting knowledge gain is not only expected to make risk analysis including sociotechnical aspects easier in each of these areas but could also contribute to security incident analysis and to further teaching, training and research.

References

[1] McEvoy, R., Kowalski, S.: Cassandra's calling card: Socio-technical risk analysis and management in cyber security systems

[2] Qureshi, Z.H.: A review of accident modelling approaches for complex critical sociotechnical systems. Technical report, DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION EDINBURGH (AUSTRALIA) COMMAND ... (2008)

[3] McEvoy, T.R., Kowalski, S.J.: Deriving cyber security risks from human and organizational factors–a socio-technical approach. Complex Systems Informatics and Modeling Quarterly (18) (2019) 47–64

[4] Mauw, S., Oostdijk, M.: Foundations of attack trees. In: International Conference on Information Security and Cryptology, Springer (2005) 186–198

[5] Wienen, H.C.A., Bukhsh, F.A., Vriezekolk, E., Wieringa, R.J.: Applying generic accimap to a ddos attack on a western-european telecom operator. In: ISCRAM. (2019)

[6] Baskerville, R.: Risk analysis: an interpretive feasibility tool in justifying information systems security. European Journal of Information Systems **1**(2) (1991) 121–130

[7] Salmon, P.M.: Human factors methods and accident analysis: practical guidance and case study applications. Ashgate Publishing, Ltd. (2011)

[8] Hallett, J., Larson, R., Rashid, A.: Mirror, mirror, on the wall: What are we teaching them all? characterising the focus of cybersecurity curricular frameworks. In: 2018 {USENIX} Workshop on Advances in Security Education ({ASE} 18). (2018)

[9] Salmon, P.M., Hulme, A., Walker, G.H., Waterson, P., Berber, E., Stanton, N.A.: Something for everyone: A generic accimap contributory factor classification scheme

[10] Rea-Guaman, A.M., San Feliu, T., Calvo-Manzano, J.A., Sanchez-Garcia, I.D.: Comparative study of cybersecurity capability maturity models. In: International Conference on Software Process Improvement and Capability Determination, Springer (2017) 100–113

[11] Bostrom, R.P., Heinen, J.S.: Mis problems and failures: A socio-technical perspective. part i: The causes. MIS quarterly (1977) 17–32

[12] Østby, G., Berg, L., Kianpour, M., Katt, B., Kowalski, S.J.: A socio-technical framework to improve cyber security training: A work in progress, CEUR Workshop Proceedings (2019)

[13] Hevner, A.R., March, S.T., Park, J., Ram, S.: Design science in information systems research. MIS quarterly (2004) 75–105

[14] Shen, L.: The nist cybersecurity framework: Overview and potential impacts. Scitech Lawyer **10**(4) (2014) 16

[15] Rasmussen, J., et al.: Risk management in a dynamic society: a modelling problem. Safety science **27**(2) (1997) 183–213

[16] Mumford, E.: The story of socio-technical design: Reflections on its successes, failures and potential. Information systems journal **16**(4) (2006) 317–342

[17] Sasse, M.A., Brostoff, S., Weirich, D.: Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. BT technology journal **19**(3) (2001) 122–131

[18] Saldaña, J.: The coding manual for qualitative researchers. Sage (2015)

[19] Perkins, R.W.: Diagnostic interviewing for consultants and auditors: A collaborative approach to problem solving. Consulting to Management **8**(3) (1995) 70