Developing Contextual Understanding of Information Security Risks

M. Sadok[1], V. Katos[2] and P. Bednar[3]

[1]Higher Institute of Technological Studies in Communications in Tunis, Tunisia
[2]Democritus University of Thrace, Greece
[3]School of Computing, Portsmouth University, United Kingdom
e-mail: moufida.sadok@gmail.com; vkatos@ee.duth.gr; peter.bednar@port.ac.uk

Abstract

Given the uncertainty and complexity of security risk analyses, there is a great need of tools for contextual inquiry supporting assessment of risk with multi-value scales according to different stakeholders' point of view. Such tools can be used at individual level to help develop the understanding of a problem space. At the collective level, they can be used as a mean of communication to support the discussion, comparison and exploration of different understandings. The exploration of multiple perspectives of contextual understanding avoids entrapment in various types of reductionism and eliminates tendencies towards a deterministic reasoning and the pursuit of one optimum solution. A critical challenge is first developing a large spectrum of alternatives and then managing how the differences and similarities between alternatives will be handled to efficiently support decisions in information systems security (ISS). To address the aforementioned challenges, this paper seeks to explore the potential relevance of cognitive maps use in an ISS context to support the exploration of individual understanding leading to richer elaboration of problem spaces.

Keywords

Risk analysis, Systemic risk, Cognitive map, Contextual analysis, Information security, Uncertainty

1. Introduction

In information systems security (ISS), the objectives of the risk analysis process are to help to identify new threats and vulnerabilities, to estimate their business impact and to provide a dynamic set of tools to control the security level of the information system. In their practices, organisations employ and balance between prevention and response security management approaches (Baskerville et al., 2014). Many of the existing risk analysis models and frameworks focus mainly on the technical modules related to the development of security mitigation and prevention and do not pay much attention to the influence of contextual variables affecting the reliability of the provided solutions (Samela, 2008; Siponen and Willison, 2009). Moreover, Siponen and Iivari (2006) identified a gap in research on ISS policies when it comes to handle exceptional situations of business. The importance of context for systemic analysis has been widely recognized (e.g. Checkland, 1981; Checkland and Poulter, 2006; Ulrich, 1983). A systemic view of security would result in a better understanding of

organizational stakeholders of the role and application of security functions in situated practices and an achievement of contextually relevant risk analysis (Bednar and Katos, 2010). The study of Spears and Barki (2010) provides a particular application of this view in the context of regulatory compliance and confirms the conclusion that the engagement of users in ISS risk management process contributes to more effective security measures and better alignment of security controls with business objectives.

Given the uncertainty and complexity of security risk analyses, there is a great need of tools for contextual inquiry supporting assessment of risk with multi-value scales according to different stakeholders' point of view. Such tools can be used at individual level to help to develop the understanding of a problem space. At the collective level, they can be used as a mean of communication to support the discussion, comparison and exploration of different understandings. The exploration of multiple perspectives of contextual understanding avoids entrapment in various types of reductionism and eliminates tendencies towards a deterministic reasoning and the pursuit of one optimum solution. A critical challenge is first developing a large spectrum of alternatives and then managing how the differences and similarities between alternatives will be handled to efficiently support decisions in ISS.

To address the aforementioned challenges, this paper seeks to explore the potential relevance of cognitive maps use in ISS context to support the exploration of individual understanding leading to richer elaboration of problem spaces. A case study is used to illustrate the concept.

The remainder of this paper is organized as follows. In the section 2, a short review of existing ISS models found in the literature is provided. Section 3 discusses the need for particular tools for contextual inquiry under uncertainty and complexity. In Section 4 a case study is given to illustrate the use of cognitive maps. Finally, the conclusive remarks are presented in section 5.

2. Related literature

A number of researchers have addressed the uncertainty and complexity related to ISS applying several theories as well as operations research techniques. The involvement of security experts has been a significant input in many of the models proposed. In Feng and Li (2011), an improved version of the evidence theory is used to deal with the uncertainty in ISS risk assessment. The proposed model requires experts' beliefs inputs to establish the ISS index system and quantify index weights. However, the authors recognise the need to better elicit practitioners' assessments of the strength of the evidence. In practice, the evaluation of risk under uncertainty through index weights appears to be highly structured reductionist and simplistic passing over the subjectivity inherent to any human problem solving process. It is also important to define relevant stakeholders in specific situation of risk analysis. In Ryan *et al.* (2012), the security expert judgment elicitation method is applied to quantify information security risks "where the experts' weights are derived from the

experts' responses to a set of seed variables whose values are known by the analyst and which are used to ''calibrate'' the accuracy of the experts' opinions". This method of codification is based on a list of a pre-determined questions and answers; however, in real world situations a problem space is not 'given' but created by the interest of relevant stakeholders who make use of their own norms and values, derived through experience, in the context of risk analysis. Moreover, it is limiting to disqualify out of context any understanding or analysis developed by any of the involved stakeholders or creates any kind of discrimination between them. All the contextual (and situated) perspectives should be considered as relevant. The concept of weight has also been used in Gupta *et al.* (2006) who propose a genetic algorithm approach to match security technologies to vulnerabilities. Without applying real case studies the techniques described in their approach, the authors argue that the estimation of weights depends on the types and preferences of the organization which will influence the decisions regarding the number of vulnerabilities covered and the cost of implemented security solutions.

Based on the expert's experience and a database of observed cases, Feng *et al.* (2014) develop a security risk analysis model using Bayesian network techniques and ant colony optimisation algorithms. The developed model identifies causal relationships of risk factors and vulnerability propagation analysis. In spite of the interest of the proposed model, it is difficult to apply it in practice to cope with unpredictable risks and more complex security risk analysis problems as the database of observed cases can only support the prediction of already know risks. It is also not apparent how to obtain the data to do so. The judgment of security risks cannot be only based on the security expert experience and knowledge, as the risk is contextually situated (Katos and Bednar, 2008).

Another stream of research in ISS risk assessment draws up on the estimation of likelihood occurrences and impact of vulnerabilities and threats. Sommestad *et al.* (2010) provide an overview of several studies and methods based on probabilistic assessment of security incidents and their potential consequences. However, the discrete and non-linear nature of security failures limits the usefulness and relevance of an assessment based on probabilities (Brooke and Paige, 2003). Sun *et al.* (2006) propose to use the notion of plausibility of a negative outcome to measure ISS risk as it covers residual uncertainty. The authors suggest, for example, Delphi techniques to obtain consensus about values of evidence strength and recognise that the structure of their model is dependent on users' understanding of the interrelationships between risk factors. However, as a consequence of subjectively known contextual dependencies, consensus about values of evidence is not necessarily achievable.

We suggest therefore that two issues need to be further investigated in the field of ISS risk management. First, traditional probability theory is handicapped in the sense that it cannot capture and represent events in an uncertain domain. That is, probabilistic analysis requires that the probability distributions are known for all events. This limitation was initially addressed by Dempster (1967) and further refined by Shafer (1976). According to the Dempster Shafer mathematical theory of evidence (DST), classical probability is extended in such a way that events can be

described at a higher level of abstraction, without requiring one to resort to assumptions within the evidential set. Furthermore, Dempster and Shafer developed an algebraic system to combine events and produce measures for events that can be contradictory.

Classic probability could be viewed as a special case of DST. In DST hypotheses are represented as subsets of a given set. A hypothesis is a statement which holds with some probability. An interesting feature in DST is that the probability assigned to a hypothesis need not be calculated or proven in the classic probability sense. Therefore, a probability can be a person's view on the validity of the respective hypothesis (Katos and Bednar, 2008). Second, the description of a problem space which is uncertain and complex requires the generation of multi-perspectives and mutually inconsistent possible alternatives. Unique perspectives of individual stakeholders may be particularly important in highlighting aspects of a problem situation which may have become 'invisible' due to over-familiarity (Bednar and Welch, 2006). At a collective level, it is important to recognise and consider each individual's unique perspectives without temptation to unify or integrate the differences in a shared understanding of a problem space, to seek a premature consensus or to set up an artificial imposed scale of agreement.

3. Use of cognitive maps for ISS risk analysis

One manoeuvre for coping with uncertainty and unstructured situations involves sense-making and interpretation processes (Weick, 1995). To support such processes of reflection that assign meaning to data cognitive maps are constructed (Daft and Weick, 1984). A cognitive map (CM) consists of nodes and relations an individual uses to develop his/her understanding in specific problem space. When the relations are limited to causality effect cognitive map is the so-called cause map. The nodes are variables that may be continuous or dichotomous and can take on different values (Weick, 2001). Cognitive maps, as a model of thinking, may act as a tool to facilitate decision-making, problem-solving, and negotiation within the context of organizational intervention (Den, 1992).

In the specific context of security risks, each breach provides the opportunity to develop understanding of risk in a way that incrementally allows the improvement of security practices. The development of understanding may not necessarily prevent the next breach but can support the learning about how to manage and respond to unpredictable risks. It is argued in this paper that the exploration and understanding of issues are not only conducted by technical experts in security but also by experts in context such as managers or end users engaged in a specific problem space. Furthermore, given that there are many cases in information security where exceptions need to be made due to the increased complexity of the problem; experts have to face contradicting opinions and problem descriptions. All complex problems suffer from this. For example, conceptual maps and rich pictures are used in Soft Systems Methodology (Checkland, 1981; Checkland and Poulter, 2006) to address complex problems and to support dialogue and conversation about problematic situations. As such, documenting the individual's view of a problem by the means of

cognitive maps may help in the development of more appropriate and flexible security policies and controls.

As there is increased complexity and uncertainty, it is possible that each individual can make more than one description of potential problem issue due to more than one understanding of potential issue (Bednar, 2000; 2007) and so each individual could come up with more than one cognitive map. This would result in more sophisticated cognitive maps at an individual level. Still each individual would potentially end up having more than one cognitive map. The result would be that a group would potentially have more than three cognitive maps to discuss and compare. The following discussion and systematic analysis between individuals could focus on similarities and differences of understanding of individual cognitive maps. Some cognitive maps may be recognized by all individuals in a group as easy to understand but not necessarily to agree upon. Some cognitive maps may be recognized as not easy to understand in the same way but all participants and so should not be aligned with each other. Instead they should be developed and categorized further using heuristics.

Such systematic analysis might support learning about threats and risk. And develop a number of additional and contextually relevant heuristics for continuity of inquiry - a kind of knowledge that the team through these conversations develop a better language for dialogue. It is learning about learning and heuristics which support this learning process. This help the team of professionals to get a better and more developed overview and insight into complexities of problem space and also their common and diverse understandings of the problem space they are interested in.

In terms of security policies and controls, it may mean that there should not be a single policy that will cover the needs of all the involved stakeholders in the risk analysis process. As such, trying to force compliance with one policy (i.e. no exceptions) could lead to problematic security as people will be driven to circumvent the underlying security controls or to give up on their own professional best practices.

4. Case study

In this section we describe three CMs as produced by three stakeholders respectively following a security breach.

ACME Ltd. like many other companies suffered a data breach. Following a preliminary assessment from the security expert, the company was exposed to an Advanced Persistent Threat, as it seemed that the attack was targeted and custom made to exploit the particular security gaps of the company. More specifically the external security expert – who was in fact commissioned to conduct an audit for the company a couple of years ago and had some good knowledge on the security posture of the company – was not surprised, as he had identified several vulnerabilities, most of which were not fully addressed. His view of the possible causes of the breach is captured with the CM as shown in Figure 1.

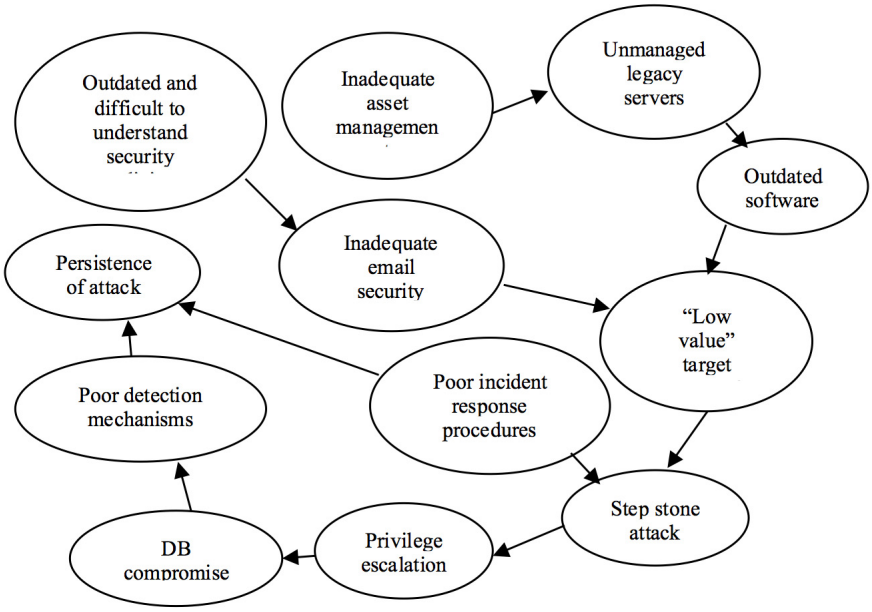

Figure 1: Security expert' CM

However, the systems administrator had a different view of the cause of the attack vector. He did not agree with the security consultant, mainly because the latter had an outdated view of the infrastructure; two years ago the Bring Your Own Device (BYOD) paradigm was not as prevalent and the infrastructure has dramatically changed ever since.

The network perimeter is completely different as many users bring their portable devices in their job environment bypassing most security controls: the firewall is not capable of inspecting and filtering all network traffic, documents and saved on smartphones and laptops in unencrypted forms, users are addicted to downloading a number of apps on the smartphones. As such the administrator is very upset with the plethora of functionality and applications he has no control of and his view of the problem stems from the adoption of BYOD where the company was unprepared to embrace. His CM is presented in Figure 2.

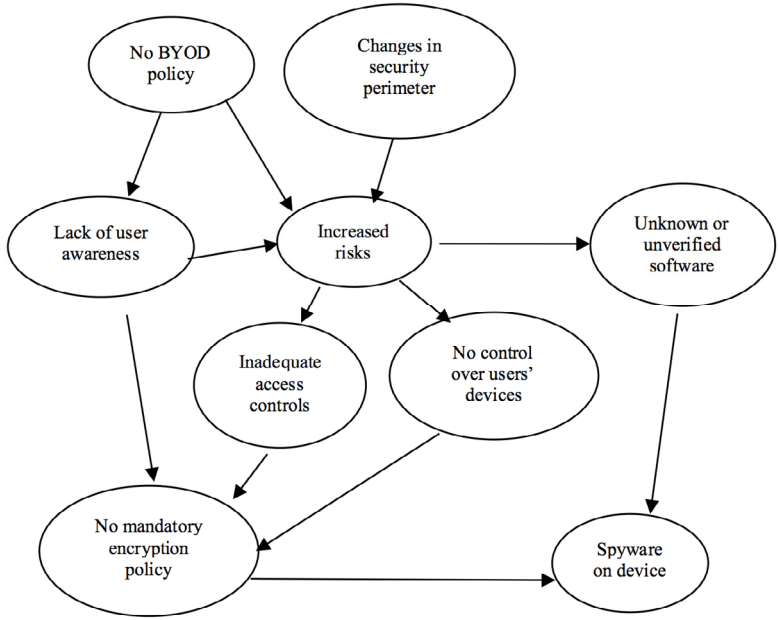

Figure 2: Systems administrator' CM

One of the end users feels somewhat responsible for the breach, as she recalled of two incidents that she did not considered being of significant importance.

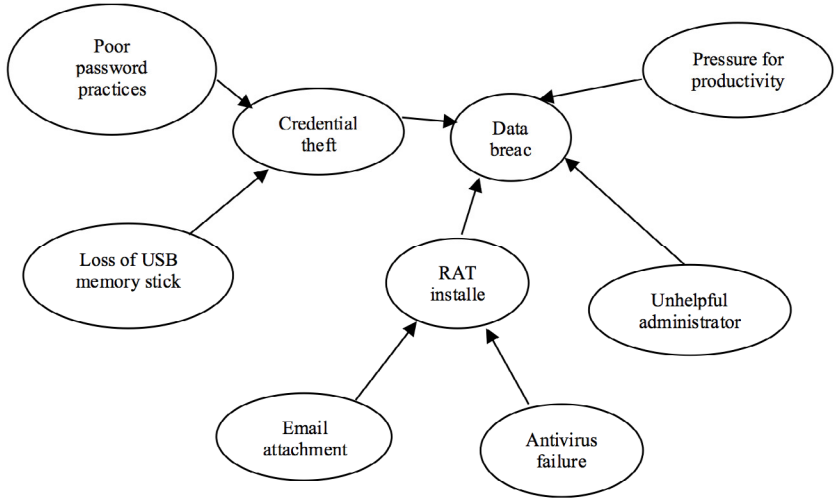

Figure 3: End user' CM

The first incident was an email she received about 8 months ago appearing to be from the Finance Department asking her to complete an attached file with some personal information to receive a salary bonus. The attachment once opened cause her computer to crash and upon rebooting it the email was lost, so she thought that she misunderstood the whole content and context of the email. The second incident involved her losing a USB stick on her way home, about 6 months ago. The USB contained password protected documents, but the password was the same with the one she uses to log into the corporate system. She never reported the incident before, because she did use password protection on USB device, but after talking to the security expert, she realized that the password was perhaps weak and could have been recovered. Her view of the cause of the breach is captured in the CM in Figure 3.

For the above CMs the following assumptions can be made:

- Each stakeholder assumes that his/her CM is correct and represents his/her true understanding of reality,
- While the stakeholders might not agree with each other they all want to solve the problem,
- All CMs could potentially be contextually relevant, more or less correct or wrong.

The benefit of having multiple CMs supports the exploration of a wider problem space from multiple perspectives. This is particularly useful in the case where the attack vector is unknown.

The involved stakeholders try to understand and compare through structured discussions the similarities and differences between their views of the problem space as described by their respective CMs. Each stakeholder can identify relationships between all of the CMs and categorize similarities and differences. The categorization can be made using an appropriate reasoning tool such as paraconsistent logic that allows ambiguity and uncertainty in judgement to be expressed. This can also be done by the application of methods such as the Diversity Network (e.g. Katos *et al.* 2006). As the three CM's describe three potentially different and incompatible understandings of what ought to be a relevant attack vector to address, more than one security policy could be delivered. Furthermore more than one perspective allows the organization to better identify vulnerabilities and threats, and eventually implement more appropriate security controls and policies.

5. Conclusion

This paper explored security risk analysis as an example of an inquiry into a complex, ambiguous and uncertain problem space. As such the process needs to support stakeholders to develop a widening of problem understanding before stakeholders commit to a problem definition. This is done through developing multiple contextual understandings of information security risks by using CMs

which then are used by stakeholder in a dialogue for the discovery and description of relationships between the CMs as understood by each stakeholder. The objective with this effort is not to merge, integrate or combine different CMs as it might lead to framing stakeholders' perspectives and views. Instead we argue that there must be recognition in the problem identification process that stakeholders may have different subjective and potentially valid problem experiences. We suggest the consideration of multiple security policies to reflect the differing CMs of experts, managers and users. We recognise that there is a limit to how many CMs will be used in practice. Then a relevant question for future research would be how to determine and incorporate the chosen CMs.

This work would benefit from further developing of how frameworks such as Strategic Systemic Thinking (e.g. Bednar, 2000) and methods such as diversity networks could be applied in the identification process of similarities and differences between multiple CMs. It would also aid in the decision making processes among the involved stakeholders.

6. References

Baskerville, R., Spagnoletti, P. and Kim, J. (2014), "Incident-centered information security: Managing a strategic balance between prevention and response", *Information & Management*, Vol. 51, pp138-151.

Bednar, P. and Katos, V. (2010), "Digital forensic investigations: a new frontier for Informing Systems", in D'Atri, A. and Sacca, D. (Ed.) *Information Systems: People, Organizations, Institutions and Technologies*, Springer Physica-Verlag, Berlin Heidelberg, ISBN: 978-3-7908-2147-5.

Bednar, P. and Welch, C. (2006), "Structuring uncertainty: sponsoring innovation and creativity", in Adam, F. et al. (Ed.) *Creativity and Innovation in Decision Making and Decision Support*, London, Decision Support Press, ISBN: 1-905800-00-2.

Bednar, P.M. (2000), "A Contextual Integration of Individual and Organizational Learning Perspectives as part of IS Analysis", *Informing Science Journal*, Vol. 3, No. 3, pp145-156.

Bednar, P.M. (2007), "Individual emergence in contextual analysis", *Problems of Individual Emergence: Special issue of Systemica*, Vol. 14, pp23-28.

Brooke, P.J. and Paige, R.F. (2003), "Fault trees for security system design and analysis", *Computers & Security*, Vol. 22, No. 3, pp256-264.

Checkland, P. (1981), Systems Thinking, Systems Practice, John Wiley & Sons, Chichester, ISBN 0471279110.

Checkland, P. and Poulter J. (2006), Learning for Action, John Wiley & Sons, Chichester, ISBN 100470025549.

Daft, R.L. and Weick, K.E. (1984), "Toward a Model of Organizations as Interpretation Systems", *Academy of Management Review*, Vol. 9, No. 2, pp284-295.

Demspster, P. (1967), "Upper and lower probabilities induced by a multivalued mapping", *Annals of Statistics*, Vol. 28, pp325-339.

Den, C. (1992), "On the nature of cognitive maps", Journal of Management Studies, Vol. 293, pp261-265.

Feng, N. and Li, M. (2011), "An information systems security risk assessment model under uncertain environment", *Applied Soft Computing*, Vol. 11, pp4332–4340.

Feng, N., Wang, H. and Li, M. (2014), "A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis", *Information Sciences*, Vol. 256, pp57–73.

Gupta, M., Rees, J., Chaturvedi, A. and Chi, J. (2006), "Matching information security vulnerabilities to organizational security profiles: a genetic algorithm approach", *Decision Support Systems*, Vol. 41, pp592-603.

Katos, V. and Bednar, P. (2008), "A cyber-crime investigation framework", *Computer Standards & Interfaces*, Vol. 30, pp223–228.

Katos, V., Bednar, P. and Welch, C. (2006), "Dealing with epistemic uncertainty in the SST framework", in Adam, F. et al. (Ed.) *Creativity and Innovation in Decision Making and Decision Support*, London, Decision Support Press, ISBN: 1-905800-00-2.

Ryan, J.J.C.H., Mazzuchi, T.A., Ryan, D.J., Lopez de la Cruz, J. and Cooke, R. (2012), "Quantifying information security risks using expert judgment elicitation", *Computers & Operations Research*, Vol. 39, pp774–784.

Salmela, H. (2008), "Analysing business losses caused by information systems risk: a business process analysis approach", *Journal of Information Technology*, Vol. 23, pp185-202.

Shafer, G. (1976), *A Mathematical Theory of Evidence*, Princeton University Press, ISBN: 9780691100425

Siponen, M. and Iivari, J. (2006), "Six design theories for IS security policies and guidelines", *Journal of the Association for Information systems*, Vol. 7, No. 7, pp 445-472.

Siponen, M. and Willison, R. (2009), "Information security management standards: Problems and solutions", *Information & Management*, Vol. 46, pp267-270.

Sommestad, T., Ekstedt, M. and Johnson, P. (2010) "A probabilistic relational model for security risk analysis", *Computers & Security*, Vol. 29, pp659-679.

Sun, L., Srivastava, R.P. and Mock, T.J. (2006) "An Information Systems Security Risk Assessment Model Under Dempster-Schafer Theory of Belief Functions", *Journal of Management Information Systems*, Vol. 22, No. 4, pp109-142.

Ulrich, W. (1983), *Critical Heuristics of Social Planning*, Wiley, Chichester, ISBN: 0-471-95345-8.

Weick, K. (1995), *Sense-making in Organizations*, Sage Publications, London, ISBN:0-8039-7176-1.

Weick, K. (2001), *Making sense of the organization*, Blackwell Publishers, Oxford, ISBN: 0-631-22317-7.