Contextual Dependencies in Information Systems Security

Bednar, Peter; Sadok, Moufida; Katos, Vasilis

Published in:
AIS SIGSEC and IFIP TC 11.1

2013

Bednar P., Sadok M. and Katos V. (2013). "Contextual Dependencies in Information Systems Security. AIS SIGSEC and IFIP TC 11.1 *Workshop on Information Security & Privacy*, WISP 2013, Milan, Italy, 2013.

CONTEXTUAL DEPENDENCIES IN INFORMATION SYSTEMS SECURITY

Authors:

Bednar Peter, School of Computing, University of Portsmouth, UK [peter.bednar@port.ac.uk]

Sadok Moufida, Higher Institute of Technological Studies in Communications in Tunis, Tunisia

Katos Vasilios, Electrical and Computer Engineering, Democritus University of Thrace, Greece

ABSTRACT

This paper addresses the contextual dependencies related to the use of information systems security and criticizes the predominance of technical and formalized paradigm in the development and implementation of IS security policies and procedures. The underlying epistemology of our research lies in the interpretative paradigm. It explores the patterns of how the contextual use of information systems security is involved according to a business/organizational practice perspective. It elicits the detailed processes and practices that constitute the pragmatic perspective in developing information security activities.

KEY WORDS

Information systems security, contextual analysis, socio-technical analysis, user engagement, information systems methodologies

CONTEXTUAL DEPENDENCIES IN INFORMATION SYSTEMS SECURITY

INTRODUCTION

Although there is a wide consensus in the information systems (IS) community that security should be incorporated in the complete IS analysis, development and implementation process, systematic and systemic treatment of systems analysis and development with elements of information systems security (ISS) seemed to exhibit some belatedness. Siponen (2005) draws a distinction between IS, software engineering, computer science and mathematics and associates the different research communities with the mentioned disciplines. As such, researchers in the area of computer science and mathematics have a positivist orientation, whereas researchers in IS often subscribe to the interpretive paradigm. Irrespective of the separation between computer science and software engineering, it appears that the crucial factor that had an impact on the inclusion (or exclusion) of security practices in IS methodologies was the interpretivism vs. positivism view. For example in the commonly available academic reference work on IS development by Avison and Fitzgerald (2006), the reference to data centric focus of security is very pertinent. While ISS is not inherently excluded from IS development methodologies it is contextually taken for granted (e.g. not made explicit). IS methodologies mention security without explicitly providing methods for its implementation. Explicit ISS appears to fall mainly under the computer science discipline (usually positivist with an inherent focus on artefact development), strongly coupled with mathematics approaches (such as cryptography for example). A conceptual approach focusing on rational and formal descriptions leads work intended to cater for ISS in practice to almost solely focus upon data systems security. Therefore the result would tend to be developed independently of the needs of the surrounding human

activity system. Unfortunately, ISS is dependent on human motivation and behaviour within the stakeholder context. This conceptual and paradigmatic mismatch explains the language espoused where people talk about "educating the user"; "train the user"; "make the user follow proper security procedures" and so on. It ignores the fact that as change is required from the user the system as a whole (human activity system) obviously was either not designed at all explicitly but as a result of unintended consequences of data system security design. The problem with requiring people to change behaviour is that any professional activity is dealt with in an effective way due to some contextually relevant reason. To request people to change behaviour is to try to change organizational practices without understanding the effective behaviour of the involved stakeholders in the first place. We argue that a monolithic secure systems development methodology would be of limited value to IS. ISS functions are dependent on both human and infrastructural elements of an IS and should not be considered in isolation from each other.

The remainder of the paper is organized as follows. First, a review of existing practices found in the literature is presented. We move on to present highlights from the IS and secure systems domains, leading to the main contribution of this paper which is the identification of contextual perspectives of information systems security.

EXISTING PRACTICES AND RELATED WORK

According to the CSI (2011), CLUSIF (2012) and PWC (2012) reports an important percentage of the interviewed enterprises have proceeded to the formalization of their security policies and the assessment of security risks. The vast majority of them use different types of security technology and mainly antivirus software, firewall and intrusion detection system. A number of available standards (e.g. ISO 27001), guidelines (e.g. Risk Management Guide for Information Technology Systems), best practices frameworks (e.g. Information Technology Infrastructure

Library) and methods (e.g. Operationally Critical Threat Asset and Vulnerability Evaluation) exist to assist organizations to manage information security, analyze risks and set-up efficient controls. The main recommendations of these reports are in favor of more training and education for the staff to guarantee more compliance to security policy guidelines as well as the formalization of the security organizational procedures to have more "standardized behavior".

However, the existence of a security policy by itself does not mean its efficient application or relevance. In the case of the UK businesses (PWC 2012), 21% think the level of staff understanding is poor. The CLUSIF 2012 report shows that only 19% of the interviewed enterprises take into account the business process and not only focus on the data processes while analyzing risks. The internal security experts are the most common involved source in the assessment of security threats (CLUSIF 2012, PWC 2012). The malware infection, phishing, data corruption and laptop theft are the most type of attacks experienced according to the aforementioned reports. In fact, the employed security technologies can only prevent the already-known attacks.

One could furthermore argue that these reports are adopting a formal approach of security and confusing between information systems security and data systems security. The focus on a model of business process, rather than on a real world organizational context: As is clearly visible in the confusion between the territory and the map identifiable in IS analysis and design practices (Bednar, 2007). This means that ISS cannot be an add - on but has to be an intertwined aspect of any IS design effort and change practice. Security processes which are modeled outside of the real world organizational context are prone to antagonize effective organizational practices and the literature maintains a plethora of such real world cases (Bednar and Katos, 2009). In the case study conducted by Kolkowska and Dhillon (2013), the workers noted that "The checks and

balances that have been built into the system are not necessarily the way in which any of the case-workers operate" (ibid, p.8) and "They were also threatening us about the consequences of non-compliance. Nobody however focused on the reasons why people were not complying to the security rules" (ibid, p.10). In the ISS literature, various studies have argued for practice-based organizational frameworks of security policies and controls. The issues explored in this stream of studies cover the influence of the contextual factors such as national culture (Yildirima et al., 2011), organizational structure and culture, management support, training and awareness, users' participation in the formulation process, business objectives, legal and regulatory requirements (Karyda et al., 2005; Knapp et al., 2009). Another focus of attention of ISS researches has been the compliance of employees to security procedures and guidelines viewed from behavioral perspective and applying socio-cognitive theories (Herath and Rao, 2009; Ifinedo, 2012; Vance et al., 2012). Although understanding how organizational and environmental factors as well as compliance behavior may affect the efficient use of security controls questions about the relevance of security policies and measures are not addressed. The proposed models and frameworks focus more on the application of security policies, consider the need to shape and monitor the behavior of employees to ensure compliance with security requirements, and sustain the assumption that ISS is an add-on. We believe that the influence of users is crucial mainly in the early steps of the definition of security scope and objectives.

ANALYSIS AND DESIGN OF SECURE SYSTEM

As security analysis is closely coupled with risk analysis, the CRAMM methodology (UK's Central Computing and Telecommunications Agency's Risk Analysis and Management Method) is a widely used risk analysis methodology. The identification of context according to CRAMM is based on the submission of questionnaires to systems users particularly data groups are

employed to identify the sensitive assets and address the threats and vulnerabilities related to the identified assets. However, the assessment of security risks and threats needs tools for contextual inquiry under uncertainty and complexity (Katos and Bednar, 2008; Bednar and Katos, 2010).

The specific security methods, methodologies and standards are generally speaking structured, formalized, systematic and focus on formal behavior and actions of organizational members. To develop models of human behavior based on description of organizational activity will have little real world significance as can be seen through the history of IS development failures (see for example Morton and Hu (2008) analysis of ERP projects failure because the implementation is based on a technical-requirements rather than on business needs or context focus). A very possible attitude in organizational behavior is that security issues are turned a blind eye to. It is possible that in many organizations it is not acceptable to highlight security threats. The breaches security surveys outline the embarrassment of the interviewed enterprises about reporting the intrusions to third party outside the organization. People may not "want to know", some will experience comments on weaknesses in security as comments on their personal competence. To highlight security threats brings with it several organizational, social and cultural dangers. People could find themselves accused of being a security threat, e.g. "if you had not mentioned the security threat it would not have been known and therefore not a problem". This kind of phenomena means that there are real organizational incentives not to discuss or make an effort to prove any threat as that in itself would by definition be a breach of security and the employee might not be treated well as a result. People's unwillingness to admit and highlight real security threats could be justified by the introduction of regulatory controls and compliance (e.g. Sarbanes-Oxley Act) which attempts to remedy this issue to some extent. By failing to appreciate the complex relationships between use, usability and usefulness, the security procedures imposed

are not only subject to possible misuse but they are likely to be a core hindrance to everyday legitimate work. The weakest link is not necessarily in the (technical) system itself but the difference between the formal model of usage and real usage of system content (data) as such in a human activity system. This realization leads Tryfonas et al. (2001) to propose an interpretive framework for expanding and incorporating the security functions in the whole IS development.

CONTEXTUAL PERSPECTIVES OF INFORMATION SYSTEMS SECURITY

In order to demonstrate the importance and necessity of the contextual dimension in the design of a secure information system, consider the case of the White Hats, Grey Hats and Black Hats. All three types of hackers employ the same modus operandi of breaking into systems, but with from different ends. White Hats are supposed to be the good guys, Grey Hats are supposed to be those White Hats who pretend to be Black Hats (that is the devil's advocate), for example to test security measures. Black Hats are the bad guys. It is sometimes suggested (e.g. Mahmood et al. 2010) that there is a lot of research focusing on White Hats and not as much on Black Hats. But such a suggestion may be misleading as it is far from clear who is or is not White or Black Hat. In research White Hats are often assumed to be those who develop, promote and apply security policies and practices. Those who circumvent security policies and procedures for their personal gain are assumed to be Black Hats. A security breach is assumed by many security researchers to be identical with breach of security policy, further more it is also often automatically assumed to be causing damage to the business. However if policy was developed as an add-on to the real world business practices it is quite possibly the case that breach of security policy may in some instances be necessary as in practice it might be the only way for an employee to do a good job. The relevant consequential focus in security research is then taken for granted to be how to create countermeasures 'so designed to lessening the damage caused'. So instead of helping

business actors to identify those security breaches that are the result of de-contextualized policy making practices, this particular agenda can lead IS Security professionals to fail to recognize the real underpinning reasons for particular stakeholder behaviour. Explicitly ISS people are looking for how to create not just countermeasures but also retributions for violations of security measures. Research is suggested to be focused on collecting (what is assumed to be) black hat data by studying 'those employees who do not have privileges on certain resources and yet make consistent attempts to access those resources.' Such behavior is assumed to be 'an insider threat' and recommendations are made to look at 'log data of enterprise single sign-on systems that typically monitor all authentication and authorization activities'. Unfortunately such data collection does not say anything about the reasons for why people feel it necessary to access resources which they have no official privileges for and so does not help to question the management assumptions about the appropriateness of any particular security policy in context of the real world work situation. Additionally to automatically treat employees as threat and suspects is a sure way to alienate those very employees that the management would like to have motivated for best business practice. Furthermore, the inherent political aspects and hidden agendas of information security controls may have an adverse effect on the goals of information security. For example, the access control for information security tasks is a component of the widely used information security standard ISO 27001. In practice, the choice and implementation of access control mechanisms are in a large extent influenced by the determination of the top managers to control the visibility, transparency and traceability of information flow in the organization. In this setting, security arguments can be used to sustain an organizational power game and defensive routines which limit the use of cognitive capacities, block communicative action and support a functional stupidity as described by Alvesson and Spicer (2012). The IS

users are under the control of the organization and afraid to lose their job will follow norms and rules even when they are not convinced about their appropriateness. Moreover, the use of quantitative metrics in the setting of a bureaucratic and centralized management to measure the productivity implies more formalization of procedures, practices and control mechanisms.

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, 2009). 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.

CONCLUSION

Security considerations have to be present as early as the design phase as it has been demonstrated historically that if security is treated as an afterthought and a bolt-on to the system, it will not serve its purposes. The data centric focus influences work practices and creates unintended consequences and changes in a human activity design instead of being a part of its design. Samela (2008) considers that business process analysis is understudied method when it comes to assess IS risks. Moreover, IS analysis should understand and include the irrational behavior of the users. Ariely (2008) discusses assumptions about rational decision making process and argues for example that when it comes to motivation social norms could potentially be more powerful and efficient than money. Misleading assumptions about rational and irrational behavior of users may explain many security measures failure. In this paper we argued that the challenge of introducing security in a sensible and useful manner can be addressed by

considering the contextual perspectives. This conclusion can also be expressed in the following terms: "*Knowing that systems with potential for meaningful use are available is a necessary, but not sufficient, condition to bring about desire for use in any particular individual. Work of developers is often perceived within a narrow, largely (socio-) technical definition of information systems. However, it must be recognized that such systems are inherently dependent not only upon their social but also individual and cultural sense-making context"*. (p. 53. Bednar and Welch, 2006).

REFERENCES

Alvesson, M., and Spicer, A. 2012. "A stupidity-Based Theory of Organizations", *Journal of Management Studies* (49:7), pp. 1194-1220.

Avison, D., and Fitzgerald, G. 2006. *Information Systems Development: Methodologies, Techniques and Tools*, 4th edition, London: McGraw- Hill.

Ariely, D. 2008. *Predictably Irrational*, New York: HarperCollins.

Bednar, P.M. 2007. 'Individual emergence in contextual analysis', Problems of Individual Emergence: Special issue of *Systemica*, 14(1-6), pp. 23-28.

Bednar, P., Katos, V. 2009. "Addressing the human factor in information systems Security", In 4th Mediterranean Conference on Information Systems, MCIS, Athens.

Bednar, P., Katos V. 2010. "Digital forensic investigations: a new frontier for Informing Systems". In D'Atri A., and D. Saccà. (eds.) *Information Systems: People, Organizations, Institutions and Technologies*. Berlin Heidelberg: Springer Physica-Verlag. pp. 361-372.

Bednar, P.M. and Welch, C. 2006. 'Incentive and desire: covering a missing category' MCIS 2006. Proceedings of the Mediterranean Conference on Information Systems, Venice, Italy.

CLUSIF, 2012. "Menaces informatiques et pratiques de sécurité en France", www.clusif.asso.fr

CSI, 2011. "Computer Crime and Security Survey", http://www.gocsi.com.

Herath, T., and Rao, H.R. 2009. "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness" *Decision Support Systems* 47, pp. 154–165.

Ifinedo, P. 2012. "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory", *Computers & Security* (31), pp. 83-95.

Karyda, M., Kiountouzis, E., and Kokolakis, S. 2005. "Information systems security policies: a contextual perspective", *Computers & Security* (24), pp. 246-260.

Karyda, M., Kokolakis, S., and Kiountouzsi, E. 2001. "Redefining Information Systems Security: Viable Information Systems" Proceedings of the 16th IFIP International Conference on Information Security, M. Dupuy, P. Paradinas (Eds.), pp. 453-467.

Katos, V., and Bednar, P. M. 2008. "A cyber-crime investigation framework", *Computer Standards & Interfaces* (30), pp. 223–228.

Knapp, K. J., Morris, F., Marshall, T. E., and Byrd, T. A. 2009. "Information security policy: An organizational-level process model", *Computers & Security* (28), pp. 493–508.

Kolkowska, E., and Dhillon, G. 2013. "Organizational power and information security rule compliance", *Computers & Security* (33), pp. 3-1 1.

Mahmood, M.A., Siponen, M., Straub, D., Rao H.R. and Raghu, T.S. 2010. "Moving toward black hat research in information systems security". *MIS Quarterly* (34:3), pp. 431-433.

Morton, N. A., and Hu, Q. 2008. "Implications of the fit between organizational structure and ERP: A structural contingency theory perspective", *International Journal of Information Management* (28), pp. 391- 402.

PWC. 2012. "Information security breaches survey technical report", available at www.pwc.co.uk

Salmela, H. 2008. "Analysing business losses caused by information systems risk: a business process analysis approach", *Journal of Information Technology* (23), pp. 185–202.

Siponen, M. 2005. "Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods", *Information and Organization* (15), pp. 339-375.

Spears, J. L. and Barki, H. 2010. "User participation in information systems security risk management**"**, *MIS Quarterly* (34:3), pp. 503-522.

Tryfonas, T., Kiountouzis, E., Polymenakou, A. 2001. "Embedding security practices in contemporary information systems development approaches", *Information Management & Computer Security*, (9:4), pp. 183-197

Vance, A., Siponen, M., and Pahnila, S. 2012. "Motivating IS security compliance: Insights from Habit and Protection Motivation Theory", *Information & Management* 49, pp. 190–198.

Yildirima, E. Y., Akalpa, G., Aytacb, S. and Bayramb, N. 2011."Factors influencing information security management in small-and medium-sized enterprises: A case study from Turkey", *International Journal of Information Management* (31), pp. 360-365.