# Understanding Security Practices Deficiencies: A Contextual Analysis

Sadok, Moufida; Bednar, Peter

*Published in:*
Human Aspects of Information Security and Assurance Conference Proceedings

2015

# Understanding Security Practices Deficiencies: A Contextual Analysis

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

[1]Higher Institute of Technological Studies in Communications in Tunis, Tunisia
[2]School of Computing, University of Portsmouth, UK
[3]Department of Informatics, Lund University, Sweden
E-mails: Moufida.sadok@port.ac.uk, peter.bednar@port.ac.uk

## Abstract

This paper seeks to provide an overview of how companies assess and manage security risks in practice. For this purpose we referred to data of security surveys to examine the scope of risk analysis and to identify involved entities in this process. Our analysis shows a continuous focus on data system security rather than on real world organizational context as well as a prevalent involvement of top management and security staff in risk analysis process and in security policy definition and implementation. We therefore suggest that three issues need to be further investigated in the field of information security risk management in order to bridge the gap between design and implementation of secure and usable systems. First, there is a need to broaden the horizon to consider information system as human activity system which is different from a data processing system. Second, the involvement of relevant stakeholders in context for risk analysis leads to better appreciation of security risks. Third, it is necessary to develop ad-hoc tools and techniques to facilitate discussions and dialogue between stakeholders in risk analysis context.

## Keywords

Information security, Risk analysis, Security practices, Contextual analysis, Security surveys

## 1. Introduction

Security surveys published in many countries by professional bodies provide an overview of security practices of companies. The analysis of these surveys also provides opportunities to reflect on ways how companies deal with increasing security risks. This paper considers three security surveys published in USA, UK and France. Hence, the focus will be not just on describing security practices, but, rather, on the identification of gaps in such practices and alternative perspectives for better management of security risks. In fact, the trend towards social networking, BYOD and cloud computing technologies among other factors has increased security vulnerabilities and threats.

The key findings of several security surveys reveal that companies are struggling to keep up with security risks (e.g. The Global State of Information Security Survey, 2014; 2015; Symantec Internet Security Threat Report 2014; 2015). In particular, enterprises experience difficulties in assessing and managing their security risks,

applying appropriate security controls, as well as preventing security threats. These findings also indicate that security controls and procedures deployed by enterprises cannot match the requirements of their real business processes.

We argue in this paper that two reasons could potentially explain the poor effectiveness of the implemented security solutions and procedures: the boundary problem of risk analysis scope and the background of involved actors in risk assessment and in security policy design. The drive for change is three-fold: first, we realized that security surveys are adopting a formal approach of security and are confusing information systems security with data systems security; second, we can draw a correlation between this perspective and security practices patterns; and third, we provide alternative perspectives on the process and practice of security risk management to handle an effective alignment of security controls with business requirements.

The remainder of the paper is organized in three sections. The first section introduces related literature in practice-based information systems security (ISS). The second section reports key findings of security surveys in USA, UK and France. The third section discusses identified gaps in security practices and proposes alternative perspectives to address deficiencies in security design and implementation. The conclusion sets up a research agenda for potential future works.

## 2. Background

In the ISS literature, a wealth of prior research sheds light on many ways that organizations can use to take into consideration contextual factors such as national culture as (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; Shropshire et al., 2015).

It is also acknowledged that security measures 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. 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". By failing to appreciate the complex relationships between use, usability and usefulness, security procedures imposed are not only subject to possible misuse but they are likely to be a core hindrance to everyday legitimate work. Albrechtsen (2007) has furthermore identified that an increased security workload might create difficulties for work functionality and efficiency. The author also noticed a trivial effect of documented requirements of expected information security behaviour and general awareness campaigns on user behaviour and awareness. The study of Parsons et al., (2014) has also noticed the

lack of efficiency of generic courses based on a lecture on knowledge of security policy and procedure.

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. Consequently, designers have to find a balance between security, performance and usability (Sommerville, 2011) and IT specialists should also continue to work on methods that minimize inconvenience and delays (Oz and Jones, 2008).

The implementation of a security policy is also expected to change organisational procedures and practices as well as to shape and monitor the behavior of employees, through education and training, to ensure compliance with security requirements. Bocij *et al.*, (2008) argued for the formulation of a comprehensive policy on security in order to ensure employees adhesion to policy guidelines. Albrechtsen and Hovden (2010) discussed ways in which security awareness and behaviour may be improved and changed through dialogue, participation and collective reflection. In addition, one line of solution is to enhance the situational awareness that involves an intelligence-driven process to systematically collect and analyse security risk data prior to decision-making (Webb *et al.*, 2014; Franke and Brynielsson, 2014).

To attempt to explain why deficiencies in the practice of information security risk assessment occur, a stream in ISS research has focused on the background of involved actors in risk analysis and security policy processes. For example, Samela (2008) pointed out that business process analysis is an understudied approach when it comes to assess ISS risks. In most of the companies, professionals with operational knowledge pertinent to risk analysis are not efficiently involved (Shedden et al., 2011). Therefore, there is a need to conduct risk analysis activities by business process owners (Coles and Moulton, 2003). Taking several researches recommendations that emphasize the centrality of human and social issues in information security, Reece and Stahl (2015) have discussed new areas of competences that can potentially be used to found a new claim of professional identity of information security practitioner. The authors recommend including particular skills and knowledge in undergraduate socialisation and training.

In order to demonstrate the importance and necessity of the contextual dimension in the design of a secure information system, 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. A systemic and value-focused 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; Dhillon and Torkzadeh, 2006). Therefore, a holistic security strategy needs to include human aspects as a core part of secure and usable systems (Furnell and Clarke, 2012).

## 3. Existing practices

While information security risks have evolved and financial costs of cybercrime have increased, security practices and strategies have not adequately kept up with dynamic and challenging attacks that are highly complex and difficult to detect.

According to the PwC-US (2014), CLUSIF (2014) and PwC-UK (2014) reports an important percentage of the interviewed enterprises have proceeded to the formalization of their security policies. However, the existence of a security policy by itself does not mean its efficient implementation or relevance. In the case of the UK businesses, only a quarter of respondents with a security policy believe their staff have a very good understanding of it. Moreover, 70% of companies where security policy was poorly understood had staff-related breaches versus 41% where the policy was well understood.

As to security risk analysis, although there is a wide consensus that security is a high priority PwC-US (2014) report shows that only 38% align their security spending with business strategy and most of the interviewed enterprises do not implement the tools and processes necessary for a comprehensive assessment. In PwC-UK (2014), 20% of the respondents have not carried out any form of security risk assessment and many organisations still struggle to evaluate the effectiveness of their deployed security controls. In addition, an organization needs to classify its information assets in accordance to their business value and sensitivity in order to ensure an effective protection. Information assets inventories and classification help organizations to perform security risk assessment and to delimit the required protection levels as well as to ensure cost effectiveness of implemented security measures. In the case of US businesses, only 17% classify the business value of data. PwC-UK (2014) report indicates that large organisations seem to struggle to clearly define responsibilities for owning critical data and for protecting it. Also 20% said the responsibilities are not clear and, none believe the responsibilities were very clear. Discussions with senior management and views of internal security experts remain the most popular other sources for evaluating cyber threats. Large organisations rely on external security consultants and alerts from government/intelligence services.

In France, Clusif (2014) provides an extensive overview of security practices of 350 companies and 150 hospitals. Table 1 illustrates that a relatively large (47%) percentage of enterprises and hospitals (41%) do not carry any risk analysis. This could be related in some extent to the lack of data classification which is a necessary input to risk analysis process.

| | Data inventory | | Risk analysis | |
|---|---|---|---|---|
| | **Companies** | **Hospitals** | **Companies** | **Hospitals** |
| **Yes, totally** | **31%** | **17%** | **21%** | **19%** |
| **Partly, data system** | **14%** | **30%** | **22%** | **27%** |
| **Partly, data jobs** | **21%** | **25%** | **8%** | **13%** |
| **No** | **32%** | **25%** | **47%** | **41%** |

**Table 1: Percentage of enterprises and hospitals carrying out data classification and risk analysis, adapted from Clusif (2014)**

Another aspect comes out this table is when a data inventory is achieved, it is clearly focusing on data system as data related to particular activities or jobs are mostly overlooked.

Delving into the background or organizational position of involved entities in risk analysis and security policy formulation reveals some interesting findings. For companies, Clusif survey respondents report a significant influence of top management and IS directorate on security policy definition. In table 2, only 12% of respondents involve directors of business activities such as marketing or production in security policy design. Parsing further Clusif data, we noticed that the hierarchical reporting of ISS executive belongs to IS directorate in 46 % of the cases and to top management in 27 %.

| | **Security policy** | **Risk analysis** |
|---|---|---|
| **Top Management** | **50%** | **-** |
| **IS Directorate** | **54%** | **-** |
| **ISS Executive** | **39%** | **56%** |
| **Job Director** | **12%** | **12%** |

**Table 2: Involved entities in risk analysis and security policy definition, adapted from Clusif (2014)**

When it comes to areas of risk mitigation, most organizations are still focused on updating their technologies and providing more training and education for staff to guarantee more compliance to security policy guidelines as well as the formalization of the security organizational procedures to have more "standardized behavior" (PwC-UK, 2014; Clusif, 2014). This leads to the conclusion of the predominance of

technical and formalized paradigm in the development and implementation of IS security policies and procedures.

## 4. Discussion

A comprehensive review of security surveys has highlighted a number of gaps in security practices. Essentially, we consider that the distinction between IS as a data processing system and IS as a human activity system provides a frame of reference to explain the reasons why the gaps in matching security practices to organizational and business needs continue to be relevant issues to explore in IS security research. Therefore, we first argue for broadening the scope of security risk analysis; Second, involving relevant stakeholders in context and third further investigating techniques and methods to allow discussion and develop understanding of security risks in uncertain and complex environment.

The data centric focus in ISS practices influences work practices and creates unintended consequences and changes in a human activity design instead of being a part of its design. The prevalence of centralized security controls and related top-down management are challenged by dynamic business and technological environments. Basing security risk analysis solely on data system, and ignoring human activity system, means that misleading assumptions about rational and irrational behaviour of users may explain many security measures failure. If security policy and procedures were 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. Filkins B. (2013) illustrates this misfit in the case of the help desk services which are not consider enough in risk analysis scope even though they could be a vulnerable entry point to conduct social engineering attacks or to disclosure sensitive data.

Taking a proactive approach to develop a holistic security strategy, systemic risk analysis requires attention be paid to the background of involved actors in this process. The challenge of introducing security in a sensible and useful manner can be addressed by considering the contextual perspectives. By considering the human activity systems as a point of reference rather than a variable IS development process as an ongoing contextual inquiry (Bednar, 2000; 2007; Bednar and Welch, 2014) is characterized as an emergent systemic change process conducted through sense making and negotiations among relevant stakeholders. From a socio-technical perspective, it is claimed that a viable system would be more user-centric by accommodating and balancing human processes rather than entertaining an expectation of a one sided change of behavior of the end user.

As noted in security surveys, the involvement of security experts has been a significant input in many of the ISS models (Feng and Li, 2011; Ryan *et al.*, 2012; Feng *et al.,* 2014). However, 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). In practice, the evaluation of risk under uncertainty and

complexity requires the involvement of relevant stakeholders who make use of their own norms and values to set up the boundaries of a problem space. This leads to 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.

To assist and facilitate assessment of risk with multi-value scales according to different stakeholders' point of view, a potential interdisciplinary research area emerges to develop techniques and modelling support for analysis aiming at inquiries into uncertain and complex problems spaces. In this setting, the SST framework (Bednar, 2000) incorporates para-consistent logic, techniques for structuring uncertainty from multiple systemic perspectives and techniques for modelling diversity networks. Sadok *et al.*, (2014) addressed the potential relevance of cognitive maps use in ISS context to support the exploration of individual understanding leading to richer elaboration of problem spaces.

Being aware of the merits of sharing information and knowledge about security threats, the PwC-US (2014) report points up that 82% of companies with high-performing security practices collaborate with others (e.g. third-party service providers and partners) to learn and to stimulate conversations about security risks and tactics. We argue in this paper that the exploration and understanding of security risks should equally involve internal stakeholders to better align security practices to business needs.

## 5. Conclusion

This paper aimed to shed light on key findings of security surveys in relation to risk analysis scope and involved actors. More fundamentally, deficiencies in security practices can be attributed to many reasons but it is relevant to include among them an exclusive technical focus and a top-down approach. Emphasising the centrality of human issues in information security, we highlight in this paper that the contextualization of security risk analysis as well as security policy design and implementation continue to be relevant and necessary research topics to explore. Questions about security failures in context could address the relevance of security policies and measures from professional stakeholders' perspective as in many cases they work around security compliance or bypass security measures to effectively do the work.

Rather than a dominant emphasis on technologies, for instance, it is essential to fund processes that fully bridge the gap between design and implementation of secure and usable systems through open discussion and dialogue between relevant stakeholders leading to better contextual appreciation of risks.

# 6. References

Albrechtsen, E. (2007), "A qualitative study of users' view on information security", *Computers & Security*, Vol. 26, pp 276-289.

Albrechtsen, E. and Hovden, J. (2010), "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study", *Computers & Security*, Vol. 29, pp 432-445.

Bednar, P. (2000), "A Contextual Integration of Individual and Organizational Learning Perspectives as part of IS Analysis", *Informing Science Journal*, Vol. 3, No. 3, pp 145-156.

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. (2007), "Individual emergence in contextual analysis", *Systemica*, Vol. 14, No. 1-6, pp 23-38.

Bednar, P. and Welch, C. (2014), "Contextual Inquiry and Socio-Technical Practice", *Kybernetes*, Vol. 4, No. 3, pp 9-10.

Bednar, P.M. and Katos, V. (2009), "Addressing the human factor in information systems security", In Poulymenakou, A., Pouloudi, N., Pramatari, K. (eds) 4th Mediterranean Conference on Information Systems, Athens, Greece, September 25-27.

Bocij, P., Chaffey, D., Greasley, A., & Hickie, S. (2008), *Business information systems – Technology, Development & management for the e-business*, Pearson Education Limited, ISBN: 978-0-273-71662-4.

Clusif, (2014) Menaces informatiques et pratiques de sécurité en France, www.clusif.asso.fr

Coles, R. S and Moulton R. (2003), "Operationalizing IT risk management", *Computers & Security*, Vol. 22, No. 6, pp 487-493.

Dhillon, G. and Torkzadeh, G. (2006) "Value-focused assessment of information system security in organizations", *Information Systems Journal*, Vol. 16, pp 293-314.

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, pp 57–73.

Filkins B. (2013) "The SANS 2013 Help Desk Security and Privacy Survey", www.sans.org

Franke, U. and Brynielsson, J. (2014), "Cyber situational awareness-A systematic review of the literature", *Computers & Security*, Vol. 46, pp 18-31.

Furnell, S. and Clarke, N. (2012), "Power to the people? The evolving recognition of human aspects of security", *Computers & Security*, Vol. 31, pp 983-988.

Herath, T., and Rao, H.R. (2009), "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness", *Decision Support Systems*, Vol. 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*, Vol. 31, pp 83-95.

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

Katos, V. and Bednar, P. (2008), "A cyber-crime investigation framework", *Computer Standards & Interfaces*, Vol. 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*, Vol. 28, pp 493–508.

Kolkowska, E., and Dhillon, G. (2013), "Organizational power and information security rule compliance", *Computers & Security*, Vol. 33, pp 3-11.

Oz, E., & Jones, A. (2008), *Management information systems*, Cengage Learning EMEA, London, ISBN: 978-1-84480-758-1.

Parsons K., McCormac, A., Butavicius, M., Pattinson, M., and Jerram, C. (2014), "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)", *Computers & Security*, Vol. 42, pp 165-176.

PwC-UK, 2014 UK information security breaches survey, www.pwc.co.uk

PwC-US, 2014 US State of Cybercrime Survey, www.pwc.com

Reece, R.P. and Stahl, B.C. (2015), "The professionalisation of information security: Perspectives of UK practitioners", *Computers & Security*, Vol. 48, pp 182-195.

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.

Sadok, M., Katos, V. and Bednar P. (2014) ) "Developing contextual understanding of information security risks", International Symposium on Human Aspects of Information Security & Assurance (HAISA 2014), Plymouth University, 8th - 10th July 2014.

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

Shedden P., Scheepers R., Smith W., Ahmad A. (2011), "Incorporating a knowledge perspective into security risk assessments", *VINE Journal Information Knowledge Management System*, Vol. 41, No. 2, pp 152-166.

Shropshire J., Warkentin M., and Sharma S. (2015), "Personality, attitudes, and intentions: Predicting initial adoption of information security behavior", *Computers & Security*, Vol. 49, pp 177–191.

Sommerville, I. (2011), *Software engineering*, Pearson Education Inc, ISBN: 978-0-13-705346-9.

Spears, J. L. and Barki, H. (2010) "User participation in information systems security risk management", *MIS Quarterly*, Vol. 34, No. 3, pp 503-522.

The Global State of Information Security Survey (2015) "Managing cyber risks in an interconnected world", www.pwc.com/gsiss2015

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

Webb J., Ahmad A., Sean B. Maynard S.B. and Shanks G. (2014), "A situation awareness model for information security risk management", *Computers & Security*, Vol. 44, pp 1-15.

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*, Vol. 31, pp 360-365.