Teaching Business Systems Analysis to Cyber-Security Managers: a Socio-Technical perspective

Moufida Sadok[1] and Peter Bednar[2]

[1] Institute of Criminal Justice Studies, University of Portsmouth, UK
[2] School of Computing, University of Portsmouth, UK
moufida.sadok@port.ac.uk
peter.bednar@port.ac.uk

Abstract. This paper reports a teaching experience of business systems analysis (BSA) to cyber-security management students. This unit places great emphasis on connecting security function to business requirements from a socio-technical (ST) perspective. Specific topics of lectures and seminars are discussed to outline the necessity of tuning and tailoring BSA content to fit the needs of contemporary security professionals. The paper shows examples of how ST theory provides a relevant theoretical background to bridge the gap between design and implementation of secure and usable business information systems. It also considers challenges facing lecturers as well as ways on how to improve the learning experience of future graduates.

Keywords: Systems Analysis, Information Security, Socio-Technical Theory.

1 Introduction

The necessity to include business processes, people and technology has been widely highlighted in the design and implementation of effective security solutions [7; 2; 10; 8; 17].

This would include discussions about the content and ways of teaching information security as the education of future practitioners influence their view and understanding of information security management as a discipline and as a practice. Educations programs must therefore prepare students to critically reflect on how to align security function with business needs through a holistic understanding of the role and application of security measures in business context.

However, traditional information security courses mainly focus on technical modules and do not pay much attention to the influence of contextual variables affecting the reliability of provided security solutions [6; 5]. These technically oriented security curricula are challenged by dynamic business and technological environments as many security failures in context could question their relevance. A need to balance technical content with business content is required in information security education to complement the technical and formalized paradigm in the development and implementation of information security policies [13; 23]. In practice, the study of Reece

and Stahl [16] has revealed significant tensions between technical views of security policies and those more interested in business- and human-centered security practices. The authors have recommended including particular skills and knowledge in undergraduate socialisation and training.

In this paper, the authors suggest that a potential perspective to address these concerns is offered by a socio-technical (ST) perspective focusing on reciprocal relationships between human actors and the technologies with which they engage in the workplace. It is thus concerned with harnessing human and technical aspects of organizational structures/processes in order to achieve a holistic optimization, with a view to achieving excellence [14]. The objectives of this paper are therefore twofold: firstly, we report a teaching experience of business systems analysis unit to cybersecurity management students; secondly, we discuss the relevance of some lectures topics from a ST perspective.

The remainder of this paper is structured as follows. In the next section, a short review of deficiencies in security practice found in literature is provided. Section 3 discusses the design and delivery of BSA unit through examples of lectures topics and seminars. In the final section, concluding remarks are presented.

2 Background

While security risks and financial costs of cybercrime continue to escalate, security practices and strategies have not adequately kept up with dynamic and challenging attacks [e.g. 22; 9]. In particular, enterprises experience difficulties in assessing and managing their security risks as well as in applying appropriate security controls that match the requirements of their business processes. In Sadok and Bednar [18] a comprehensive review of security surveys published by professional bodies in many different countries has highlighted a number of gaps and shortfalls in security practices. Essentially, their analysis shows a continuous technical focus on data system security rather than on real world organizational context as well as a prevalent top-down approach. In light of these results, the recommendations of security surveys suggest that an exclusive emphasis on a technology-centered view induces flaws in the design and implementation of security solutions and points to the necessity of including people and processes as a core part of secure and usable work systems.

More studies have acknowledged that security measures which are modeled outside of the real world organizational context are prone to antagonize effective organizational practices. 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 create difficulties for work functionality and efficiency [20; 11]. 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 an organized human system. Questions about security failures in context could address the relevance of security policies and controls from professional stakeholders' perspective as in many cases they work around security compliance or bypass security measures to effectively do the work [12; 1]. In addition, a top-down approach can

privilege certain groups of stakeholders particularly managers and IT professionals [21].

In this paper, we argue that the divide between design and practice of security solutions, explaining many deficiencies in information security management, can be addressed by a socio-technical approach. Contextual dependencies inherent in a ST system mean that interactions among all elements within that system contribute to shaping the whole, just as the system is changed by any element changing or leaving it. If we isolate sub-systems for analysis, e.g. task-structure-people-technology (Leavitt, 1965, cited in [19]) we risk failing to recognize the dynamic of interactions among these factors which creates the conditions for (un)successful organizational performance. Overlooking this dynamic and focusing on the optimization of social or technical aspects of a system can increase not only the number of unpredictable, unintended consequences and relationships, but the extent to which those relationships are destructive for the performance of the system [15].

The education of future security management professionals should reflect these dynamic relationships between the social and technical factors within a business context in order to adequately match security to business requirements. In particular, future graduates need to develop a broad understanding of business processes supporting the delivery of value as well as the analysis of the expectations of different groups of stakeholders including managers, business process owners and end-users. From this perspective, ST principles could potentially inform the design and development of the teaching curriculum to acquire these areas of knowledge.

3 Experience report

In this section we explain the intended learning outcomes of BSA and we provide examples of lecture and seminar content in order to illustrate the connection of security solutions and business needs.

3.1 Unit design and delivery

Business systems analysis is gaining an increasing recognition as a core unit in many business and information systems curricula. It supports students at developing analytical and problem-solving techniques for identifying and evaluating organizational and technical consequences of design and implementation of business systems. Therefore, BSA plays a crucial role in bridging the gap between business needs and technical solutions [4].

In the setting of cyber-security management course, the main aim of BSA unit is to develop fundamental understanding of business strategy and organizational context in order to provide a secure operating environment and effective management of security risks. The students are also expected to appreciate and apply different techniques of BSA. Attention must therefore be paid to aligning security to strategic, tactical and operational management goals of the business.

The design and delivery of this unit were tailored to develop a holistic view of the role of security in supporting business processes. The choice of lectures' topics and the selection of discussion papers during the seminars were influenced by the key teaching objectives.

The figure below presents a particular use of the POPIT model to illustrate how to connect security to business context. The POPIT model shows the different aspects that are relevant for BSA. The students have had the opportunity to apply this model in different analyses during seminar time and to discuss its relevance based on real case studies. As a technique, POPIT model can be also deployed to identify opportunities for business improvement or to map the scale of change of a provided solution.

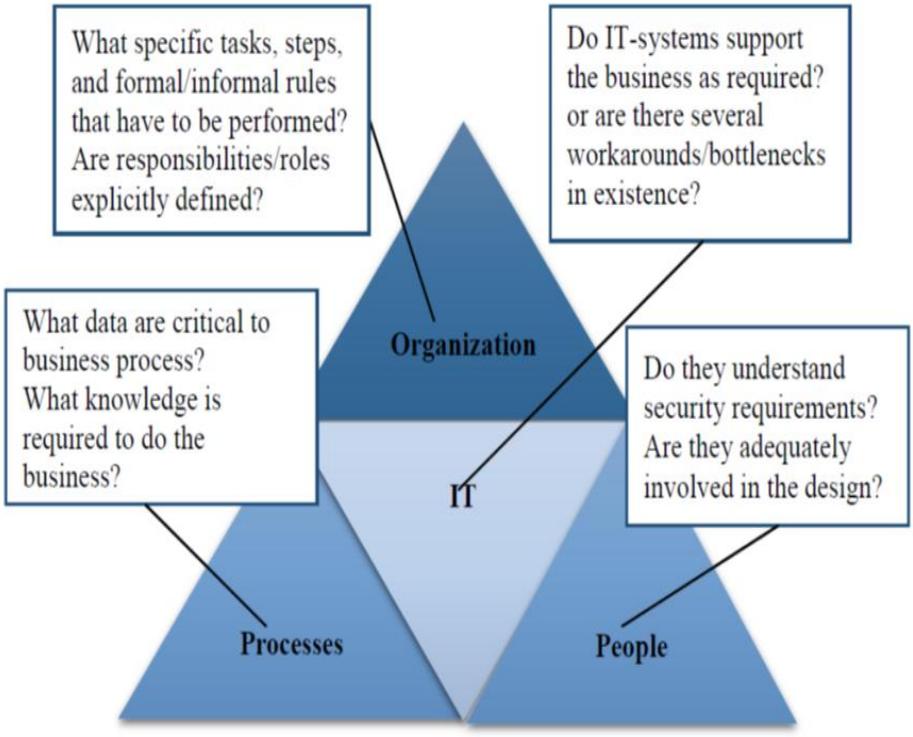

Fig. 1. POPIT model: Matching security to business context

3.2 Examples of lectures and seminars topics

In this section, we describe the relevance of four particular topics with regard to the main teaching objectives of BSA.

First, systems thinking are used as fundamental theoretical background for understanding and framing organizational problems. For example, students have opportunities to reflect on the pros and cons of reductionist or holistic systems approach. This is achieved through an understanding of the boundaries of the system under consideration, key elements to include in a problem space and the dynamic relationships between them. Systems thinking are of particular relevance as an exclusive emphasis on a technology-centered view induces flaws in the design and implementation of security solutions. Therefore, students should be aware of the impact of security solutions from a systemic point of view. The suggested reference to read introduces basic principles of systems thinking and provides many examples of socio-technical systems. Given the abstract nature of systems thinking, it was problematic to introduce its concepts to students. The teaching of this topic was based on lecture notes and seminar discussions where students were asked to describe a system and to indicate whether or not it consists of sub-systems. A "cool" video was also used to provide examples of systems thinking. This video was really appreciated by students who experienced some difficulties in the beginning of the lecture to understand this topic and its relevance with regard to business analysis and/or security management.

Second, stakeholder analysis is in general applied during the definition and elicitation of requirements in relation to the functions that the system is expected to fulfil and the features through which it will perform its tasks. Different views should be explored and articulated about why problems exist, what needs to be done to improve the situation and where the focus of the business system should lie. Security managers should adequately involve professionals with operational knowledge and end users in risk analysis and security policy definition to ensure an effectual integration of security in work practices. Therefore, the main objective of discussing this topic is to explain to future security mangers how to identify key stakeholders, how to assess their influence and how to manage their involvement and expectations. The suggested research paper to read describes the difficulties experienced by clinicians to comply with security requirements which interfere to effectively perform their job. The explanation during lecture and seminar sessions of the importance of stakeholder analysis went relatively without major difficulties and students expressed an interest in learning how to identify and manage key stakeholders that a business cannot afford to disqualify or ignore. The case study described in the research paper provided as reading material has significantly contributed to increase this interest. Another "cool" video was also used to explain difficulties experienced by consultants in articulating and understanding business needs due to communication problems

The third lecture topic is related to change management which recognizes the necessity of a number of tactics to facilitate the implementation and the adoption of new or improved solution. This is particularly important to consider as often security professionals are more focusing in explaining how employees comply with security re-

quirement than on how to explain or justify changes in security controls. The suggested paper to read explains how even when security solutions are well designed and developed the implementation can fail if efforts at change management are insufficient. Teaching change management to future cyber-security managers was challenging as students appeared to be "surprised" of including this topic in their scope of knowledge or skills. Their attitude is explained by an assumption that, when a security solution is technically robust, they take for granted its effective implementation in an organizational system. The lecture and seminar in relation to this topic went relatively well and the case study described in the research paper supporting this lecture was very helpful.

The fourth topic deals with the definition of performance measures that indicate to which extent a business or technical solution meets business needs. A particular technique used for this purpose is the balanced scorecard that assesses performance in business models including learning and growth, internal business process, customer, and financial dimensions. In the context of this unit, this technique is used to identify relevant security metrics that should support business needs and as a vehicle of communication to translate these metrics into a meaningful context from management point of view. The table below provides more details about lectures topics and supporting reading/video material.

Table 1. Examples of BSA topics and associated reading/video material

BSA topic	Examples of topic content	Reading/video material
Understanding business context	Systems thinking	"Systems thinking" in Socio-technical toolbox for business systems analysis [3] Link to the video: Systems thinking: a cautionary tale (cats in Boneo) https://www.youtube.com/watch?v=17BP9n6g1F0
Requirement analysis	Stakeholder analysis	Workarounds to Computer Access in Healthcare Organizations: You Want My Password or a Dead Patient?" [12] Link to the video: The expert: Short comedy Sketch https://www.youtube.com/watch?v=BKorP55Aqvg&t=97s
Improvement of business processes	Change management	"IS Security Menace: When Security Creates Insecurity" [1]
Evaluation of business solutions	Balanced scorecard	Link to the video: Security Metrics: Can They Be Effectively Measured Across the Enterprise? https://www.youtube.com/watch?v=0CQLJyqELDE&t=1432s

4 Concluding comments

The alignment between security and business processes needs has long been considered as a key issue in security management. The tailoring of BSA content to fit the needs of future security professionals has been informed by a ST perspective which potentially articulates security solutions for the business as a whole. One of the main learning outcomes of this unit is to develop a holistic view encompassing social and technical aspects of security management. This teaching experience shows how BSA could be designed by creating links between research and teaching activities and supporting the development of broader set of soft skills such as problem solving and critical thinking highly valued by security professionals. It also sheds light on a number of challenges facing academics teaching business units in a curriculum with technical vocation or expected by students as technical. According to a first evaluation of this unit, the students are equally divided between hard and soft thinkers. The former group of students still believe on the "supremacy" of technical solutions, the later rather recognizes the need for contextual analysis of the business in order to ensure effective design and implementation of security solutions. To improve the learning experience, this unit would benefit from inviting security professionals to ensure that unit content aligns with required practitioner skills and to provide students with real organizational experiences.

References

1. Balozian, P. and Leidner, D.: IS Security Menace: When Security Creates Insecurity. Thirty Seventh International Conference on Information Systems, Dublin (2016).
2. Bednar, P. and Katos, V.: Addressing The Human Factor In Information Systems Security. MCIS 2009 Proceedings, Athens, Greece, 25-27 September, Paper 72 (2009).
3. Bednar, P.M. and Sadok, M.: A Socio-technical toolbox for business systems analysis and design", Proceedings of the 1st International Workshop on Socio-Technical Perspective in IS Development (STPIS'15) co-located with the 27th International Conference on Advanced Information Systems Engineering (CAiSE 2015), Stockholm, Sweden, June 9 (2015).
4. Cadle, J. et al.,: Business Analysis. 3rd ed. London: BCS, The Chartered Institute for IT (2014).
5. Chen, H., Maynard, S.B. and Ahmad, A.: A comparison of information security curricula in China and the USA", 11th Australian Information Security Management Conference, Edith Cowan University, Churchlands, 2-4 December (2013).
6. Dark, M.J., Ekstrom, J. and Lunt, B.: Integrating information assurance and security into IT education: a look at the model curriculum and emerging practice. Journal of Information Technology Education: Research, 5(1), 389-403 (2006).
7. Dhillon G, Backhouse J. Information system security management in the new millennium. Communications of ACM, 43(7), 125-8 (2000).
8. Furnell S, Clarke N.: Power to the people? The evolving recognition of human aspects of security. Computer & Security, 31, 983-8 (2012).
9. Global Economic Crime Survey: Adjusting the Lens on Economic Crime (2016). available at: www.pwc.com/crimesurvey

10. Kayworth T, Whitten D.: Effective information security requires a balance of social and technology factors. MIS Q Exec, 9(3), 163-75 (2010).
11. Kolkowska, E., and Dhillon, G.: Organizational power and information security rule compliance. Computers & Security, 33, 3-11(2013).
12. Koppela, R., Smith, S., Blythe, J. and Kothari, V.: Workarounds to Computer Access in Healthcare Organizations: You Want My Password or a Dead Patient?. Studies in Health Technology and Informatics, 280, 251-220 (2015).
13. Long, J., & White, G.: On the global knowledge components in an information security curriculum-a multidisciplinary perspective. Education and Information Technologies, 15, 317-321(2010).
14. Mumford, E.: Redesigning Human Systems. Hershey: IRM Press (2003).
15. Mumford, E. "The story of socio-technical design: reflections in its successes, failures and potential. Information Systems Journal, 16, 317–342 (2006).
16. Reece, R.P. and Stahl, B.C.: The professionalisation of information security: Perspectives of UK practitioners. Computers & Security, 48, 182-195 (2015).
17. Sadok M. and Bednar P.: Information Security Management in SMEs: Beyond the IT Challenges". Tenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2016: 209-219), July 19-21, Frankfurt, Germany. ISBN 978-1-84102-413-4(2016).
18. Sadok, M. and Bednar, P.: Understanding Security Practices Deficiencies: A Contextual Analysis", in Furnell, S. and Clarke, N. (Ed.), Human Aspects of Information Security & Assurance, HAISA 2015, Lesvos, Greece, July 1-3, 151-160 (2015).
19. Seidel, S., J. Recker, and J. van Brocke: Sensemaking and sustainable practicing: functional affordances of information systems in green transformations". MIS Quarterly, 37(4), 1275-1299 (2013).
20. Shedden, P., Scheepers, R., Smith, W., Ahmad, A.: Incorporating a knowledge perspective into security risk assessments", VINE Journal Information Knowledge Management System, 41(2), 152-166 (2011).
21. Stahl, B. C., Doherty, N. F. and Shaw, M.: Information security policies in the UK healthcare sector: a critical evaluation", Information Systems Journal, 22, 77-94, (2012).
22. The Global State of Information Security Survey: Turnaround and transformation in cybersecurity (2016). available at: www.pwc.com/gsiss.
23. Woodward, B., Imboden, T., & Martin, N. L.: An undergraduate information security program: More than a curriculum. Journal of Information Systems Education, 24(1), 63-70 (2013).

