Proceedings of the Enterprise Engineering Working Conference (EEWC) Forum 2017, Antwerp, Belgium, 09-May-2017 to 11-May-2017

Defining a research method for engineering a Business Information Security artefact

Yuri Bobbert
NOVI University of Applied Sciences, Utrecht, Netherlands
University of Antwerp, Antwerp, Belgium
Radboud University, Nijmegen, Netherlands
y.bobbert@novi.nl

Abstract: This paper proposes research methods for designing and engineering a Business Information Security (BIS) artefact. Defining research methods to establish artefact functions (e.g. dash-boarding, risk register) that reflect the parameters of control for Board of Directors, is the main motivation for this research paper. The ultimate goal is to engineer this BIS artefact and thereby solve the problem of a low level of BIS maturity. We propose a research method that can be used to establish an experimental dashboard with initial parameters of control, based on a Design Science Research (DSR) approach. Group Support System (GSS) research can assist organisations applying the artefact into the organisations with the accompanying collaboration and decision making (fit to purpose) processes.

Keywords: Business Information Security, Design Science Research, Group Support Systems

Introduction

Information Security is a strategic issue for business leaders and several institutions and communities have launched numerous initiatives to encourage business leaders to ensure good stewardship in this area [1]. The associated compliance obligations and the increase in security breaches have made many business leaders aware of its impact on the business continuity [2], civil and legal liabilities [3] reputation [4], employability and financial position [5], [6]. Within this multidisciplinary context of Information Security we therefore use the term “Business Information Security” [7]. Most of the contributions by practitioner’s bodies [8], [9] [10] are prescriptive in nature [11]. Little academic research has been done on determining the BIS parameters which boards can use to improve their BIS maturity. This paper focusses on examining the “parameters of control”, that can function as requirements, via multiple qualitative research methods proposed by Johannesson and Perjons’ Design Science Research (DSR) Framework [12]. DSR aims to solve real problems by creating knowledge and understanding of a design problem and the solutions are acquired by establishing and applying artefacts. In this research we therefore refer to an artefact that contributes in solving the Business Information Security problems at hand. We formulated the following research question: *Which research methods contribute to defining the requirements for the parameters of a Business Information Security artefact?*

Examining research methods to translate business problems to artefact requirements

Design science strategy focuses on solving real-life problems. According to Hevner et al. [13] it involves generating knowledge and building artefacts to solve defined business problems. Business requirements are aligned with technical artefact requirements via an iterative process

referred to as the "design cycle" [14]. This cycle involves designing, testing and evaluating the artefact [15]. It includes an academic rigour cycle and a practical relevance cycle [16]. A continuous process of iterations, which are initially framed in the experimental phase, establishes the artefact [12]. In the table below we summarize the most important qualitative interpretivist methods to gain, capture and transfer knowledge items to be used in the artefact design process, according to the DSR approach of Johannesson and Perjons [12].

Table 1 Research methods and their contribution to Business Information Security

Type of research within DSR	**Contribution to designing and engineering a Business Information Security artefact**
1.Literature research	Explicating and defining the problem in a systematic, structured way. Objectivity removes the element of Fear Uncertainty and Doubt (FUD). Unbiased, structured point of departure for the design cycle. Requires a certain level of expertise in the topic.
2.Delphi research	Anonymous inventory and selection of views and standpoints (preferably based upon literature data). Rigorous examination process for scrutinizing the problem via, for example, expert opinions. Collecting global views on criteria requirements with the use of technology. Knowledge sharing. Enables double loop learning via multiple iterations. Automated. No geographical limitations. Limited in group interaction and discussion.
3.Case Study Research (CSR)	Deeper qualitative insight into BIS parameters and requirements within a certain industry/country. Used for confirmatory and exploratory studies related to validating requirements. Detailed insight into the effectiveness of requirements (i.e. critical success factors). Validating and evidencing the artefact requirements. Supports retroperspectives. The personal approach encourages the target group (Boards of Directors) to engage in BIS. CSR is a time intensive and consuming.
4.Group Support System research (GSS)	Enables to create, share and capture knowledge as well as design items. Stimulates design thinking and stakeholder collaboration due to the "group element". Ability to collect, assess and select product requirements in a very short timeframe. Supports the regulative process [13] of testing and validating requirements. Processing large data sets. Double Loop learning. Bridging knowing-doing gaps. Stimulating group dialogues (i.e. among Boards of Directors and Management teams). Makes it possible to establish group consensus. Supports the decision-making process. Threat of the "law of the decibel". Requires professional group moderation skills [14].

The proposed definition of a "research method to design and engineer a BIS artefact" starts with the initial phase of rigours literature research (1) to explicate the problem and followed by Delphi Research (2) to predefine views and standpoints and further explicate the problem via multiple views and iterations. After that Case Study Research (3) can provide in depth knowledge data on certain influences to BIS such as context, regulations, technology or culture. The gathered data during Delphi and CSR is then used in GSS to fuel the design and decision making process. GSS can be applied to determine the requirements among stakeholders and to prepare or guide the stakeholder –user- group to discuss the implementation (fit to purpose). This DSR methodology based on a structured process [15], [16], [17], [18], [13], [19], [12] in order to improve the Maturity of Business Information

Security is coined and published as the “MBIS method” in several publications [20], [21], [22], [23], [24].

Conclusion

In this paper we make two propositions: a) refers to the product and data view and b) focuses on implementing the artefact and facilitating meetings. The first proposition (a) was involved in the previous mentioned MBIS research publications according to the MBIS method [20], [23], [22]. The second proposition (b) was researched and tested in collaboration with Antwerp Management School among twenty five Chief Information Officers (CIO) and Chief Information Security Officers (CISO), who validated the implementation of the predefined artefact requirements [25]. The use of GSS in facilitating implementation and decision-making (fit to purpose) related to BIS has also been researched and published [21] [24]. The artefact is used by academics and practitioners and assists Board of Directors (BoD) into gaining more control. For example via a dashboard that provides scores of the current versus the desired state of BIS maturity. Conclusive we can state that by making use of the multiple methods that are proposed in the paper contribute in the design and engineering of the BIS artefact as well as the implementation into organisations.

References

[1] WEF, "Partnering for Cyber Resilience; Risk and Responsibility in a Hyperconnected World - Principles and Guidelines," World Economic Forum,, Davos, Swiss, 2015.

[2] B. Cashell, W. Jackson, M. Jickling and B. Webel, "The Economic Impact of Cyber-Attacks," Congressional Research Service, The Library of Congress, United States, 2004.

[3] Fox-IT, “DigiNotar Certificate Authority breach, “Operation Black Tulip”,” FOX IT in assignment of the Ministry of the Interior and Kingdom Relations, Den Haag, 2011.

[4] G. Walsh, V. Mitchell, P. Jackson and S. Beatty, “Examining the Antecedents and Consequences of Corporate Reputation: A Customers perspective,” Britisch Journal of management; Blackwell Publishing LtD, UK, 2009.

[5] M. Ishiguro, H. Tanaka, K. Matsuura and I. Murase, "The Effect of Information Security Incidents on Corporate Values in the Japanese Stock Market," Institute of Industrial Science, The University of Tokyo, Tokyo, Japan, 2011.

[6] H. Cavusoglu, B. Mishra and S. Raghunathan, “The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers,,” International Journal of E-Commerce, Dallas, Texas United States, 2-2002.

[7] V. Solms, "From Information Security to Business Security," Computer & Security, Elsevier, South Africa, 2005.

[8] ISACA, COBIT5 for Information Security, United States: ISACA , 2012.

[9] ISF, Corporate Governance Requirements for Information Risk Management, UK: Information Security Forum.

[10] ITGI, Information risks; Whose Business are They, United States : IT Governance Institute, 2005.

[11] E. Koning and H. Bikker, “Using Standards to Create Effect in the Boardroom,” *ISACA Journal*, no. 2, 2013.

[12] P. Johannesson and E. Perjons, An introduction to Design Science, Stockholm University:

Springer, 2014.

[13] R. Wieringa, Design Science Methodology: For Information System and Software Engineering, Berlin: Springer, 2014.

[14] G. M. J. Kolfschoten and H. Proper, “De fata morgana van Group Support Systemen,” *Informatie,* vol. 4, no. 5, pp. 10-14, 2016.

[15] R. Winter, “Design Science Research in Europe,” *European Journal of Information Systems,* vol. 17, pp. 470-474, 2008.

[16] J. Dietz and J. Hoogervorst., “The discipline of Enterprise Engineering,” *International Journal of Organizational Design and Engineering,* vol. 3, no. 1, pp. 86-114, 2013.

[17] A. Albani, D. Raber and R. Winter, “A Conceptual Framework for Analysing Enterprise Engineering Methodologies,” *Enterprise Modelling and Information Systems Architectures,* vol. 11, no. 1, 2016.

[18] V. J. Aken and A. Nagel, “Organising and managing the fuzzy front end of new product development,” in *ECIS working paper series; Vol. 200412*, Eindhoven: Technische Universiteit Eindhoven, 2004.

[19] S. Hevner, J. March, Park and S. Ram, "Design Science Research in Information Systems," *Management Information Systems Quarterly,* vol. 28, no. 1, pp. 75-105, 2004.

[20] Y. Bobbert and J. Mulder, "A Research Journey into Maturing the Business Information Security of Mid Market Organizations," International Journal on IT/Business Alignment and Governance, 1(4), 18-39, October-December 2010, United States, 2010.

[21] Y. Bobbert and J. Mulder, “Boardroom dynamics: Group Support for the Board’s Involvement in a Smart Security,” *ISACA Journal* , no. 5, 2016.

[22] Y. Bobbert and J. Mulder, “Governance Practices and Critical Succes Factors suitable for Business Information Security,” in *International Conference on Computational Intelligence and Communication Networks*, India, 2015.

[23] Y. Bobbert and J. Mulder, "Group Support Systems Research in the Field of Business Information Security; a Practitioners View," in *46th Hawaii International Conference on System Science*, Hawaii US, 2013.

[24] Y. Bobbert and J. Mulder, “Vergaderen om te besluiten: Het gebruik van Group Support Systemen in informatiebeveiliging,” *Platform voor Informatiebeveiliging,* no. 3, pp. 4-7, 2016.

[25] G. Mari, “Cyber Security; Facts or Fiction,” Antwerp Management School, 14 11 2016. [Online]. Available: http://blog.antwerpmanagementschool.be/.

[26] F. Peters, Reputatie onder druk; Het managen van reputaties in een veranderende samenleving, Den Haag: SDU Uitgevers, 2012.

[27] J. Allen, “Governing for Enterprise Security (GES) Implementation Guide,” Carnegie Mellon University, Software Engineering Institute, CERT , US, 2007.

[28] B. Lebek, J. Uffen, M. Neumann, B. Hohler and M. Breitner, “Information security awareness and behavior: a theory-based literature review,” *Management Research Review,* vol. 12, no. 37, pp. 1049 - 1092, 2014.

[29] M. Workman, W. Bommer and D. Straub, "Security lapses and the omission of information security measures: A threat control model and empirical test," *Computers in Human Behavior,* vol. 24, no. 6, p. 2799–2816, 2008.

[30] V. J. Aken and A. Nagel, “Organising and managing the fuzzy front end of new product development,” in *ECIS working paper series; Vol. 200412*, Eindhoven