International Journal of IT/Business Alignment and Governance
Volume 8 • Issue 2 • July-December 2017

On Exploring Research Methods for Business Information Security Alignment and Artefact Engineering

Yuri Bobbert, University of Antwerp, Antwerp, Belgium & Radboud University, Nijmegen, Netherlands & NOVI University of Applied Sciences, Utrecht, Netherlands

ABSTRACT

This paper examines research methods for designing and engineering a Business Information Security (BIS) artefact. Preventing and responding to cybercrime is becoming an integral part of management practices which are supervised by the Board of Directors (BoD), and it can no longer be perceived as just traditional IT. In order to improve the maturity of business information security a transformation is needed and this requires adequate reporting and dashboarding. Dashboard functions such as the current versus the desired state of the Maturity of Business Information Security (MBIS) reflect certain parameters that boards can influence. Determining the key dashboard functions that reflect these parameters of control was the main motivation for this research paper and the ultimate goal was to engineer a BIS artefact. We propose a research and design method that could be used to establish an experimental dashboard with initial parameters of control based on a Group Support System (GSS) approach. Finally, GSS is evaluated as a method for a) examining which parameters are effective for BIS, from multiple perspectives and b) helping to implement the artefact (make it fit the purpose) as well as the associated business alignment and decision-making.

KEYWORDS

Business Information Security, Design Science Research, Enterprise Transformations, Group Support System, Information Systems Design and Development

INTRODUCTION

Information Security is now 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 (WEF, 2015). The associated compliance obligations and the increase in security breaches have made many business leaders aware of its impact on the business continuity (Cashwell, Jackson, Jickling, & Webel, 2004), civil and legal liabilities (Fox-IT, 2011) reputation (Walsh et al., 2009; Peters, 2012), employability and financial position (Ishiguro et al., 2011; Cavusoglu et al., 2002). This is why Von Solms (2009) has argued that Information Security Management (ISM) is part of Information Security Governance (ISG). The IT Governance Institute (ITGI) states that ownership of data and its information risks are the responsibility of businesses and their owners (ITGI, 2005) as well as the IT department (Solms, 2005). The IT department might own the physical hardware and software assets, but not the data. To define security requirements in critical value chains and business processes, such as segregation of duties or use cases for logging, business involvement is required (S. Von Solms & R. Von Solms, 2009). Within this multidisciplinary context of Information

DOI: 10.4018/IJITBAG.2017070102

Security we therefore use the term "Business Information Security" (V. Solms, 2005). Managing Business Information is a prerequisite for improving Business Information Security maturity (Allen, 2007). The International Federation of Accountants (IFAC) (IFAC, 2004) and ISACA (ISACA, 2012) describe information security as an integrated enterprise activity requiring proper governance of the work done in this area by the board and executive management.

Basie and Rossouw von Solms differentiate three levels: the strategic level (Board of Directors and Executive Management), the tactical level (Senior and middle management) and the operational level (lower management and administration). All directive setting and controlling activities (including monitoring and evaluating) are seen as part of the strategic level of governance (R. Von Solms & B. Von Solms, 2006). An example is the adoption of Information Security Control Frameworks such as the Information Security Forum (ISF) Standard of Good Practice. All activities designed to put these directives into practice take place at the tactical management level. The tactical level involves formulating policies and guidelines, for example establishing minimum standards that the organisation needs to adhere to, such as incident management and supply chain management. The level below the tactical level is where these policies and guidelines are translated into procedures and working methods. For example, this is the level where monitoring software is configured which triggers incident response processes or imposes stricter guidelines for suppliers. This paper focuses on defining artefact requirements for the strategic level which are substantiated by tactical and operational data.

Most of the contributions by practitioner's bodies such as the ISACA (ISACA, 2012), the National Institute of Standards and Technology (NIST), the Information Security Forum (ISF) and the ITGI (ITGI, 2005) are prescriptive in nature (Koning & Bikker, 2013). 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 (Johannesson & Perjons, 2014). 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 at hand. This is why we formulated the following research question: Which research methods contribute to defining the requirements for the parameters of a Business Information Security artefact?

Structure of the Paper

This paper first positions the main concepts of business information security and the problems at hand. It addresses the relevance of doing interpretivist qualitative research by making use of multiple research methods. These methods are being elaborated, in the fourth section of this paper, completed with their contribution towards BIS research and the way forward in artefact requirement setting. It concludes with the most relevant qualitative research methods, as part of DSR research, to be adopted in the continuation of this artefact research and development project. It positions two propositions, the first is on how to capture and structure the research data into the artefact (data and product view) and the second one is applying this data towards organisations in order to improve the BIS state (focuses on implementing the artefact and facilitating meetings), also referred to as Improving the Maturity of Business Information Security (MBIS). It finishes off with some examples of the methods being used in scientific and empirical studies and publications.

FROM BUSINESS PROBLEMS TO ARTEFACT REQUIREMENTS

Design science strategy focuses on solving real-life problems. It involves generating knowledge and building artefacts to solve defined business problems. Design science strives according to Perjon and Johannesson "…to create models, methods and implementations that are innovative and valuable…" (2014). Artefacts are built on functionalities that contribute to solving these problems. Business requirements are aligned with technical artefact requirements via an iterative process referred to as the "design cycle". This cycle involves designing, testing and evaluating the artefact. It includes an academic rigour cycle and a practical relevance cycle. A continuous process of iterations, which are initially framed in the experimental phase, establishes the artefact. Examples include establishing Minimum Viable Products (Ries, 2009) and, later on, engineering an artefact that can serve multiple stakeholders needs.

Wieringa (1996) defines business needs as the starting point for setting requirements. The needs, which can reflect business problems, are translated into objectives, which are defined in terms of products and specifications about the desired behaviour of products. Each product specification is a statement of objectives for its subsystems. In client-oriented development, "…the needs of the client may even change because of the determination of objectives. This is called requirements uncertainty. The characteristic feature of product evolution is that an evaluation of experience of the product after it is developed, leads to a (re)development of the product. The logical structure of product evolution is the same as the logical structure of feedback control." (Wieringa, 1996). In this paper, we describe the initial process of defining functional and non-functional technical requirements during the first iteration of the artefact. In this paper, we describe the initial process of defining functional and non-functional technical requirements during the first iteration of the artefact. We describe this as an "experiment", so it is our intention to focus on the business level (ontological, transactions and facts). We thereby accept uncertainty and "fuzziness" during the development process (Aken & Nagel, 2004). In later iterations of artefact development additional requirements can be built in.

EXAMINING RESEARCH METHODS FOR BUSINESS INFORMATION SECURITY

The BIS problem is complex, ambiguous and difficult to examine using a predefined method. We therefore examine the most relevant methods which we could find in the current literature. Researchers have found that both quantitative and qualitative research differ with respect to epistemological foundations (Saunders & Lewis, 2007). Within quantitative research the principal approach is deductive in nature i.e. testing a theory with the help of quantitative data collection methods. Within qualitative research the principal orientation is inductive in nature. The main aim is to generate theories. Within quantitative research the ontological orientation is objective. It considers social reality to be an external objective reality. This is often referred to as objectivism (Saunders & Lewis, 2007). Objectivism is an ontological position that claims that social entities (e.g. organisations) exist in a reality that is external to – and independent of – social actors. Within qualitative research the ontological orientation is that of constructing a situation based on details, and trying to understand the reality behind it. This is often associated with the term constructionism or social constructionism (Saunders & Lewis, 2007). Interpretivism is the epistemology that sees the role of the researcher as part of a "social subject." The researcher observes, analyses and interprets phenomena which he or she is part of. Positivists believe in applying methods from the natural sciences to study social reality. The epistemological orientation behind quantitative research is a particular form of positivism, applying quantitative methods from the natural sciences models to research a particular subject. It would be wrong to suggest that several research strategies cannot be combined. On the contrary, most of the research done in Information System Science or in Information Security involves a combination of qualitative and quantitative methods. Qualitative characteristics such as explorability and complexity

can be combined with 'strong' quantitative characteristics, such as generalizability or deductibility (Recker, 2013).

Lebek et al. (2014) found that 55 percent of most academic research on Information Security (IS) is based on empirical research using quantitative methods. Within this 55 percent, 50 percent are based on quantitative methods and only 5 percent on qualitative methods. Lebek et al. encourage the application of qualitative and interpretivist studies to explore deeper the factors that influence BIS, such as behaviour, attitudes and awareness. Also, Workman et al. emphasize the need for additional qualitative, interpretive studies in BIS (Workman, Bommer, & Straub, 2008).

Three major studies over the last 15 years – those by Abraham (2011), Lebek et al. (2014) and Siponen (2000) – examined the literature on intangible factors related to success in BIS, such as user awareness, management commitment, peer influences and behaviour. According to Workman, the limited amount of research in this area limits research on IS in general. Zooming deeper into the Lebek et al. study, she states that only five of the 144 studies include >500 respondents. The authors argue that "An empirical sample is relevant as long as it is representative and generalizable. Samples consisting of students and/or IS professionals do not reflect the population of interest. With reference to internal, external and construct validities, surveying students and IS professionals is seen more critically than having a smaller sample size, as long as it represents reality." Four publications: Siponen et al. (2010), Al-Omari et al. (2012), Pahnila et al. (2007), Hovav and D'Arcy (2012) used >500 respondents who were employees, i.e. valid representatives. The remaining studies were based on using professionals or students as respondents. Clearly, this underscores the importance of carrying out qualitative research on relevant stakeholder groups.

RESEARCH METHODS

In this research paper, we explore research methods that are suitable for qualitative research on Business Information Security we review the most important qualitative interpretivist methods to gain, capture and transfer knowledge items to be used in the design process.

Literature Research

When one encounters a business problem, it is not always clear what to examine in order to arrive at answers that can explain and potentially solve the problem. Business problems are usually not well defined and they don't have clear boundaries. Within Information Security research papers, we observe a large degree of consensus among academics, but there is considerable disagreement among practitioners (Flores et al., 2014; Siponen & Willison, 2009; Hu et al., 2012) on how to frame this topic and the numerous problems related to it. Disagreement among practitioners is also due to the complexity of the solutions or advice given (Flores, Antonsen, & Ekstedt, 2014). This suggests a need for additional academic research to provide clear definitions and it also highlights the importance of empirical research (Workman et al., 2008) Explicating a problem with academic rigour automatically involves thoroughly decomposing the theoretical concepts that contribute to the problem. This is done by systematically deriving concepts and related topics from the literature (Hart, 1998).

Literature research encourages both academic and practice-oriented researchers to think critically about their subject and scrutinise their concepts, constructs and viewpoints in order to clearly explain the research problem and formulate research questions. Systematic literature reviews are important for Business Information Security. The key contribution of embracing systematic literature review principles in BIS research is the move away from "Fear, Uncertainty and Doubt" towards rigour. It also helps to remove researcher bias. Bias is a pitfall for interpretive researchers, so it should clearly be taken into account in their research. Thus, BIS research uses literature research as the basis for a structured, objective, unbiased point of departure.

The Delphi Research Method

Delphi research is mainly used to gain a deeper qualitative view of a certain phenomenon – to examine propositions, theories and viewpoints using an iterative process (Linstone, 2002). Delphi can be used to elicit views from experts but also the standpoints of user groups, expert groups, stakeholder groups and consumer panels. This form of qualitative research enables researchers to propose practices or theories and, through a process of multiple iterations, get a group of respondents to form a qualitative view (Linstone, 2002). The respondent group can rank, prioritise or scrutinise this view. In the case of Information Security, it enables researchers to include organisation-specific elements that might influence either the process or the content. For example, a researcher may have derived certain best practices from the literature but want to validate them with a certain group of respondents. Schmidt et al. (2001) developed a ranked list of common risk factors for software projects as a foundation for building theory about IS project risk management. The participants were three panels of experienced software project managers based in Hong Kong, Finland and the United States. Thus, Delphi is not geographically limited.

In terms of parameters for MBIS, reviewing anonymous views held by experts, the research by Maes (2014), De Haes and Grembergen (2008) seems promising, in particular for generating standpoints, practices and criteria among experts and thus solving the epistemological problem of knowing too little or too much. When it comes to research about Information Security strategy formulation, the decision-making process for those at the strategic level is evident (Rakhorst, 2013). In other words, we can share knowledge about strategy, but as long as directors or executive managers do not take this knowledge into account, it is useless. So, to effectively transfer knowledge to other groups, for example in order to establish a learning organisation (Flores et al., 2014), we consider qualitative methods in order to transfer standpoints or propositions to other groups (such as management teams, boards of directors, project teams, etc.).

Group Support System (GSS) Research

A Group Support System facilitates the effective collection, organisation, evaluation, cross-impact analysis and reporting of data (Vreede, Boonstra, & Niederman 2002), with the assistance of a group moderator. A GSS is often used either to create divergence or convergence in standpoints, for example those relating to the decision-making process (Bobbert & Mulder, 2016). GSS requires establishing a predefined agenda for a meeting and prompts the facilitator to analyse in advance the topic, the size (Dennis, Valacich, & Nunamaker, 1990) and composition of the group, as well as differences in participants' issues and interests. This makes it possible to align the meeting to the desired outcomes. The role of the facilitator is to make sure everybody has a voice in the meeting and to stimulate a free-flowing discussion. The facilitator must help members share their experiences, elicit the views of all participants, keep them on track and record responses (Newby, Soutbar, & Watson, 2003).

According to Moorsel et al., facilities such as GSS provide the solution to the epistemological problems of capturing and sharing knowledge and thus feed decision-making. They also help monitor and report on carrying decisions (Moorsel, Stepanova, & Parkin, 2009). The knowing-doing gap (Pfeffer & Sutton, 2001) often prevents organisations being successful in a certain practice. GSS can bridge this gap in two ways, first by making the problem explicit, based on theoretical constructs and concepts. And second, by establishing awareness and a mutual level of knowledge among those involved with the problem (object and subject). This stimulates group dialogue and facilitates socialisation (Nonaka, 1994) thinking (Lebek, Uffen, Neumann, Hohler, & Breitner, 2014), discussions (Rutowski, Van de Walle, & Eede, 2006) and using the decision-making process for strategic planning (Pai, 2006), i.e. maturing. This is why we propose GSS as a qualitative research method for examining knowledge management and the decision-making process within BIS.

Case Study Research (CSR)

Case Study Research is one of the most popular ways of doing qualitative research (Silvermann, 2005). It is also widely used within Information System research by business management to gain a qualitative view of certain phenomena. Robert Yin defines CSR as an empirical inquiry that can be used to investigate contemporary phenomena within a real-life context (Yin, 1994). It's especially useful when boundaries between the phenomena and the context are unclear. Case studies provide deeper qualitative insights into phenomena, making use of multiple data sources and multiple data collection methods, such as documentation, observation, interviews and secondary data acquired from other sources. CSR is used for confirmation and exploration (testing and building theories) (Recker, 2013; Eisenhardt, 1989). Another use of CSR is to explain phenomena. Typically, interpretive CSR is used to explore possible explanations.

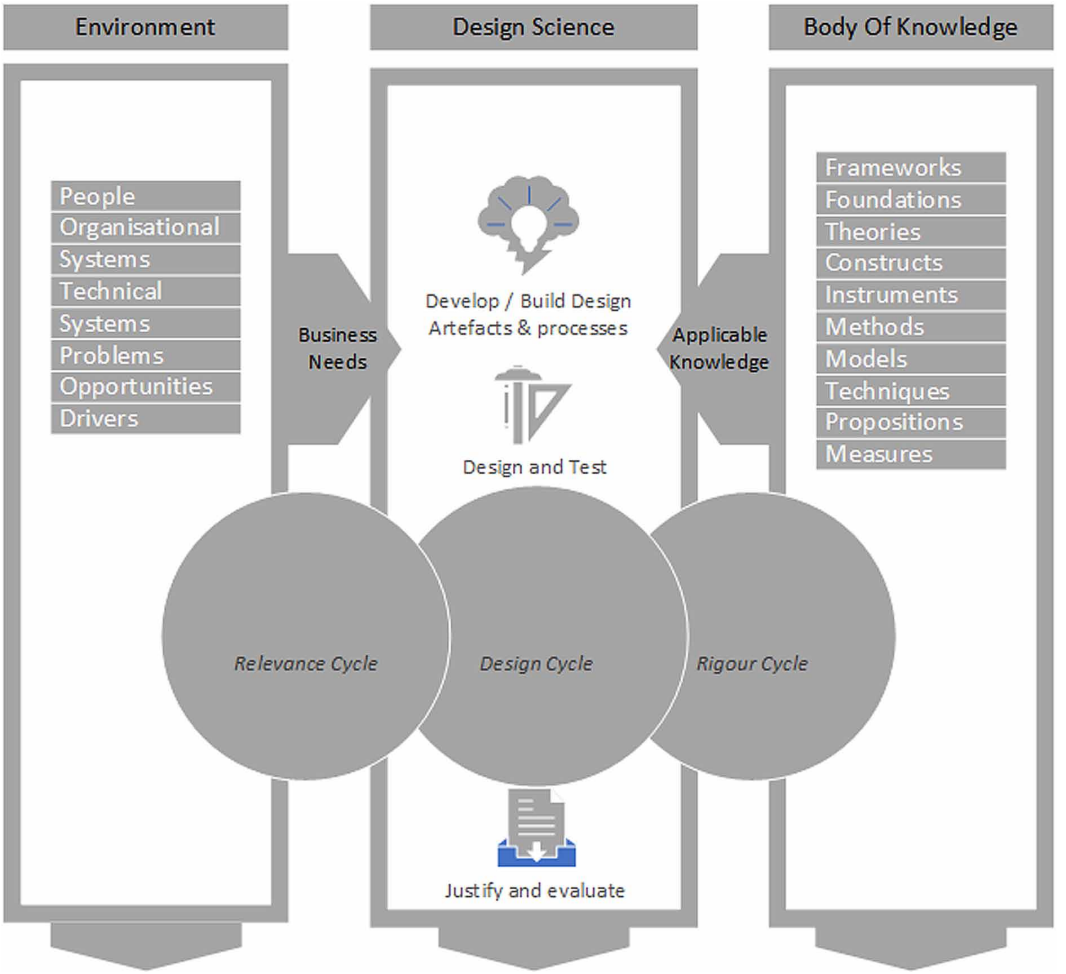
In Business Information Security research, there is a need to explore general topics such as interventions that improve the maturity of BIS. This can be done using qualitative methods such as Delphi, Surveys or Group Support. Although the strength of these methods lies in their ability to reach out to a larger population of respondents, CSR makes it possible to dive deeper based on previously collected data. It provides an in-depth understanding of the phenomena. With multiple cases, it "… strengthens the results by replicating the pattern-matching ability and hereby increases confidence in the robustness of the results…" (Recker, 2013). In Business Information Security research, the effects of intangible factors are relevant for successful engagement in the MBIS process and implementing certain controls. These intangible factors (e.g. leadership and culture) can be examined using CSR. Extreme case studies provide detailing on specific ontological and epistemological issues observed during, for example, face-to-face interviews. 'Extreme' case studies can also be used to validate artefacts or instruments (e.g. security surveys or checklists). In the case of BIS a body of knowledge can be built where there is no list of governance practices that can be used by practitioners. CSR can be used to validate such a list, together with directors or managers. Within BIS research it becomes important to collect evidence, especially due to stricter regulations and auditing guidelines. CSR that encompasses systematic data collection (observations and interviews) stored in an artefact (e.g. data collection tooling) that can be validated by an auditor increases plausibility and credibility. Credibility because it provides proof of outcomes and plausibility because – due to the use of tooling – the researcher is forced to collect and store relevant knowledge items. This triangulation of methods where the data that is gathered – by observing, interviewing and documenting – is captured in a tool that includes corroboration (Plutchik, 1983).

In conclusion, we can state that CSR is limited when it is used to explore and generate generalizable data. To explore general propositions, we propose the use of questionnaires. And to capture and transfer knowledge we propose GSS or surveys. These can play a role in the quest for Business Information Security governance practices that can form a frame of reference for boards. For practitioners, we propose the use of group discussion and group prioritisation. This data set can later on be used in a deeper qualitative analysis of the findings from GSS or Delphi research. CSR can also be used to study certain intangible factors such as culture, leadership and perceptions. Within BIS research these factors play a major role in determining whether a board of directors adopts BIS and they therefore influence the success of improving MBIS. CSR can also be used to examine the impact of certain parameters on MBIS.

Design Science Research (DSR) Strategy

Triangulation of methods is increasingly used within Design Science Research to clarify a problem, define requirements for an artefact and demonstrate whether the artefact solves that problem. "The design-science paradigm seeks to extend the boundaries of human and organisational capabilities by creating new and innovative artefacts…" (Hevner, March, Park, & Ram, 2004). When investigating Business Information Security and the kind of problems that can arise, we can distinguish two types of problems. Horst Rittel (1969) refers to "wicked problems", e.g. problems that are difficult or impossible

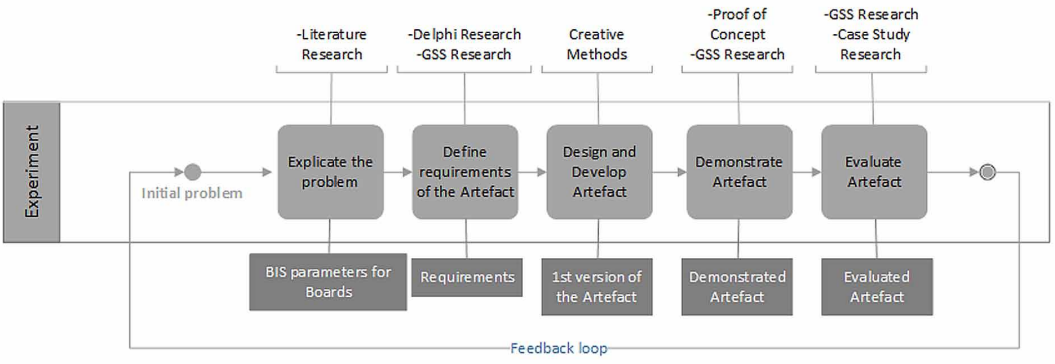
Figure 1. Hevner's Design Science Research Framework (2004)



to solve (for example poverty) and "tame problems" – those that can be solved with a particular solution within a certain timeframe (e.g. involving algorithms and constructions) (Johannesson & Perjons, 2014). We developed, tested and validated artefacts using the design science framework that was proposed by Hevner in 2004; see Figure 1 (Hevner et al., 2004).

On the right is a representation of the theoretical knowledge base that provides the materials with which design science is accomplished. This body of knowledge consists of prior established frameworks, foundations, theories or constructs. The knowledge base in effect establishes the academic rigour of the design sciences. On the left side, the practical business environment is represented. This defines the problem space in which the topic and its related problems arise. The environment encompasses people, organisational systems (structures, processes and relational mechanisms), technology etc. and confirms the relevance of design science. In the centre of the framework the design science artefact is crafted by activities related to designing, building, developing and evaluating an artefact that meets an identified business need. As a follow-up to Hevner's work, Perjon and Johannesson (2014) presented the seven DSR guidelines which are visualised in Figure 2. These guidelines can help researchers understand the requirements for effective DSR. Although design science focuses mainly on the artefact and not primarily on the execution of procedural steps, we

Figure 2. A Design Science Research Approach to Developing Experimental Artefact Requirements (Adapted from Perjon and Johanesson)



propose to use the approach taken by Perjon and Johanesson and propose multiple research methods to identify each step of the process used to establish the artefact. A key characteristic of DSR is the continuous alteration and maintenance of the artefact via feedback loops. In the initial phase of prototyping and experimenting the final product and its features are unclear. Wieringa refers to "requirement uncertainty" when establishing artefact requirements. In the first iterations, the artefact has just enough features to gather validated learning about the product and its continued development (Riesm 2009). This is why the exact requirements are initially not yet clear and continue to evolve over multiple iterations of feedback loops. Van Aken (2004) refers to "fuzzy front end", which makes designing precise, immediate requirements impractical.

Validating the artefact in order to execute DSR is seen as one of the main challenges of DSR publications, since validating is hard and complex (Arnott & Pervan, 2010) Another challenge is objectivity; this refers to the extent to which research is impartial and freed from the subjective judgement of the researcher, especially with interpretivist research such as BIS (Recker, 2013). DSR is sometimes limited in precision due to the absence of rigour in practical environments. The output of the research iterations largely depends on the way the problem is framed. When there is insufficient or incomplete input for the design science framework, the outcome is poor (Johannesson & Perjons, 2014). This identification and explication process within BIS research ideally comes from the literature, GSS and/or Delphi research methods.

The Use of GSS in Setting Requirements

GSS can also facilitate the creative process of setting functional requirements for a design science research artefact (Trembley, Hevner, & Berndt, 2010), i.e. indicators of the individual maturity level. The Delphi research method (using surveys) is ideally positioned parallel to or before GSS to scrutinise or validate specific content in the literature. According to Tremblay (2010), validation by testing against expert opinions (in focus groups) enhances the academic rigour as well as the relevance of research and contributes to a sound knowledge base. There is no 'ideal size' for a focus group (Fern, 1982) "Focus group sessions can be structured, or unstructured, depending on the purpose of the research. The group discussion is led, and controlled, by a facilitator whose role it is to: stimulate a free-flowing discussion; help members share their experiences; elicit the views of all participants; keep group members on track; and capture responses." (Newby et al., 2003). The role of the facilitator is important in order to avoid the "Ash Effect" where certain individuals dominate the group dynamics and therefore the outcome (Asch, 1951). Since the size of the group has an impact on the ability of the group to achieve a productive outcome (Dennis et al., 1990) the selection of the right (number of) experts is key to obtaining collective intelligence. The group solution is better than any one member

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). 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	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 [60] 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 business alignment process and decision-making process. Threat of the "law of the decibel". Requires professional group moderation skills.

could have produced before the discussion (Linstone, 2002). So, too many participants may cause too much 'noise on the line' and too few participants may compromise the data.

DEFINED RESEARCH METHOD

In this paper, we have examined a number of methods for designing and engineering a BIS artefact, based on the literature. The core contribution of the methods used in combination with DSR is summarized in Table 1 below and this provides an answer to our research question: Which research methods contribute to defining the requirements for the parameters of a Business Information Security artefact? The conclusion of this examination is that GSS can contribute by: a) examining, selecting and defining parameters (e.g. artefact requirements) and b) establishing consensus and decision-making related to implementing the artefact to address the business problem of BIS (fit for purpose).

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 on 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 (Johannesson & Perjons, 2014; Aken & Nagel, 2004; Hevner et al., 2004; Wieringa, 2014; Winter, 2008; Dietz & Hoogervorst, 2013; Albani et al., 2016) to improve the Maturity of Business Information Security is coined and published as the "MBIS method" in several publications (Bobbert & Mulder, 2016a; 2010; 2015; 2013; 2016b).

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 BIS research. It was published in the International Journal of Business IT Alignment in 2012 (Bobbert & Mulder, 2010), and presented at the HICSS conference in the USA in 2013 (Bobbert & Mulder, 2013) and at the International Conference on Computational Intelligence and Communication Networks in 2015 (Bobbert & Mulder, 2015). The second proposition (b) was researched and tested in collaboration with Antwerp Management School among 25 CIOs and CISOs, who tested the implementation of the predefined artefact requirements (Mari, 2016). The participants ranked the use of a scorecard as the number one requirement to be engineered in an artefact. This illustrates the relevance of the topic and the contribution of this MBIS research. Ongoing research has been performed on applying GSS for identifying and defining requirements for an artefact that can enable knowledge management within a financial institute. The use of GSS in facilitating implementation and decision-making related to BIS has been researched and published in the ISACA Journal (Bobbert & Mulder, 2016a) and (in Dutch) in the Platform voor Informatie Beveiliging (PvIB) magazine (Bobbert & Mulder, 2016b).

The initial aim of this research paper is to examine ways of defining parameters of control using qualitative methods with the final objective to specify requirements for a BIS artefact. A limitation of this paper is the focus on the first two stages of Johannesson and Perjons' DSR framework, namely examining the research methods that can define the requirements for an artefact. This paper is limited in describing how the requirements were engineered into the artefact and how these requirements were validated by the stakeholders. This demonstration and evaluation part of the artefact development is, since 2010, subject to ongoing research. The artefact is restricted accessible for organisations as well as researchers via the url; https://apps.securimeter.eu/.

When the qualitative approach is further enhanced via the rigour and relevance cycles and data from the environment is entered into the artefact, it becomes a knowledge base. This makes quantitative analysis of the gathered data possible. When this data set is sufficiently extensive, statistical analysis can be performed, which enables representative sampling. Statistical inference could be the subject of future research.

REFERENCES

Abraham, S. (2011). Information Security Behavior: Factors and Research Directions. In *Proceedings of the Seventeenth Americas Conference on Information Systems*.

Aken, V. J., & Nagel, A. (2004). Organising and managing the fuzzy front end of new product development. In *ECIS working paper series*. Eindhoven: Technische Universiteit Eindhoven.

Al-Omari, A. E.-G. O. & Deokar, A. (2012b). Information security policy compliance: the role of information security awareness. In *Proceedings of the American Conference on Information Systems*.

Albani, A., Raber, D., & Winter, R. (2016). A Conceptual Framework for Analysing Enterprise Engineering Methodologies. *Enterprise Modelling and Information Systems Architectures*, *11*(1).

Allen, J. (2007). Governing for Enterprise Security (GES) Implementation Guide. USA: Carnegie Mellon University.

Arnott, D., & Pervan, G. (2010). *How relevant is Fieldwork to DSS Design Science Research*. Australia: IOS Press.

Asch, S. (1951). Effects of group pressure upon the modification and distortion of judgment. In H. Guetzkow (Ed.), Groups, leadership and men. Pittsburgh, PA: Carnegie Press.

Bobbert, Y., & Mulder, J. (2010). 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.

Bobbert, Y., & Mulder, J. (2013). Group Support Systems Research in the Field of Business Information Security; a Practitioners View. In *Proceedings of the 46th Hawaii International Conference on System Science*, Hawaii.

Bobbert, Y., & Mulder, J. (2015). Governance Practices and Critical Succes Factors suitable for Business Information Security. In *Proceedings of the International Conference on Computational Intelligence and Communication Networks*, India.

Bobbert, Y., & Mulder, J. (2016). Boardroom dynamics: Group Support for the Board's Involvement in a Smart Security. *ISACA Journal, 5*.

Bobbert, Y., & Mulder, J. (2016). Vergaderen om te besluiten: Het gebruik van Group Support Systemen in informatiebeveiliging. Platform voor Informatiebeveiliging, 3, 4-7.

Cashell, B., Jackson, W., Jickling, M., & Webel, B. (2004). *The Economic Impact of Cyber-Attacks*. United States: Congressional Research Service, The Library of Congress.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2002). 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*, *2*.

De Haes, S., & Van Grembergen, W. (2008). Practices in IT Governance and Business/IT Alignment. ISACA Journal, 2.

Dennis, A. R., Valacich, J. S., & Nunamaker, J. F. (1990). An experimental investigation of the effects of group size in an electronic meeting environment. *IEEE Transactions on Systems, Man, and Cybernetics*, *20*(5), 1049–1057. doi:10.1109/21.59968

Dietz, J., Hoogervorst, J., Albani, A., Aveiro, D., Babkin, E., Barjis, J., & Winter, R. et al. (2013). The discipline of Enterprise Engineering. *International Journal of Organizational Design and Engineering*, *3*(1), 86–114. doi:10.1504/IJODE.2013.053669

Eisenhardt, K. (1989). Building Theories from Case Study Research. *Academy of Management Review*, *14*(4), 532–550.

Fern, E. (1982). The Use of Focus Groups for Idea Generation: The effects of Group Size, Acquaintanceship, and Moderator on Response Quantity and Quality. *JMR, Journal of Marketing Research*, *19*(1), 1–13. doi:10.2307/3151525

Flores, W., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. Computers & security, 43, 90-110.

Fox-IT. (2011). DigiNotar Certificate Authority breach, "Operation Black Tulip." FOX IT in assignment of the Ministry of the Interior and Kingdom Relations, Den Haag.

Hart, C. (1998). *Doing a Literature Review*. London: Sage.

Hevner, S., & March, J. (2004). Design Science Research in Information Systems. *Management Information Systems Quarterly*, *28*(1), 75–105.

Hovav, A., & DArcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. *Information & Management*, *49*(2), 99–110. doi:10.1016/j.im.2011.12.005

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. Decision Science, 43(4), 615-60.

IFAC. (2004). *Enterprise Governance: Getting the Balance Right*. London: International Federation of Accountants.

ISACA. (2012). *COBIT5 for Information Security*. United States: ISACA.

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

Ishiguro, M., Tanaka, H., Matsuura, K., & Murase, I. (2011). *The Effect of Information Security Incidents on Corporate Values in the Japanese Stock Market*. Tokyo, Japan: Institute of Industrial Science, The University of Tokyo.

ITGI. (2005). *Information Risks; Who's Business are they?* United States: IT Governance Institute.

ITGI. (2005). *Information risks; Whose Business are They*. United States: IT Governance Institute.

Johannesson, P., & Perjons, E. (2014). *An introduction to Design Science*. Stockholm University: Springer. doi:10.1007/978-3-319-10632-8

Kolfschoten, G., Mulder, J., & Proper, H. (2016). De fata morgana van Group Support System. *Informatie*, *4*(5), 10–14.

Koning, E., & Bikker, H. (2013). Using Standards to Create Effect in the Boardroom. *ISACA Journal,* 2.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. (2014). Information security awareness and behavior: A theory-based literature review. *Management Research Review*, *12*(37), 1049–1092. doi:10.1108/MRR-04-2013-0085

Linstone, H. T. M. (2002). *The Delphi Method, Techniques and Applications*. New Jersey: New Jersey Institute of Technology.

Maes, K. (2014). *The exploration of a process perspective on business cases and its relationship with the perceived success of IT enabled investments*. Antwerpen: University of Antwerp.

Mari, G. (2016). Cyber Security; Facts or Fiction. Antwerp Management School. Retrieved from http://blog.antwerpmanagementschool.be/

Moorsel, A., Stepanova, D., & Parkin, S. (2009). A Knowledge Base for Justified Information Security Decision-Making. Newcastle University, New Castle.

Newby, R., Soutbar, G., & Watson, J. (2003). Group Support System Approach. *International Small Business Journal*, *21*(4), 421–433. doi:10.1177/02662426030214003

Nonaka, I. (1994). A Dynamic Theory of Organizational Knowledge Creation. *Organization Science*, *5*(1), 14–37. doi:10.1287/orsc.5.1.14

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. In *Proceedings of the 40th Hawaii International Conference on System Sciences*, Big Island, HI. doi:10.1109/HICSS.2007.206

Pai, J. (2006). *An empirical study of the relationship between knowledge sharing and IS/IT strategic planning (ISSP)*. Emerald Group Publishing Limited.

Peters, F. (2012). *Reputatie onder druk; Het managen van reputaties in een veranderende samenleving*. Den Haag: SDU Uitgevers.

Pfeffer, J., & Sutton, R. (2001). *The Knowing-Doing Gap: How Smart Companies Turn Knowledge into Action*. Harvard Business School Press.

Plutchik, R. (1983). *Foundations of Experimental Research*.

Rakhorst, J. (2013). Structures processes and relational mechanisms needed to formulate a good business information security strategy [thesis]. Antwerp Management School, Belgium.

Recker, J. (2013). *Scientific Research in Information Systems*. Australia: Springer. doi:10.1007/978-3-642-30048-6

Ries, E. (2009). Minimum viable product. Startuplessonslearned. Retrieved from http://www.startuplessonslearned.com/2009/08/minimum-viable-product-guide.html

Rittel, H. (1969). Reflections on the Scientific and Political Significance of Decision Theory. The Institute of Urban and Regional Development, University of California.

Rutkowski, A., van de Walle, B., & Eede, G. (2006). The effect of Group Support Systems on the Emergence of Unique Information in a Risk Management Process: a Field Study. In *Proceedings of the 39th Hawaii International Conference on System Sciences*, Hawaii. doi:10.1109/HICSS.2006.459

Saunders, M., & Lewis, P. T. A. (2007). *Research Methods for Business Students*. Essex, England: Pearson Education Limited.

Schmidt, R., Lyytinen, K., Keil, M., & Cule, P. (2001). Identifying software project risks: an international Delphi study," *Journal of Management Information Systems, 17*(4), 5-36.

Silvermann, D. (2005). *Doing Qualitative Research*. London: Sage Publications.

Siponen, M. (2000). Critical analysis of different approaches to minimizing user-related faults in information systems security. *Information Management & Computer Security*, *5*(8), 197–209. doi:10.1108/09685220010353178

Siponen, M. (2010). Neutralization: New Insights into the problem of Employee Information system security policy violations. *Management Information Systems Quarterly*, *34*(3), 487–502.

Siponen, M., & Willison, R. (2009). Information Security management standards: problems and solutions. *Information & Management, 46*.

Solms, V. (2005). From Information Security to Business Security. In *Computer & Security*. South Africa: Elsevier. doi:10.1016/j.cose.2005.04.004

Tremblay, M., Hevner, A., & Berndt, D. (2010). The use of focus groups in design science research. *Design Science Research in Information System Science*, *22*, 121–143. doi:10.1007/978-1-4419-5653-8_10

Von Solms, R., & Von Solms, B. (2006). Information Security Governance; A model based on the Direct–Control Cycle. *Computers and Security, 25*, 408–412. doi:10.1016/j.cose.2006.07.005

Vreede, G., Boonstra, J., & Niederman, F. (2002). What is effective GSS facilitation? A qualitative inquiry into participants' perceptions. In *Proceedings of the 35th Hawaii International Conference on System Sciences*, Delft University of Technology, Netherlands. doi:10.1109/HICSS.2002.993942

Walsh, G., Mitchell, V., Jackson, P., & Beatty, S. (2009). Examining the Antecedents and Consequences of Corporate Reputation: A Customers perspective. *British Journal of management*. doi:10.1111/j.1467-8551.2007.00557.x

World Economic Forum (WEF). (2015). Partnering for Cyber Resilience; Risk and Responsibility in a Hyperconnected World - Principles and Guidelines.

Wieringa, R. (1996). *Requirements Engineering: Frameworks for Understanding*. Amsterdamn: VU Press.

Wieringa, R. (2014). *Design Science Methodology: For Information System and Software Engineering*. Berlin: Springer.

Winter, R. (2008). Design Science Research in Europe. *European Journal of Information Systems*, *17*(5), 470–474. doi:10.1057/ejis.2008.44

Workman, M., Bommer, W., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799–2816. doi:10.1016/j.chb.2008.04.005

Yin, R. (1994). *Case Study Research*. Beverly Hills: Sage.