Winter 12-11-2022

Beyond economic and financial analyses: A revelatory study of IT security investment decision-making process

Rajiv Kohli
College of William and Mary, rajiv.kohli@mason.wm.edu

Suprateek Sarker
University of Virginia

Mikko Siponen
University of Jyväskylä

Mari Karjalainen
City of Oulu

Beyond Economic and Financial Analyses: A revelatory study of IT security investment decision-making process

Rajiv Kohli[1]
Raymond A. Mason School of Business,
William & Mary,
Williamsburg, VA USA

Suprateek Sarker
McIntyre School of Commerce,
University of Virginia,
Charlottesville, VA, USA

Mikko Siponen
University of Jyväskylä,
Jyväskylä, Finland

Mari Karjalainen
City of Oulu
Oulu, Finland

Xiuyan Shao
School of Economics and Management,
Southeast University,
Nanjing, China

ABSTRACT

Information Technology (IT) security breaches and the extent of damage they may cause to an organization are inherently uncertain. Therefore, managers' decisions about whether to make IT security investment (ITSI) and how much, depend upon a subjective assessment of the economic value of the investment and the likelihood of the damage to the organization. When managers delay or fail to decide on whether and how much to invest in IT security, it can make organizations vulnerable to operational and strategic perils. Based upon interviews, document reviews, and observations in three organizations in Finland that made ITSI decisions to acquire a secure email application system, we examined the process through which ITSI decisions were made. Using institutional logics as the theoretical scaffolding, we find that ITSI decisions are driven by more than economic and financial analyses. We find that when stakeholders' logics conflict with each other's logics, framing through discourse gives way to a dominant logic, or a hybrid

[1] Corresponding author rajiv.kohli@mason.wm.edu (+1) 757-221-3267

logic which in turn results in an ITSI decision outcome. Trigging events, within or outside the organizations, can lead to iterations of the decision-making process. Using the metaphor of a spiral, we illustrate the repetitive iterations through which institutional logics shape stakeholders' ITSI decision-making process.

Keywords: IT Security, Revelatory Study, Decision making, cybersecurity, behavioral

INTRODUCTION

Information Technology (IT) security related cyber breaches are a global menace. For years, cyber breaches have interrupted organizational operations and compromised private data, and these perils have further accelerated due to dispersed workforce during COVID-19, leaving organizations even more vulnerable. IT security experts point to *underinvestment in IT security infrastructure* and the *senior managements' apathy* among the major reasons for unpreparedness of organizations with respect to cyber threats (Kelly 2017); yet relatively few scholarly works have examined the process to understand how IT Security Investment (ITSI) decisions unfold within organizations and why many seemingly essential ITSI are stalled or declined.

IT security professionals face challenges in getting their organizations to commit to ITSI due to multiple stakeholders who do not have a clear sense of the overall risks of cyberattacks, malware, and data leaks because cyber risk reports are highly technical (Boehm, et al. 2020), and when business managers do engage with understanding cyber risks, they are often divided over the utility of ITSI. Given the different ways managers perceive security threats, they find it difficult to agree on ITSI decisions, leaving organizations vulnerable to cybersecurity uncertainties (Jalali, et al. 2019).

Previous literature on ITSI has primarily focused on ways to improve algorithms to calculate optimal levels of investments, develop comparative tools to evaluate ITSI alternatives, implementation of IT security systems, and the importance of ITSI to organizations. These research streams may be characterized as the decision-theoretic approach, the game-theoretic approach, the neo-institutional economics approach, and the baseline approach. A sole reliance on economic and quantitative analyses also ignores or simplifies the importance of human agency and managerial volition in making decisions in highly uncertain contexts, where the key metrics (e.g., threat likelihoods, value of intangible assets) are poorly understood, unavailable or speculative (Magnusson, et al. 2007, Shao, et al. 2020). Recognizing the salience of the social context, Kwon and Johnson (2014) express the need to *"...pay considerable attention to the decision processes in security management in order to maximize the effectiveness of the investments*." (p. 468, emphasis added). Considering the limitations in our understanding of ITSI decisions, we seek to understand how ITSI decisions are *actually* made in organizations, and the specific considerations that drive the decision makers' choices. Therefore, our primary research question is: ***What is the process through which ITSI decisions are made in organizations?*** Our objective is to examine the nature of the ITSI decision-making process because we believe that understanding the process is key to devising ways in which ITSI proposals can be better managed when they are being considered for approval. Based on our interpretation of three cases studies, in this extended abstract we seek to reveal: a) the complexity of the decision-making process and characteristics of ITSI, b) how ITSI decisions are revised over time, and the circumstances associated with the revised decisions; c) critical events that may cause a change in the reasoning behind the decision; and d) the ways in which the divergent interests are reconciled.

The rest of the paper is organized as follows. We provide an overview of the relevant literature on IT investments and ITSI. Next, we present our theoretical scaffolding, that is informed by the literature on institutional logics. We then describe our methodology and provide narratives of three case studies. Thereafter, we present interpretation and discussion of our findings, and illustrate it with a spiral model to organize ITSI decision making.

OVERVIEW OF THE RELEVANT LITERATURE

Organizations safeguard information systems (IS) through investments such as e-mail encryption, intrusion detection systems, anti-virus software, and education campaigns (Johnston and Warkentin 2010; Puhakainen and Siponen 2010). Nonetheless, organizations tend to invest insufficiently in IS security (Ernst & Young 2012).

Although overall ITSIs in organizations have increased, by and large, they have not kept up with the significantly higher increases in overall IT assets that need to be protected, known as *technical debt,* which raises potential security threats to the IT infrastructure (Ernst & Young 2012). To overcome technical ITSI debt, IT managers must make a strong business case for ITSI and expand business mangers' understanding of the IT security vulnerabilities (ISF 2013; Wood and Parker 2004). This understanding is often lacking because general managers and managers from functional areas of the organization fail to appreciate IT security risks. Further, fragmented interests and priorities among business managers, lack of direct relevance to their operations, and mixed views regarding ITSI solutions underestimate cybersecurity risks.

As IT security investments are a form of IT investment, it is reasonable to ask whether IT security investment decisions can be explained by the way IT investment decisions are made. We argue that although the two are similar in that they require committing financial and human resources, typically ITSI needs a different type of advocacy and justification process compared

to other IT investments that can be justified by economic or financial metrics such as return on investment (ROI). We summarize past IT investment research into five perspectives -- service, isomorphic, compliance, survival and strategic. Upon assessing compatibility of each perspective with the underlying assumptions of ITSI, we find that past IT investment research is generally economics-driven and measure efficient customer services, comply with regulations, and mitigate risk, keeping up with competitors, and competitive advantage. We find that among the five perspectives, only compliance and survival perspectives are based on risk-based assumptions and focus on how to deploy or exploit IT investments. As such, they offer little insight into the *process* through which ITSI decisions are carried out, particularly how different stakeholder objectives coalesce to arrive at a decision. An understanding of what drives the ITSI approval process is important because without it, managers cannot acquire or deploy cybersecurity technologies and protect the organization.

Economic approaches are useful after the stakeholders have arrived at a shared understanding of the importance of ITSI, and past IT investment literature can potentially inform managers how to extract greater value from the ITSI. For example, questions about how ITSI should it be allocated efficiently to different parts of the organization and when, are relevant *after* ITSI is agreed upon and approved. Therefore, it is important that organizations first reconcile the divergent positions of stakeholder decision-makers and establish a common ground for the decision-making process.

In the IT Security Investment literature, evaluation methods such as return on investment (ROI) and break-even analysis (BEA) have been proposed to inform whether the benefits are worthy of the investment. This decision-theoretic approach typically focuses on selecting the optimal level of investment that will keep the firm operational. The limitation of the decision-

theoretic approach is that it does not account for the uncertainties from external risks (Knight 1965) and impact on the operations.

THEORETICAL SCAFFOLDING

As indicated above, research in IS academic literature is dominated by what can broadly be characterized as an economic perspective, yet we find accumulating anecdotal and empirical evidence that there are gaps in our understanding of ITSI and ITSI decision-making practices when we rely solely on the economic perspective (Magnusson et al. 2007). Therefore, we needed a theoretical perspective that would serve as a "scaffolding" for exploring a phenomenon to help us discern a) the different stakeholders' perspectives, b) the disagreements between the different perspectives with respect to ITSI, and c) how these different perspectives were eventually resolved (or went unresolved, in some cases). Haveman and Gualtieri (2017) propose that institutional logics may be seen as "systems of cultural elements (values, beliefs, normative expectations) by which people, groups, and organizations make sense of and evaluate their everyday activities and organize these activities in time and space.*"* Institutional logics are appropriate to study the ITSI context because probabilities of a cyberattack and the potential damage are often unknown *a priori*, there hardly exist a reliable source of information that can be used to accurately predict future attack and impact on an individual organization.

Our cases focus on the *intra-organization-level decision-making process* associated with ITSI, and we seek to uncover the logics that guide decisions at different points in time pertaining to a particular ITSI decision and the mechanisms of resolution of competing or contradictory logics. Given that our study focuses upon the agency of stakeholders/managers and their decision-making, we propose that that "decision logics" is a more appropriate label for the

decision-making process, while noting that the connections with the higher-level institutional logics are present but implicit. Next, we provide a brief discussion on the methodology.

METHODOLOGY

We adopted the interpretive case study approach (Walsham 1995, Walsham 2006) to gain an "experience-near" understanding of the process of ITSI decision-making that has, thus far, been largely missing in the literature. The data for this three-case study came primarily from 11 stakeholders, some of whom were interviewed more than once. The average interview time for each stakeholder was 67 minutes, including follow-up interviews. Most interviews were conducted by a subset of authors between 2014-20. We also examined documents and observed operations in which ITSI was implemented. The three cases that we report in this study, all from Finland, offered us the opportunity to study the ITSI phenomenon within a variety of circumstances though within a similar national context, which allowed us to identify recurrent patterns and offer transferable abstractions, within certain boundary conditions. Our methodological approach for uncovering the ITSI *decision-making processes* is consistent with previous approaches that "involved interpreting the narratives of the interviews to discern a temporal sequence among activities…"; this is in line with the study of "... change processes in the fields of organization studies (Langley and Tsoukas 2010)" and IS (Karjalainen, et al. 2019).

CASE NARRATIVES

We present an abbreviated narrative for CASE 1: Education Corporation (EduCo), an education-and-training service organization with more than 3000 employees. Employees in many departments who work with proprietary and confidential datasets are concerned about the computer security. Considering the internal concerns of security risks and the need to comply with state and federal regulations, the Chief Information Security Officer (CISO) felt the need

for an email-encryption software (EES, a pseudonym) that was functionally suitable and technically advanced.

Decision point #1 (pilot approved)

Given the security gap due to the lack of suitable email encryption, and after evaluating various solutions, the CISO proposed a pilot project to the CEO. The proposal involved evaluating EES and its suitability for EduCo. The CISO framed the need for EES as one that would overcome the gap between the current preparedness against cybersecurity hacks and the stated EduCo strategic goals of providing an environment where data for education and research projects and consulting advice can be exchanged in an electronically secure manner. The CEO approved the ITSI to initiate a pilot project for EES.

Decision point #2 (project funding declined by the executive board)

Despite the CISO's efforts in the pilot, and an overall positive report, the proposal for EES implementation was declined by the executive board. Upon review of the implementation plan, several executive board members who were from the units across EduCo expressed concerns that the EES would cause unnecessary disruption in their unit's operation while others felt that the value from EES was insufficient. Given the vastly different priorities and perspectives of the executive board members about what is strategic, and the lack of clarity regarding the risks and benefits of the proposed investment as per the standard investment template that the company used for evaluating return-on-investment (ROI) in other projects, the CISO was unable to convince the executive board that the ITSI was a worthy of organization-wide implementation.

Decision point #3 (a new pilot approved): Several months later, a new executive was appointed to head EduCo's Human Resources (HR) department. As a trained attorney, she was alarmed to

see that employees frequently sent emails containing confidential information through regular emails. She framed her arguments to appeal to the pride the members of the organization had related to its image and reputation that EduCo was a contemporary organization, given that some other leading organizations in the industry had adopted similar solutions. A pilot was approved and acceptance of SECEMAIL pilot across the organization offered reassurance that it would not impede operations and preserve EduCo's reputation of as a leader.

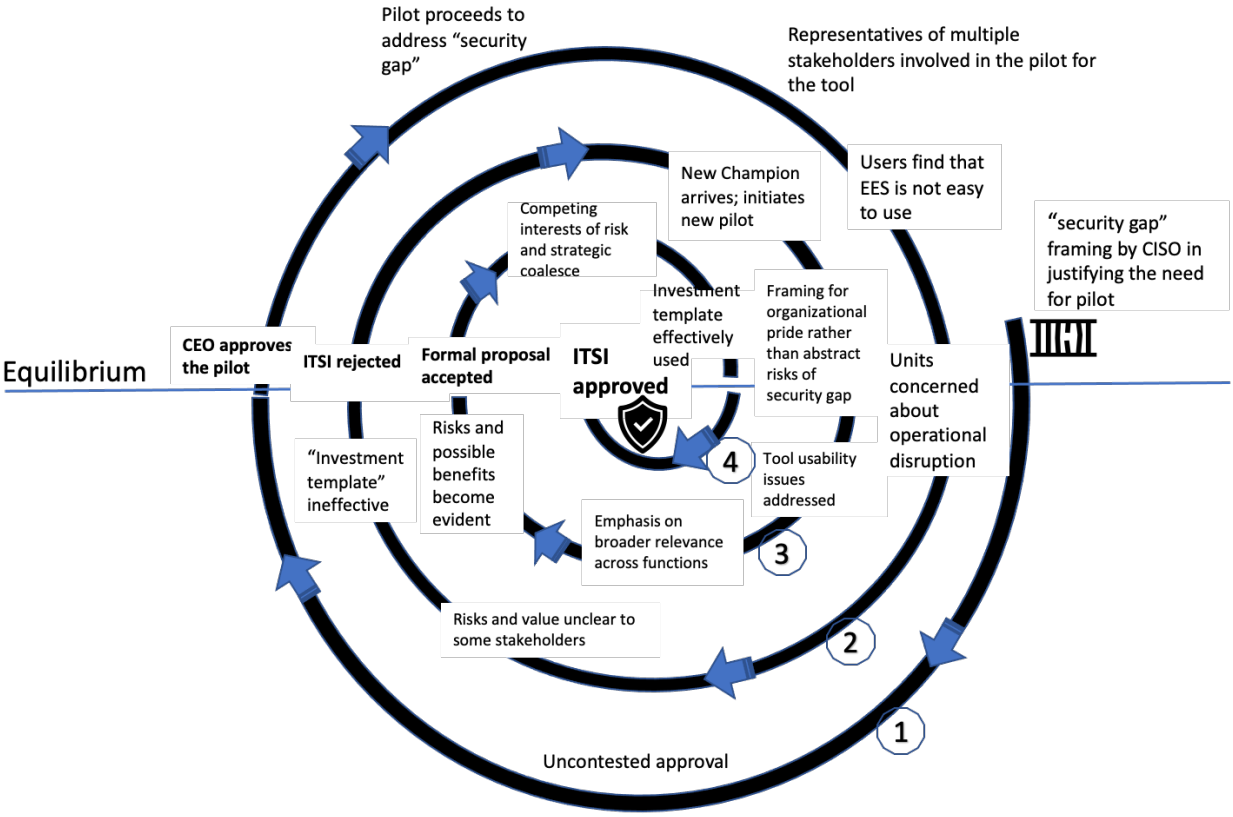

Figure 1: Spiral model of ITSI decision making process for EduCo (Case 1). Numbers inside circles refer to the iteration

Decision point #4 (project approved by the executive board): After getting positive feedback from the pilot testing, the CIO made the proposal for SECEMAIL, using the standard investment template, as before, to justify the IT security investment. Importantly, the proposal could make the risks and financial implications concrete and relatable for the board members now that they

understood the technology and how it affected their areas and the company's overall image and security. With the image of the organization as contemporary technologically-savvy at stake, the executive board approved the ITSI. Several factors contributed to the decision to approve.

INTERPRETATION AND DISCUSSION

Based on our understanding of the cases and the broader business environment in which the organizations functioned, we identify four dominant **decision-logics** evident in the ITSI decision-making contexts:, the ***strategic logic***, the ***local optimization logic***, the ***risk management logic***, and the ***financial management logic***.

The second theme is that of **temporality,** and hence changing contexts, associated with ITSI decisions. The third theme is the way **ITSI is framed** by those advocating the ITSI or championing it in the organization. The fourth theme is related to the idea of how the different **logics interact** with each other and coalesce, because of framing, power dynamics, and interventions such as training. The fifth theme is that of **equilibrium**, "a state of balance between opposing forces and actions that is either static... or dynamic" (Merriam-Webster.com).

Summary of Key Findings

First, ITSI decision-making seldom occurs in one-shot, and thus studying such decisions with cross-sectional studies can lead to, at worst, a flawed understanding, and at best, an incomplete understanding. The spiral model (Figure 1) is a suitable tool for research as well as practice because it illustrates how ITSI decisions transcend economic and financial metrics and risk, and involve decision makers' changing logics, and negotiations among the logics.

Second, rather than think of factors that lead to ITSI decisions, it may be useful to view them as driven by "logics" derived from the institutional environment, that decision-makers rely on to make decisions.

Third, framing can play a critical role in this decision-making process. The same framing can be effective or ineffective at different points in the process. Given that the risks are too abstract for many stakeholders in the early phases of the decision-making process, the detailed risk analysis may play a more important role in latter iterations. Our case study data also suggested similar patterns with respect to the financial logic.

Finally, we find that there are several equilibrium points at which a decision-process can stop. Many of these equilibria are temporary, and a trigger can lead to further consideration, and reconsideration and revision of an ITSI decision. The implication of this finding is that decision makers who feel strongly about ITSI must not assume that an ITSI decision that was denied or shelved, is final. We found that it takes time and patience to secure the entire organization's commitment for investments. While we did not encounter any case in which an approved ITSI decision was reversed, we believe that is altogether possible, if contextual conditions shift, it can trigger a new iteration in which a different decision logic is dominant, and the decision is reversed.

CONCLUSION

Though the IT business value literature provides rich insights into economic justification of IT investments, we have made the case for the need to revisit and re-examine ITSI decisions. As the probabilities and impacts of cybersecurity incidents are often difficult to predict in advance, we argued that managers must exercise decision logics, drawn from their values and beliefs, to guide their decisions. Through the interpretation of three case studies, involving investment in a secure email (SECEMAIL) in Finland, we find evidence that managers view ITSI through logics based upon their professional background that is often in conflict with other managers' logics. Our longitudinal perspective reveals that framing the problem through discourse can help in aligning

logics which in turn results in an ITSI decision outcome. A specific contribution we offer through this research note to the extant literature is an understanding of the ITSI decision making process. We find that ITSI decisions are not a one-shot decision, and that the various institutional logics, provide a more complete picture of ITSI decision making, than economical models alone.

REFERENCES

Boehm, Jim, James M. Kaplan, Peter Merrath, Thomas Poppensieker and Tobias Stähle, "Enhanced cyberrisk reporting: Opening doors to risk-based cybersecurity," *McKinsey on Risk*, 9, Issue Number, 2020, 1-10.

Haveman, Heather A and Gillian Gualtieri, "Institutional logics," In *Oxford research encyclopedia of business and management*, 2017,

Jalali, M. S., M. Siegel and S. Madnick, "Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment," *Journal of Strategic Information Systems*, 28, 1, (2019), 66-82.

Karjalainen, Mari, Suprateek Sarker and Mikko Siponen, "Toward a theory of information systems security behaviors of organizational employees: A dialectical process perspective," *Information Systems Research*, 30, 2, (2019), 687-704.

Kelly, Lisa, "Making a return on IT security investment," (2017),

Knight, Frank H., *Risk, Uncertainty and Profit*, Harper & Row, New York,, 1965.

Kwon, Juhee and M Eric Johnson, "Proactive versus reactive security investments in the healthcare sector," *MIS Quarterly*, 38, 2, (2014), 451-A3.

Langley, Ann and Haridimos Tsoukas, "Introducing perspectives on process organization studies," *Process, sensemaking, and organizing*, 1, 9, (2010), 1-27.

Magnusson, Christer, Josef Molvidsson and Sven Zetterqvist, "Value creation and return on security investments (ROSI)," *Proceedings of the IFIP International Information Security Conference*, 2007, 25-35.

Shao, Xiuyan, Mikko Siponen and Fufan Liu, "Shall we follow? Impact of reputation concern on information security managers' investment decisions," *Computers & Security*, 97, (2020), 101961.

Walsham, Geoff, "Interpretive case studies in IS research: nature and method," *European Journal of information systems*, 4, 2, (1995), 74-81.

Walsham, Geoff, "Doing interpretive research," *European Journal of Information Systems*, 15, 3, (2006), 320-330.