DOCTORAL CONSORTIUM

ORGANIZING FOR CYBER RESILIENCE: BALANCING RESILIENCE PARADIGMS FOR SUSTAINABLE IT BUSINESS VALUE

ZIGGY VAN GIEL
University of Antwerp, Faculty of Business and Economics, Antwerp, Belgium
ziggy.vangiel@uantwerpen.be

Organizational cyber resilience has been mentioned in literature to take a business-first perspective on ensure both short-term and long-term achievement of business objectives through technology. Nevertheless, it appears that it is still mostly approached from a technical perspective. When a business-first perspective is used, literature makes suggestions that are neither based on theory, nor on empirical findings. By using a design science research approach and relying on a combination of literature, surveys, interviews and case studies, this PhD project aims to develop strategies to achieve organizational cyber resilience by proposing specific organizational capabilities.

DOI
https://doi.org/10.18690/um.fov.4.2025.55

ISBN
978-961-286-998-4

Keywords:
cyber resilience, IT governance, digital strategy, engineering resilience, ecological resilience

University of Maribor Press

1 Introduction

The increasing reliance of organizations on IT for the achievement of their business objectives in combination with the increasing frequency and sophistication of external threats pose significant risks to organizations' survival. For that reason, there has been a call to transition from a traditional IT risk management approach to one centered around cyber resilience. Organizational cyber resilience is in this context defined as "the ability to deliver the intended outcome despite adverse cyber events". As compared to other concepts such as cybersecurity, it is said to take the business as a starting point. Despite organizational cyber resilience being positioned as a business-driven approach, existing literature reveal a persistent technical perspective. This gap underscores the need for research that integrates IT business value into cyber resilience.

This doctoral project aims to provide insights into how organizations can effectively organize and structure themselves to balance engineering and ecological resilience perspectives in the context of IT, ensuring both continuity through fast recovery and sustainable survival in an evolving external environment. Finally, this enables the organization to deliver short-term continuity and ensure long-term sustained IT business value.

2 Problem definition

Despite the growing body of knowledge on cyber resilience, existing literature predominantly focus on technical and operational aspects, often neglecting the organizational, business, and strategic dimensions. Nevertheless, cyber resilience is said to take the business as a starting point instead of the technical considerations. Because cyber resilience evolved in parallel from different domains and is often applied to specific problems, there is still conceptual ambiguity regarding cyber resilience.

Next, academic literature presents abilities that are said to lead to organizational cyber resilience. However, those propositions are neither based on empirical observations, nor on existing theoretical foundations. They are rather suggested abilities that would increase the chance of an organization to be cyber resilient. However, applications of those frameworks to case studies has yielded differing

results regarding the relevance of them. Also, there is no differentiation based on specific contingency factors. However, from contingency theory, and its application to IT governance theory, we know that there is no silver bullet that would work for every organization.

Finally, cyber resilience has been discussed as the next evolution of both cybersecurity and IT risk management. Combined with the conceptual relationship between cyber resilience and the broader (organizational) resilience domain, there is no consensus on the outcome of organizational cyber resilience. Depending on the specific niche, it can be business continuity, security, or something else.

Combining all the above, this research focuses on the following elements. Firstly, there is a need to provide conceptual clarity on what organizational cyber resilience entails, how it can be defined, and what fundamental paradigms form its basis. Secondly, based on the conceptual clarity and definition of organizational cyber resilience, the outcomes of it should be identified. Thirdly, theoretically grounded organizational capabilities for cyber resilience should be proposed that are validated through empirical observations. Combined these elements should answer the following research question: *How can organizations design and implement strategies to enhance their organizational cyber resilience?*

To conclude, this project is centered around (1) the antecedents or enablers of organizational cyber resilience, (2) the conceptualization, definition and theoretical paradigms underlying cyber resilience, and (3) the outcomes of cyber resilience for organizations. This is visualized in Figure 1.

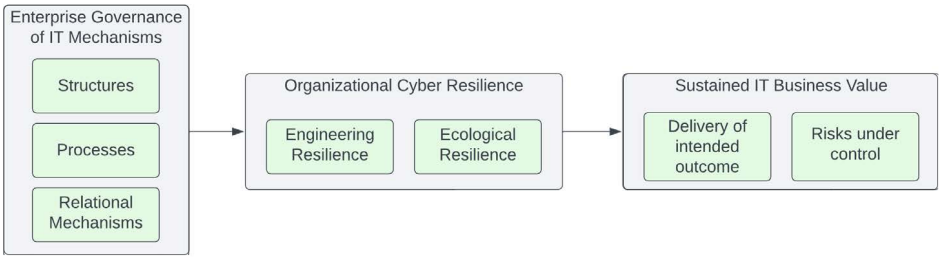

Figure 1: Conceptual model

3 Methodological approach of the different work packages

This doctoral project adopts a mixed-methods and design science approach conducted in different phases. While the overarching methodology can be specified as design science research with the aim to design strategies to improve organizational cyber resilience, different separate research initiatives can be identified. First, based on existing literature a bibliometric analysis and systematic literature review (SLR) are conducted. While the former aims to uncover trends in cyber resilience literature, the latter aims to provide conceptual clarity on what organizational cyber resilience entails, what theoretical perspectives are being used, and what is needed to achieve it. Consequently, organizational agility has been identified as an important aspect of organizational cyber resilience. Therefore, based on an international survey, the impact of different aspects of enterprise governance of IT on agility is analyzed. Next, because the capabilities proposed in literature are rather suggestions and not based on theory, a next phase employs a design science approach to propose capabilities that balance rigor and relevance. Finally,

3.1 Literature review: Bibliometric analysis & SLR

The first phase consisted out of a quantitative and qualitative literature review. First the quantitative literature review was a bibliometric analysis focusing on cyber resilience to uncover the trends in the domain. For this the process described by Zupic and Cater (2015) on bibliometric methods was followed to analyze the current trends in cyber resilience research while considering the potential evolution towards IT business value. A search string was evaluated on February 6th, 2024, and re-evaluated on February 7th, 2025.

Next, also a scoping literature review on organizational cyber resilience was performed. The review followed the five-stage methodological framework proposed by Arksey and O'Malley (2005), with enhancements from Levac et al. (2010) to ensure rigor and transparency. A scoping review is particularly suitable for clarifying key concepts, identifying thematic characteristics, and identifying knowledge gaps (Munn et al., 2018; Peters et al., 2021). The literature selection process is visualized in Figure 2. After the selection, the data was thematically analyzed to uncover patters

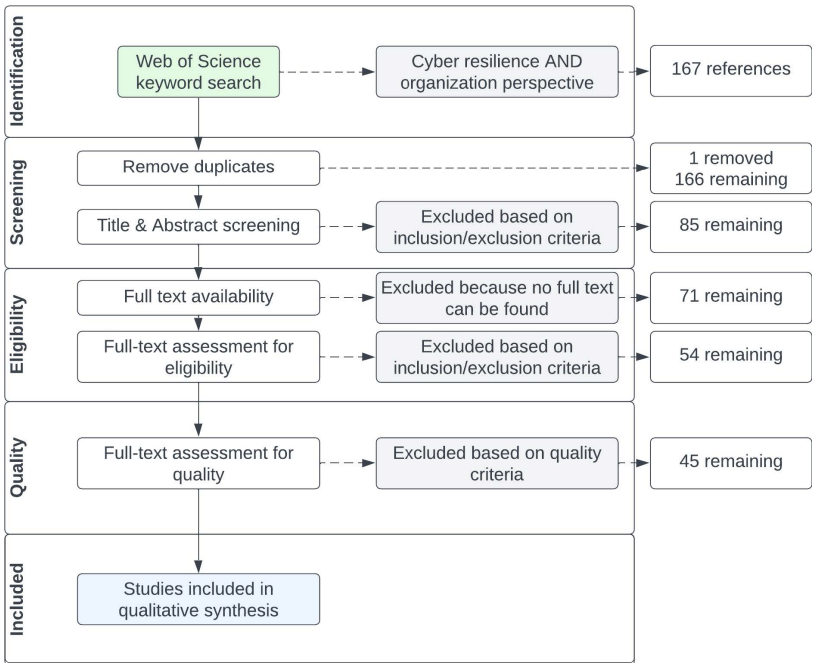

Figure 2: Scoping review literature search and selection strategy

3.2 Quantitative data collection: International survey based on COBIT 2019

The previous qualitative literature identified the organizational capabilities that are instrumental for organizational cyber resilience. Based on these capabilities, it became apparent that the operationalization of organizational agility based on Chakravarty et al. (2013) and Tallon and Pinsonneault (2011) highly aligns with organizational cyber resilience.

In collaboration with ISACA, an international survey was conducted in 2023 to measure the self-reported achievement of COBIT 2019 objectives, alignment goals, enterprise goals. Next, the survey also included questions on organizational agility based on Chakravarty et al. (2013) and Tallon and Pinsonneault (2011). As such organizational agility was operationalized through questions on three dimensions: entrepreneurial agility, adaptive agility, and business process agility.

We received 848 unique responses to the survey. However, 229 responses were incomplete as the survey was terminated before finalizing it, totaling to 619 potential valid responses. All questions on the achievement of the COBIT 2019 objectives, alignment goals and enterprise goals used a 5-point Likert scale with the option to answer "Don't know". Respondents that answered "Don't know" to every question or that gave the same answer to every question (e.g., score 2 for every question) were dropped. The reasoning was that it is very unlikely that a company has the same maturity for every aspect. The more plausible explanation would be that the respondent went quickly through the entire survey. As a result, an additional 51 observations were dropped, bringing the final total of valid responses to 568.

The data analysis included different elements. First, using some descriptive statistics an overview is proved of the sample on different dimensions such as sector, company size, threat landscape, compliancy requirements, or strategic role of IT (Nolan & McFarlan, 2005). Next, using Shapiro-Wilk test the normality of the data was assessed and assumed to be not-normally distributed. As the data originates from a Likert-scale questionnaire, the data is ordinal. Therefore, non-parametric techniques are used such as Mann-Whitney U test or partial least squares path modeling. The former is used to compare whether there are any differences between different sub-sets, while the latter is used to answer the research question on how IT governance impacts organizational agility.

3.3 System-theoretical development of organizational capabilities

Existing literature presents different abilities that organizations should possess to improve chances of cyber resilient behavior. However, they are neither empirically validated, nor theoretically grounded. Also, the theoretical paradigms used in contemporary organization cyber resilience literature appears to be highly aligned with the viable systems model of Stafford Beer (e.g., (Beer, 1979, 1981, 1985; Espejo & Reyes, 2011)). Namely, the ecological and engineering resilience perspective align with the different systems that aim to either focus on internal stability and synergies, or on adaptation to environmental changes.

As a result, a separate work package will aim to propose high-level organizational capabilities, theoretically grounded in the viable systems model. Finally, using case studies and interviews these high-level capabilities will be validated empirically.

3.4 Qualitative data collection: Case studies & Interviews

There is a close collaboration with an IT consulting company during this PhD project. This project is namely funded by the consulting firm by employing the PhD researcher. This means that the researcher has access to completed and ongoing consulting projects relating to different aspects of this PhD. Next, the researcher has also the ability to be actively involved in those projects. The ambition is to include those consulting projects in the future phases of this PhD project.

Obviously, as the PhD researcher is employed by the consulting firm, there is a clear risk of independence when the researcher participates in the consulting projects with the aim to include them in academic research. Nevertheless, this risk would be mitigated by either one of two strategies. First, case studies and/or interviews will be used to validate intermediate results. For example, this project proposes both organizational capabilities and strategies for enhancing organizational cyber resilience. Using interviews, feedback will be obtained on the proposed capabilities and strategies, while exemplary case studies will be used to illustrate the appropriateness of them.

Secondly, case studies and interviews will be used to supplement or illustrate specific aspects. For example, it has been shown in the literature review that management awareness is an important precondition for organizational cyber resilience. Also, depending on organizational characteristics, it has been shown that specific IT management and governance processes are more important. Based on these or other examples, a single exemplary case study, or a multiple extreme case study design can be used to illustrate those difference and their impact.

3.5 Bringing it all together: Design science taxonomy development

Based on the combination of the aforementioned research initiatives, a taxonomy will be developed for organizational cyber resilience strategies depending on organizational characteristics. For this, the design science research guidelines of Hevner et al. (2004) will be followed, combined with the taxonomy development method of Nickerson et al. (2013) as shown in Figure 3. This combination ensures the taxonomy of strategies are developed iteratively by incorporating continuous feedback when additional data is gathered and analyzed. While the design science

research approach ensures the proposed taxonomy to be both relevant for practice and academically rigorous, the taxonomy development model outlines the process of continuously integrating both theory and empirical findings.

That way this PhD project hopes to present strategies that are both grounded in theory and empirically validated, as compared to existing literature. Also, these insights should enable practitioners to tailor the strategies to the organization's needs based on specific characteristics.

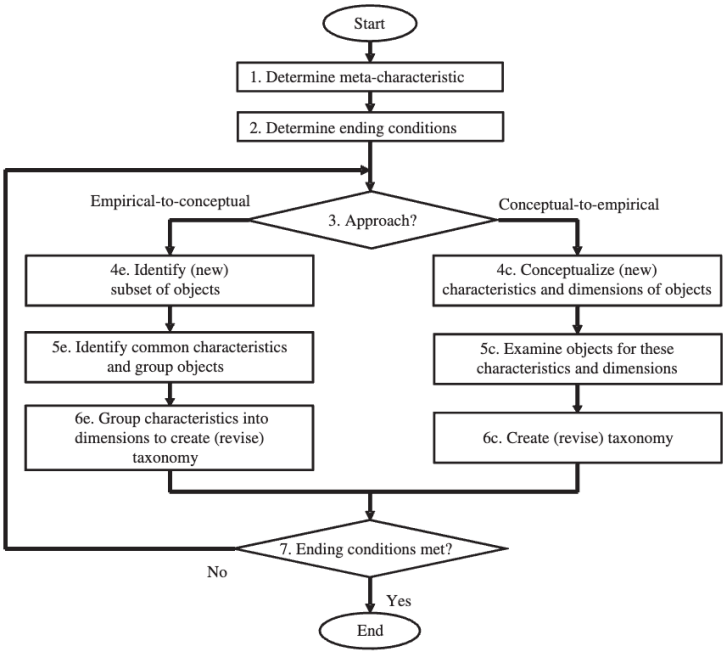

Figure 3: The taxoomy development method of Nickerson et al. (2013)

4 Risks, challenges and opportunities

This PhD project has some obvious risks, challenges and opportunities. However, the focus here will only be on the most significant differentiator as compared to other PhD projects, the explicit collaboration with an IT consulting firm.

While this offers some unique opportunities in terms of valorization and access to empirical data there are some risks and challenges that need to be discussed. Firstly, as already stated, the PhD researcher is employed by the consulting firm, which introduces the risk of conflict of interest. This risk is acknowledged and will be mitigated using the aforementioned strategies. Next, the involvement of the consulting firm could potentially hinder any alternative collaborations outside the consulting firm's network. On the contrary, when other organizations might be approached, the consulting firm might be interested from a commercial point of view, rather than an academic one. Additionally, approaching potential organizations or professionals to participate in the research becomes increasingly more difficult when an IT consulting firm is involved.

5 Conclusion

To conclude, the preliminary findings based on existing academic literature, systems-theory and two international surveys offers a good foundation for the future development of this project. Nevertheless, this project is characterized by some unique challenges and opportunities due to the involvement of an IT consulting firm as the main sponsor of this PhD project.

References

Arksey, H., & O'Malley, L. (2005). Scoping studies: towards a methodological framework. *International Journal of Social Research Methodology*, *8*(1), 19-32. https://doi.org/10.1080/1364557032000119616

Beer, S. (1979). *The heart of enterprise*. Wiley.

Beer, S. (1981). *Brain of the firm* (Second ed.). John Wiley & Sons Ltd.

Beer, S. (1985). *Diagnosing the system for organizations*. Wiley.

Chakravarty, A., Grewal, R., & Sambamurthy, V. (2013). Information Technology Competencies, Organizational Agility, and Firm Performance: Enabling and Facilitating Roles. *Information Systems Research*, *24*(4), 976-997. https://doi.org/10.1287/isre.2013.0500

Espejo, R., & Reyes, A. (2011). *Organizational Systems: Managing Complexity with the Viable System Model*. Springer.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in Information Systems research [Review]. *Mis Quarterly*, *28*(1), 75-105. https://doi.org/10.2307/25148625

Levac, D., Colquhoun, H., & O'Brien, K. (2010). Scoping studies: advancing the methodology [Article]. *Implementation Science*, *5*, Article 69. https://doi.org/10.1186/1748-5908-5-69

Munn, Z., Peters, M. D. J., Stern, C., Tufanaru, C., Mcarthur, A., & Aromataris, E. (2018). Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review approach. *BMC Medical Research Methodology*, *18*(1). https://doi.org/10.1186/s12874-018-0611-x

Nickerson, R. C., Varshney, U., & Muntermann, J. (2013). A method for taxonomy development and its application in information systems. *European Journal of Information Systems*, *22*(3), 336-359. https://doi.org/10.1057/ejis.2012.26

Nolan, R., & McFarlan, F. (2005). Information technology and the board of directors. *Harvard Business Review*, *83*(10), 96-106, 157. https://www.ncbi.nlm.nih.gov/pubmed/16250628

Peters, M., Marnie, C., Tricco, A., Pollock, D., Munn, Z., Alexander, L., McInerney, P., Godfrey, C., & Khalil, H. (2021). Updated methodological guidance for the conduct of scoping reviews [Article]. *JBI EVIDENCE IMPLEMENTATION*, *19*, 3-10. https://doi.org/10.1097/XEB.0000000000000277

Tallon, P. P., & Pinsonneault, A. (2011). Competing Perspectives on the Link between Strategic Information Technology Alignment and Organizational Agility: Insights from a Mediation Model. *Mis Quarterly*, *35*(2), 463-486. <Go to ISI>://WOS:000290842900011

Zupic, I., & Cater, T. (2015). Bibliometric Methods in Management and Organization. *Organizational Research Methods*, *18*(3), 429-472. https://doi.org/10.1177/1094428114562629