Cybersecurity-Enhanced Futures Thinking for Business Model Innovation in VUCA Environments

Miia-Maija Vakkuri, Heidi Vähänikkilä and Jyri Rajamäki
Laurea University of Applied Sciences, Espoo, Finland

miia.vakkuri@laurea.fi
heidi.vahanikkila@laurea.fi
jyri.rajamaki@laurea.fi

Abstract: In an increasingly volatile, uncertain, complex, and ambiguous (VUCA) business environment, organizations must adopt forward-looking strategies to remain resilient and competitive. This study builds upon the Futures Thinking and Business Model Innovation framework proposed by Vähänikkilä and Vakkuri (2025), integrating cybersecurity as a critical dimension of strategic foresight and organizational adaptability. While Futures Thinking enables companies to envision plausible and preferred futures, cybersecurity provides the structural integrity and trust necessary to realize those visions in digitalized ecosystems. Using qualitative methods, including interviews and co-creational workshops in the hospitality sector, the original research identified key barriers to Futures Thinking: lack of understanding and limited resources. This extended study proposes that cybersecurity awareness and preparedness can act as both a catalyst and a safeguard in business model innovation. Cybersecurity considerations—such as data protection, digital trust, and resilience against emerging threats—are mapped onto the five-stage innovation process: environmental scanning, vision formulation, knowledge alignment, innovation implementation, and feedback iteration. Examples from hospitality, e-commerce, and logistics illustrate how cybersecurity influences decision-making, customer trust, and operational continuity. The integration of cybersecurity into Futures Thinking tools (e.g., wild cards, foresight canvases) enhances scenario planning and supports dynamic capabilities such as sensing, seizing, and transforming. This research contributes a novel perspective to the academic discourse by linking cybersecurity with strategic foresight, emphasizing its role not only in risk mitigation but also in enabling innovation. The proposed model encourages organizations to treat cybersecurity as a strategic enabler rather than a technical constraint, fostering future-proof business models that are both visionary and resilient.

Keywords: Cybersecurity, VUCA Environments, Business Model Innovation

1. Introduction

In today's volatile, uncertain, complex, and ambiguous (VUCA) environment, hospitality companies face strong pressure because of digitalization, data-driven customer systems, and connected business networks (Bennett & Lemoine, 2014; Ivanov & Webster, 2019). Futures Thinking gives a structured way to imagine possible and preferred futures. It helps organizations learn in advance and prepare for different options (Voros, 2003; Ramírez & Wilkinson, 2016). At the same time, Business Model Innovation (BMI) allows companies to change how they create and capture value so they can stay competitive in uncertain times (Teece, 2010; Foss & Saebi, 2017).

Cybersecurity is often seen only as a technical protection, but it is more than that. It is a strategic capability that supports digital trust, operational resilience, and the success of future-oriented innovations (NIST, 2018; Woods, 2015). In this paper, we build on the Futures Thinking and BMI framework by Vähänikkilä and Vakkuri (2025) and add cybersecurity into the process. Our planned study, taking place in 2026, will use qualitative data from interviews and co-creation workshops in the hospitality sector. We argue that cybersecurity awareness and readiness can work as both a catalyst and a safeguard for business model innovation. This integration helps companies design business models that are not only innovative but also secure and resilient for the future.

2. Theoretical Foundations

2.1 VUCA and Strategic Responses

The business environment today is often described as VUCA, which means volatility, uncertainty, complexity, and ambiguity. Volatility refers to fast and unpredictable changes. Uncertainty means that future outcomes are difficult to predict. Complexity shows that many factors are connected and influence each other. Ambiguity means that information can be unclear or interpreted in different ways (Bennett & Lemoine, 2014).

VUCA conditions make planning and decision-making challenging. Traditional management tools often fail because they assume stability. Organizations need new approaches to deal with these challenges. One important approach is strategic foresight, which helps companies to look ahead and prepare for

different possible futures. It does not predict the future exactly but explores several options and supports better decisions under uncertainty (Rohrbeck & Kum, 2018; Ramírez & Wilkinson, 2016).

2.2 Futures Thinking and Business Model Innovation

Futures Thinking is a structured process that moves from scanning signals to creating scenarios and linking them to strategy (Voros, 2003). Scenario planning is one of the most common tools. It helps organizations to think about different futures and test their strategies against them. This improves robustness and resilience and gives more options for action (Schoemaker, 1995; Wright, Cairns & Goodwin, 2019).

Business Model Innovation means changing how a company creates and captures value. It can include new revenue models, partnerships, or service designs (Teece, 2010). Research shows that BMI is important for adapting to change and uncertainty (Foss & Saebi, 2017). In service industries like hospitality, BMI must fit customer journeys and digital ecosystems (Osterwalder & Pigneur, 2010; Wirtz et al., 2016).

2.3 Cybersecurity as Strategic Enabler

Cybersecurity is often seen as technical, but it is also a strategic capability. It includes preparedness, detection, response, and recovery (NIST, 2018). Strong cybersecurity builds digital trust, which influences customer behaviour and adoption of services (McKnight, Choudhury & Kacmar, 2002; Böhme & Moore, 2012). It also supports organizational resilience in complex systems (Woods, 2015; Hollnagel, 2011). This is very relevant for hospitality, where operations depend on data and digital platforms (Lu & Chen, 2015; Ivanov & Webster, 2019).

3. Proposed Framework: Cybersecurity-Enhanced Futures Thinking

Foresighting the future is an essential action in the business world. For that reason, managers must create new ways to build opportunities for using foresight methods beginning from the early stage of the business model innovation process. The following model illustrates how future thinking and business model innovation process can be linked with cybersecurity management. It introduces two phases: A) strategic and B) tactical. Companies must have a big picture of the future-oriented planning, and the practical implementation guidelines. In this process model there are five business development stages: 1) environmental scanning, 2) vision formulation, 3) knowledge alignment, 4) innovation implementation and 5) feedback and iteration (figure 1).

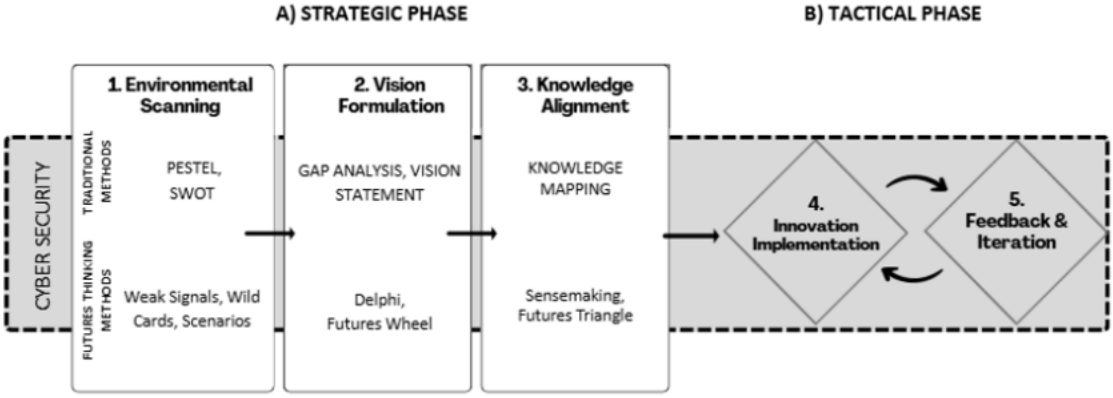

Figure 1: Cyber Security embedded Business Model Innovatin Process (modified from Vähänikkilä and Vakkuri 2025)

At every stage of the process cybersecurity is not just a technical add-on; it is a crosscutting, strategic element of the entire innovation process. It must be considered in all five stages.

3.1 Strategic Phase, Stages 1-3

This part consists of three essential stages that guides a company toward future-oriented decision-making. 1) Environmental Scanning in systematically observing and analysing external trends, drivers, and uncertainties that may affect the business. 2) Vision Formulation is creating a future vision based on insights from the environment. 3) Knowledge Alignment is about internal knowledge, competencies, and resources to support the strategic vision.

Business developing methods and tools for proceedings at strategic phase (A) has been divided to two sections, to traditional methods and future thinking methods. In this phase there are mentioned selected illustrative future thinking methods for each stage of the process. Traditional methods are more of management and market analysis approach to data gathering. Future thinking tools, on the other hand, are more oriented toward exploring uncertainties, envisioning alternative futures, and supporting strategic foresight and cybersecurity management. Companies use both traditional method tools like PESTEL analysis and future thinking tools like wild cards because they serve different but complementary purposes in strategic planning and foresight. Together, they help companies build resilient and agile strategies that consider both likely developments and surprising disruptions. The ability to use a future-oriented vision to understand and critically discuss potential scenarios is a key strategic competence in today's business environment (Moritz, 2005).

Embedding the role of cybersecurity to business model innovation process 1) Environmental Scanning: Identify cybersecurity-related trends, threats, and opportunities as part of the external environment analysis e.g., new regulations, security risks, customer expectations. 2) Vision Building: Integrate cybersecurity into the future vision – what will digital trust and data security look like in the business model of the future. 3) Knowledge Alignment: Ensure that the organization's expertise, resources, and processes support cybersecurity-oriented operations and strategy.

3.2 Tactical Phase, Stages 4-5

The tactical phase (B) translates strategic intent into action and learning. It includes two key stages: 4) Innovation Implementation, which focuses on executing the innovation strategy by developing and launching new solutions, services, or processes within the organization. After implementation last stage is 5) Feedback and Iteration, where outcomes are monitored and evaluated. Feedback is used to refine, adapt, or scale the innovation, ensuring continuous improvement and responsiveness to change. This process is not usually a step-by-step process. Instead, it often involves going back and forth between stages, with overlaps along the way. In many cases, innovation becomes connected in everyday service practices, rather than being a separate or isolated activity.

Embedding the role of cybersecurity to business model innovation process 4) Innovation Implementation: Take cybersecurity into account when developing and deploying new solutions, services, and processes e.g., integrating data protection and risk management. 5) Feedback and Iteration: Continuously assess and improve cybersecurity practices based on feedback and the evolving threat landscape.

4. Conclusions

Cybersecurity acts as both an enabler and a safeguard throughout the entire process. It supports digital trust, resilience, and the success of innovation – and therefore, it should be present at every stage, not just as a technical detail but as a strategic and cultural principle.

Ethics Declaration

Ethical clearance was not required for the research.

AI Declaration

Authors of this article used Microsoft 365 Copilot to structure the article contents they had written into coherent storyline. The tool was used to provide suggestions for improvements to text flow. The output from this tool was checked and modified by all authors, no direct text/content was used in the final article.

References

Bennett, N., & Lemoine, G. J. (2014). What VUCA really means for you. Harvard Business Review, 92(1/2), 27–42.

Böhme, R., & Moore, T. (2012). The economics of information security and privacy. Journal of Economic Perspectives, 26(3), 3–26.

Foss, N. J., & Saebi, T. (2017). Fifteen years of research on business model innovation. Journal of Management, 43(1), 200–227.

Hollnagel, E. (2011). Prologue: The scope of resilience engineering. In Resilience Engineering in Practice. Ashgate.

Ivanov, S., & Webster, C. (2019). Robots in tourism: A research agenda. Annals of Tourism Research, 78, 102762.

Lu, Y., & Chen, I. (2015). A review of hospitality information systems and e-business. International Journal of Contemporary Hospitality Management, 27(5), 879–896.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce. Information Systems Research, 13(3), 334–359.

Moritz, S. (2005) Service design—practical access to an evolving field. Köln International School of Design, Köln.

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity, v1.1. National Institute of Standards and Technology.

Osterwalder, A., & Pigneur, Y. (2010). Business Model Generation. Wiley.

Ramírez, R., & Wilkinson, A. (2016). Strategic Reframing: The Oxford Scenario Planning Approach. Oxford University Press.

Rohrbeck, R., & Kum, M. E. (2018). Corporate foresight and its impact on performance. Technological Forecasting & Social Change, 129, 105–116.

Schoemaker, P. J. H. (1995). Scenario planning: A tool for strategic thinking. Sloan Management Review, 36(2), 25–40.

Teece, D. J. (2010). Business models, business strategy and innovation. Long Range Planning, 43(2–3), 172–194.

Voros, J. (2003). A generic foresight process framework. Foresight, 5(3), 10–21.

Vähänikkilä, H., & Vakkuri, M. M. (2025). Futures Thinking: Unlocked Possibilities for Business Model Innovation in VUCA World. In Proceedings of the 25th European Conference on Knowledge Management (2 vols). Academic Conferences and publishing limited.

Wirtz, B. W., Pistoia, A., Ullrich, S., & Göttel, V. (2016). Business models: Origins, development and future research. Long Range Planning, 49(1), 36–54.

Woods, D. D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. Reliability Engineering & System Safety, 141, 5–9.

Wright, G., Cairns, G., & Goodwin, P. (2019). Teaching scenario planning: Lessons from practice. Futures & Foresight Science, 1(1), e1.