DOI
https://doi.org/10.18690/um.fov.4.2025.2

ISBN
978-961-286-998-4

BRIDGING CYBER RESILIENCE AND IT BUSINESS VALUE: A LONGITUDINAL BIBLIOMETRIC ANALYSIS

ZIGGY VAN GIEL,[1] TIM HUYGH,[2] ANANT JOSHI,[3]
STEVEN DE HAES[1]

[1] University of Antwerp, Faculty of Business and Economics, Antwerp, Belgium
ziggy.vangiel@uantwerpen.be, steven.dehaes@uantwerpen.be
[2] Open University, Faculty of Management, Science & Technology, Limburg, the Netherlands
tim.huygh@ou.nl
[3] University of Maastricht, School of Business and Economics, Limburg, the Netherlands
a.joshi@maastrichtuniversity.nl

Cyber resilience is often defined as the ability of an organization to continuously deliver the intended outcome despite adverse cyber events. While this definition takes the business and IT business value as a starting point, literature mainly focuses on technical or operational aspects of critical infrastructure or supply chains. This paper uses a longitudinal bibliometric analysis to analyze trends in both the current body of knowledge and the past body of knowledge regarding cyber resilience. The study shows that the domain shows a clear interest in emerging technologies (e.g., AI). However, it lacks fundamental conceptual research that tries to integrate cyber resilience with IT business value and the broader IT governance literature. To conclude, the results suggest that the domain would benefit from research that focuses on the business side of cyber resilience and the IT value it hopes to protect, instead of focusing on technical measures or sector-specific research.

Keywords:
IT business value,
cyber resilience,
digital transformation,
bibliometric analysis,
IT governance

University of Maribor Press

1 Introduction

Organizations increasingly depend upon information technology (IT) for the achievement of their business goals, which increases the importance of cyber resilience to ensure continuous delivery of IT business value. While there appears to be an increasing interest in cyber resilience, the literature on resilience in organizational sciences remains fragmented. One reason for this is that resilience is often applied on a specific problem rather than focusing on creating conceptual clarity first (Linnenluecke, 2017). Indeed, cyber resilience research is still in its infancy (Bellini & Marrone, 2020; Eling et al., 2021; Linnenluecke, 2017). Given its fragmented body of knowledge, the cyber resilience domain would benefit from an analysis of the main research streams. This would enable future research to focus on integrating the fragmented research streams to provide conceptual clarity and improve overall maturity of the domain. Therefore the first research question aims to provide an overview of these research streams within organizational cyber resilience to enable the integration of the fragmentated body of knowledge. *RQ1: What are dominant themes in the current literature on organizational cyber resilience? And what publications were of most influence?*

IT investments are driven by the potential realization of IT business value through benefits (e.g., increasing customer satisfaction, improved lead generation …), cost reduction, or risk minimization (Gartner, 2023). Cyber resilience, defined as "*the ability to continuously deliver the intended outcome despite adverse cyber events*" (Bjorck et al., 2015), has traditional been framed in relation to cybersecurity and IT risk management. First, while cybersecurity focuses on known complex threats, cyber resilience is said to focus on unpredictable and unknown threats to guarantee business continuity (Baikloy et al., 2020; Galinec & Steingartner, 2017). Next, Eling et al. (2021) mentioned that cyber resilience could be considered the next maturity level of IT risk management. Compared to other concepts, cyber resilience has been proposed to take the business as a starting point instead of focusing on technical approaches (Bjorck et al., 2015; Garcia-Perez et al., 2023). While some cyber resilience literature focuses on business and organizational aspects (e.g., Bagheri et al. (2023)), it is unclear whether the current body of knowledge has framed cyber resilience in relation to IT business value literature. However, the domain would benefit from a clear direct conceptual relationship between IT business value and cyber resilience. As a result, this paper aims to increase conceptual clarity by explicitly linking organizational cyber resilience to the continuous realization of IT-enabled business value. Hence the second research question focuses on exploring the extent to which this perspective is present or is being integrated in the current body of knowledge. *RQ2: To what extent is IT business value considered in the current literature on organizational cyber resilience?*

The remainder of this paper is structure as follows. Section 2 provides theoretical background on both IT business value and organizational cyber resilience with a specific focus on their conceptual definitions and operationalizations. Next, section 3 presents the methodology used for this paper. Section 4 then presents the findings of this research. Before concluding in section 6, the discussion in section 5 reflects on the implications and limitations of this paper while also presenting avenues for future research.

2 Theoretical Background

This section presents the results of a qualitative analysis of existing literature on both IT business value and organizational cyber resilience. While the former is based on an ad-hoc literature review, the cyber resilience section is based on a qualitative analysis of literature that was identified in 2024 for the bibliometric analysis.

2.1 IT Business Value

IT business value requires the continuous alignement of business and IT on a strategic, operational and structural level (Maes, 1999), which in turn is enabled through an appropriate IT governance (De Haes et al., 2020). As such, IT governance's final aim is the delivery of IT business value, while mitigating IT-related risks (Parent & Reich, 2009). Depending on how IT business value is defined, controlling IT risks might be part of IT business value. In this context, Gartner (2023) states that business value of IT can be realized in three different ways: increasing revenue, improving cost-efficiency, or mitigating risks. As such, IT business value can be seen as the impact IT has on those three different dimensions (i.e., benefits, costs, and risks). As IT risk mitigation can be considered a dimension of IT business value, the question becomes what a proper definition for IT business value would be.

There exist numerous definitions of business value in the context of IT. For example, Melville et al. (2004, p. 287) defined IT business value as "*[…] the organizational performance impacts of information technology at both the intermediate process level and the organization wide level, and comprising both efficiency impacts and competitive impacts.*" While this definition only stresses the impact on efficiency and competitiveness, mitigation of IT risks can be considered an investment in sustaining competitiveness. Next, Schryen (2013, p. 141) defined information system (IS) business value as "*[…] the impact of investments in particular IT assets on the multidimensional performance and capabilities of economic entities at various levels, complemented by the ultimate meaning of performance in the economic environment.*" This definition stresses the impact investments in IT might have on performance and business capabilities. Finally, Riera and Iijima (2019) defined digital business value as "*[…] the level of achievement of business objectives using information technologies.*" This definition focuses on the link between the realization of business objectives and IT. To conclude, these definitions establish a link between IT investments and either organizational performance or the realization of business objectives.

The current definitions of IT business value highlight a proportional impact of IT on performance or on the achievement of business objectives. However, measuring IT business value has proven to be difficult. It is namely highly contingent upon organizational characteristics and the type of IT investment. In this context, Weill and Broadbent (1998) discussed the business value hierarchy, which is visualized in Figure 1. They showed that it will be difficult to measure IT business value by using high-level measures such as revenue growth. This aligns with the findings of Davern and Wilkin (2010) that higher-level measures are inadequate to measure IT business value effectively. Using inappropriate measures of IT business value might risk false statements, which has been called the 'IT productivity paradox' (Brynjolfsson, 1993; Davern & Wilkin, 2010; Schryen, 2013). For example, using high-level measures such as financial metrics to evaluate IT business value introduces dilution (Weill & Broadbent, 1998) and neglects non-monetary value (e.g., employee/user satisfaction, improved collaboration). Just as with measures for IT business value, IT risks and their mitigation strategies need to be considered on the appropriate level (e.g., application-level versus organization-level).

There is however no one-size-fits-all for IT business value and managing IT risks. In this regard, Schryen (2013) mentioned three types of contextual factors: macro-economic, industry, and firm contextual factors. Similarly, Melville et al. (2004) distinguished between characteristics in the macro environment, competitive environment, and of the firm itself. In the context of industry contextual factors, McAfee and Brynjolfsson (2008) analyzed the competitive dynamics during a period of surging IT investments from the 1990s onwards. They found that turbulence is the highest in IT intensive industries. Because of this, Zmud and Sambamurthy (2012) concluded that organizations that invest heavily in IT, are operating in more turbulent business environments. Conversely, organizations that are operating in relatively stable environments do not need to invest heavily in IT. The environment in which an organization is operating clearly has an impact on IT business value by dictating the intensity and type of IT investments.

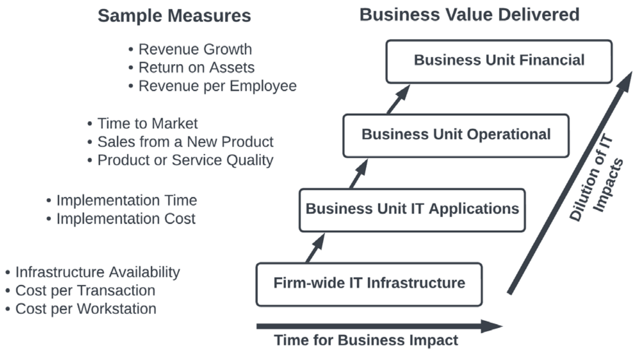

Figure 1: The Business Value Hierarchy

Source: Reproduced from Weill and Broadbent (1998)

While the external environment is an important factor influencing IT business value, also organization specific characteristics are important to consider. As mentioned before, the alignment between business and IT strategy has been considered an important precondition to realizing IT business value (e.g., (De Haes et al., 2020; Maes, 1999)). The business strategy, the accompanying business objectives, and the way in which IT supports the achievement of those objectives are important factors to consider when looking at IT business value and IT risks (Riera & Iijima, 2019).

Both perspectives (i.e., external environment factors, and organizational factors) can be combined in, what Nolan and McFarlan (2005) called, the IT strategic impact grid, as visualized in Figure 2. This model differentiates organizations based on the need for new IT, which is said to be dictated by market pressures (i.e., the external environment), and based on the dependency upon reliable IT, which is driven by the functioning and interdependence of business and IT. This model is also adopted by ISACA (2018) as a design factor in their COBIT 2019 on the IT governance operating model. Finally, from an IT risk perspective, the strategic role of IT will influence the importance of different types of IT risks (e.g., operational IT risks versus strategic IT risks, project risks versus business continuity risks etc.). As such, not every company might benefit from incorporate the same (cyber) resilience perspective (e.g., organizations that are in turnaround mode might not benefit from resilience as their dependence upon reliable IT is relatively low).

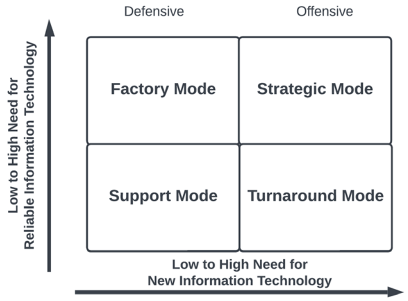

Figure 2: The IT Strategic Impact Grid
Source: Reproduced from (Nolan & McFarlan, 2005)

2.2 Organizational cyber resilience

Organizational cyber resilience has been defined in numerous ways. Firstly, one widely used definition of cyber resilience focuses on four events stages: (1) plan and prepare, (2) absorb, (3) recover, and (4) adapt and learn (Linkov et al., 2013; Linkov & Kott, 2019). It can be defined as “the ability of an organization to plan and prepare for, respond to, recover from, and adapt to a cyber arrack” (Annarelli & Palombi, 2021; Hausken, 2020; Onwubiko, 2020). Similarly, Bagheri et al. (2023) state cyber resilience consists out of “anticipation, support, recovery and adaptation in a changing environment”. The goal is then to improve the organization’s capability of facing adverse situations (Carias et al., 2020). While the event-based definitions of cyber resilience offer valuable insights, their approach is too narrow. An incident or crisis can namely be considered as process rather than an event (Williams et al., 2017). From this perspective, adverse events are solely events that manifested because of a process that preceded the event (e.g., mismanagement of risks, inadequate governance of an increasing reliance upon specific information systems).

Instead of an event-based approach, process-based approaches embed resilience thinking in the culture of an organization to build a sustainable business model (Sarkar et al., 2016). Cyber resilience then becomes "*a function of an organization's situation awareness […], management of […] vulnerabilities, adaptive capacity, risk intelligence, flexibility and agility […] in a complex, dynamic, and interconnected environment*" (Sarkar & Wingreen, 2015; Sarkar et al., 2016). It becomes clear that cyber resilience extends beyond the technical issues to include behavioral and organizational aspects (Bagheri et al., 2023). Instead of the technical domain, a holistic cyber resilience approach considers the physical, information, cognitive and social domains (Garcia-Perez et al., 2023; Linkov & Kott, 2019). It involves coordinated efforts on organizational, technological, and human factors (Safitra et al., 2023). Also, scholars argue that cyber resilience should be included in and aligned with the overall business strategy (Galinec & Steingartner, 2017; Sarkar et al., 2016). As an incident should be accepted as a likely event, cyber resilience should be considered a long-term endeavor that benefits from technology-neutral policy actions (Greiman, 2023). For that reason cyber resilience is not limited to specific processes (e.g., IT service management, IT risk management …), nor is it limited to a specific organizational sub-unit. Finally, cyber resilience is defined as "*the ability to continuously deliver the intended outcome despite adverse cyber events*" (Bjorck et al., 2015). Indeed, cyber resilience aims at sustaining the delivery of IT business value while acknowledging the potential impact of disruptions, which necessitates an organization-wide approach.

When combining the above definitions, a nuanced view on cyber resilience is presented. First, cyber resilience takes the business as a starting point by ensuring the ability to deliver value. Second, to achieve that a holistic perspective view on the organizations should be taken which extends beyond the technical. Finally, by acknowledging the potential impact of IT-related risks, cyber resilience aims to make the organization able to withstand both known and unknown disruptions. While the existing literature on cyber resilience does not explicitly incorporate IT business value, there is a clear link through their conceptualizations. Therefore, future conceptualizations and definitions of cyber resilience could benefit from the explicit integration of IT business value.

3 Methodology

This paper uses the process described by Zupic and Cater (2015) on bibliometric methods to analyze the current trends in cyber resilience research while considering the potential evolution towards IT business value. Using "cyber resilien*" as keyword relevant literature was identified from the Web of Science database. After an initial search that included synonyms (e.g., information systems resilience, organizational resilience of IT), the decision was made to not include synonyms. The number of papers that were not identified because of this was limited. However, the improved data quality and reduced need for manual screening outweighed the additional quantity of papers while increasing replicability. In Web of Science the results were refined to only include publications from the SCI-EXPANDED and SSCI indexes, and to only include articles, review articles and early access. This search was evaluated on February 6th, 2024, and re-evaluated on February 7th, 2025. The former yielded 195 results and the latter 311 results. The results of 2024 were also refined to only include references that focus on organizational aspects of cyber resilience as compared to other aspects of cyber resilience (e.g., resilience of individual applications, resilience of urban communities …). By doing that the final number of publications included in the final analysis was 66 instead of the original 195. That refinement enables an adequate analysis of the most influential references and sources based on relevant literature, while the unrefined set from 2025 gives a clear view on the different research streams that relate to cyber resilience.

As we are interested in the potential integration of IT business value perspectives in the cyber resilience domain, a co-word analysis is used to analyze the co-occurrence of bi-grams in the abstracts of the publications through the application of the Louvain clustering algorithm. This is repeated for both the 2024 and 2025 dataset to uncover potential evolution over time. Next, based on the refined set of 2024 the most local cited references, and the most relevant sources (i.e., journals or conferences) are presented.

4 Results

4.1 Trends in cyber resilience literature

When looking at the co-occurrence network of the 2024 dataset (see Figure 3), four different clusters can be identified: (1) a cluster focusing on cyber resilience of critical infrastructure (purple), (2) a cluster focusing on cyber resilience of supply chains (blue), (3) a cluster linking cyber resilience to IT risk management and cybersecurity (green), and (4) a cluster that focuses on the external perspective of cyber resilience in terms of external threats, incidents, cyberattacks and preventive measures to deal with those.

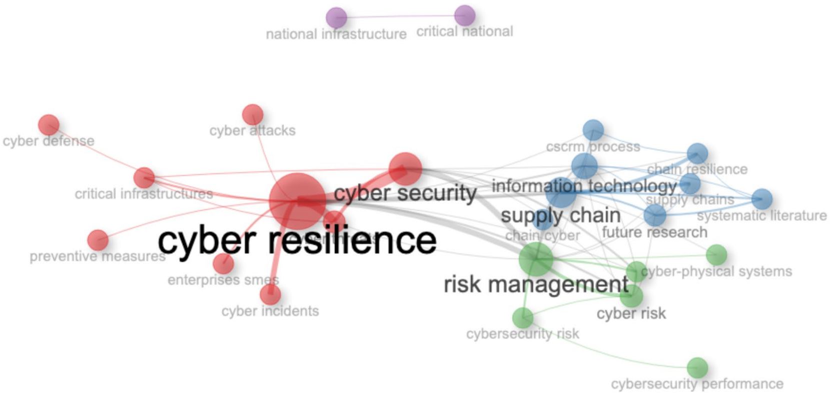

Figure 3: Co-occurence Network 2024

Source: Own analysis

Comparing these to the co-occurrence network of 2025 we again can identify four clusters (see Figure 4). Firstly, a cluster of research focuses on the cyber resilience of the energy grid and power systems (green). Secondly, the main cluster of research focuses on cybersecurity and supply chain related aspects (red). Thirdly, a cluster focuses on operational aspects of cyber resilience monitoring such as anomaly detection and injection attacks (purple). Finally, one cluster focuses on the application of emerging technologies such as artificial intelligence, machine learning, and deep learning in the context of cyber resilience and industrial control systems.

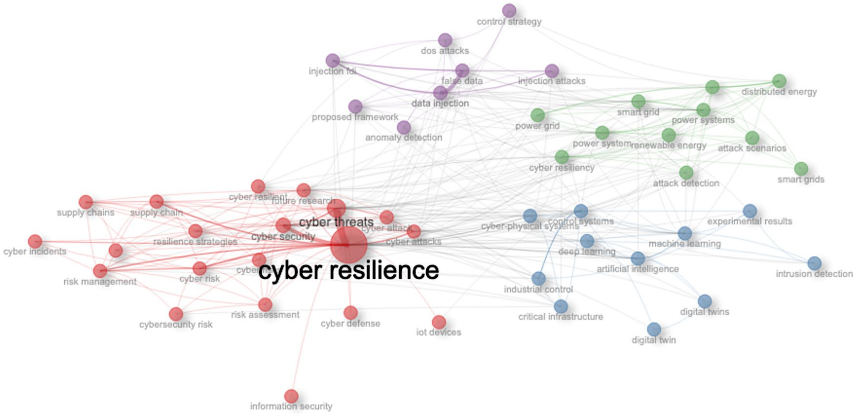

Figure 4: Co-occurence Network 2025

Source: Own analysis

4.2 Most influential references and sources

By using the most local cited references, and the most relevant sources, we can identify the influence of individual publications and identify seminal articles that lie at the basis of the domain. In Table 1 we can see that the publications of Bjorck et al. (2015), Linkov et al. (2013), and Linkov and Kott (2019) were the most influential for the cyber resilience domain. While the former presented a clear definition of cyber resilience, which was also used in this paper, the latter outlined the cyber resilience matrix that combines different event-phases of resilience (i.e., plan/prepare, absorb, recover, and adapt/learn) with four different domains (i.e., physical, information, cognitive, and social).

Table 1: Most local cited references

Reference	Number of Citations
(Bjorck et al., 2015)	13
(Linkov et al., 2013)	12
(Linkov & Kott, 2019)	11
(Boyes, 2015)	9
(Bodeau & Graubart, 2011); (Davis, 2015); (von Solms & van Niekerk, 2013)	6

Source: Own analysis

Next, Table 2 provides an overview of the most important sources for cyber resilience literature. 7 out of the 66 publications originate from Computer & Security journal. Next, IEEE Access and Supply Chain Management complete the top three of most relevant sources.

Table 2: Most relevant sources

Source	Number of documents
Computer & Security (ISSN: 01674048)	7
IEEE Access (ISSN: 21693536)	5
Supply Chain Management: An international journal (ISSN: 13598546)	4
Applied Sciences – Basel (ISSN: 20763417)	3
Sustainability (ISSN: 20711050)	3

Source: Own analysis

Combining the above trends and the most influential references and sources, we can see a focus on technical cyber resilience publications (security, monitoring, applications of emerging technologies such as AI), on risk-related aspects (risk management, external threats), and on specific sectors (supply chain, critical infrastructure, energy and power), Next to these main trends there are a limited number of references that were of significantly higher influence. The publications of Bjorck et al. (2015), Linkov et al. (2013), and Linkov and Kott (2019) were identified as most influential. These papers were conceptual papers that were already discussed in section 2. As concluded then, although there is a conceptual link, IT business value is not explicitly incorporated in cyber resilience literature.

5 Discussion

This paper started from two main research questions that focused on uncovering trends within cyber resilience literature and exploring the integration of the IT business value perspective. Based on the bibliometric analysis and the theoretical background that was provided before we indeed observe that literature applies cyber resilience to specific problems (e.g., specific sectors, specific external risks …), as mentioned by Linnenluecke (2017), instead of providing conceptual clarity first. While the most cited references were conceptual papers, they could be complemented by alternative perspectives. For example, instead of the event-based approach to cyber resilience as presented by (Linkov et al., 2013; Linkov & Kott, 2019), future research could explore a process-based perspective on cyber resilience.

Next, the definitions and conceptualizations of cyber resilience claim to take the business as a starting point (Bjorck et al., 2015; Garcia-Perez et al., 2023), and aim to enable continuous delivery of the intended outcome (i.e., continuous delivery of IT-enabled value) (Bjorck et al., 2015). However, the current literature does not reflect those perspective, evidenced by the lack of research trends in that direction and by the perspectives presented in the most cited conceptual papers. Indeed, there is a mismatch between the conceptual definition of cyber resilience and how it is used in academic literature. Therefore, future research could seek to integrate IT business value explicitly into cyber resilience conceptualizations in order to integrate the domains.

Finally, there is a stream of research focusing on IT business value that could be used to push the domain forward. Future research should take the business as a starting point when using cyber resilience and try to incorporate the final objective of cyber resilience on an organizational level: preserving IT business value. Also, past research has stated that cyber resilience is still in its infancy and lacks conceptual clarity (Bellini & Marrone, 2020; Eling et al., 2021; Linnenluecke, 2017). Nevertheless, this study has shown that there exist seminal articles that provides this conceptual clarity, but most papers neglect the broad perspective of the concept. Because of this, there is a clear need for research that applies cyber resilience holistically to an organizational context and takes the business as a starting point.

This research has different limitations which also offer opportunities for future research. Firstly, the scope is limited by a focus on IT specifically. Future research could incorporate OT as it significantly impacts the dependency upon reliable IT and cyber resilience. Next, the temporal difference shows some evolution in terms of trends. Nevertheless, future research could use a longer time horizon to uncover evolutions in the domain. Finally, the literature was selected only based on Web of Science and on only a single keyword. Future research could broaden this scope to incorporate more diverse perspectives.

6 Conclusions

This paper provided a theoretical background on IT business value and organizational cyber resilience. It claimed that there is a need to integrate IT business value because of their conceptual overlap. Next, it analyzed whether this business-first perspective is being used in contemporary research on organizational cyber resilience. While we expected to see the emergence of a trend that focuses on IT business value or related concepts, the past and current literature mainly focuses on technical aspects and emerging technologies (e.g., AI) in that context. Although cyber resilience is claimed to take the business as a starting point, as compared to cybersecurity, the literature does not reflect this evolution.

Acknowledgements

Special thanks to the two anonymous reviewers for their valuable input. Additionally, Flanders Innovation & Entrepreneurship is acknowledged together with AE, as the lead author (Ziggy Van Giel) is being funded through a Baekeland mandate at the time of conducting this research.

References

Annarelli, A., & Palombi, G. (2021). Digitalization Capabilities for Sustainable Cyber Resilience: A Conceptual Framework. *Sustainability*, *13*(23). https://doi.org/10.3390/su132313065

Bagheri, S., Ridley, G., & Williams, B. (2023). Organisational Cyber Resilience: Management Perspectives [Article]. *Australasian Journal of Information Systems*, *27*, 28. https://doi.org/10.3127/ajis.v27i0.4183

Baikloy, E., Praneetpolgrang, P., & Jirawichitchai, N. (2020). Development of Cyber Resilient Capability Maturity Model for Cloud Computing Services [Article]. *Tem Journal-Technology Education Management Informatics*, *9*(3), 915-923. https://doi.org/10.18421/tem93-11

Bellini, E., & Marrone, S. (2020, 2020). Towards a novel conceptualization of Cyber Resilience.

Bjorck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber Resilience - Fundamentals for a Definition. *New Contributions in Information Systems and Technologies, Vol 1, Pt 1*, *353*, 311-316. https://doi.org/10.1007/978-3-319-16486-1_31

Bodeau, D. J., & Graubart, R. (2011). *Cyber Resiliency Engineering Framework*. https://www.mitre.org/sites/default/files/media/publication/11_4436_2.pdf

Boyes, H. (2015). Cybersecurity and Cyber-Resilient Supply Chains. *Technology Innovation Management Review*, *5*(4), 28-34. http://timreview.ca/article/888

Brynjolfsson, E. (1993). The Productivity Paradox of Information Technology. *Communications of the ACM*, *36*(12), 67-77. https://doi.org/10.1145/163298.163309

Carias, J. F., Arrizabalaga, S., & Hernantes, J. (2020, Dec 03-04). Cyber Resilience Strategic Planning and Self-assessment Tool for Operationalization in SMEs.*IFIP Advances in Information and Communication Technology* [Information technology in disaster risk reduction, itdrr 2020]. 5th IFIP WG 5.15 International Conference on Information Technology in Disaster Risk Reduction (ITDRR), Univ Natl & World Econ, ELECTR NETWORK.

Davern, M. J., & Wilkin, C. L. (2010). Towards an integrated view of IT value measurement. *International Journal of Accounting Information Systems*, *11*(1), 42-60. https://doi.org/10.1016/j.accinf.2009.12.005

Davis, A. (2015). Building Cyber-Resilience into Supply Chains. *Technology Innovation Management Review*, *5*(4), 19-27. http://timreview.ca/article/887

De Haes, S., Van Grembergen, W., Joshi, A., & Huygh, T. (2020). *Enterprise Governance of Information Technology: Achieving Alignment and Value in Digital Organizations* (Third Edition ed.). Springer.

Eling, M., McShane, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, *24*(1), 93-125. https://doi.org/10.1111/rmir.12169

Galinec, D., & Steingartner, W. (2017). Combining Cybersecurity and Cyber Defense to achieve Cyber Resilience. *2017 Ieee 14th International Scientific Conference on Informatics*, 87-93. https://doi.org/10.1109/INFORMATICS.2017.8327227

Garcia-Perez, A., Sallos, M. P., & Tiwasing, P. (2023). Dimensions of cybersecurity performance and crisis response in critical infrastructure organisations: an intellectual capital perspective [Article; Early Access]. *Journal of Intellectual Capital*, *24*(2), 465-486. https://doi.org/10.1108/jic-06-2021-0166

Gartner. (2023). *Proving the Business Value of IT*. https://www.gartner.com/en/information-technology/topics/business-value-of-it

Greiman, V. A. (2023, Mar 09-10). Nuclear Cyber Attacks: A Study of Sabotage and Regulation of Critical Infrastructure. [Proceedings of the 18th international conference on cyber warfare and security iccws]. 18th International Conference on Cyber Warfare and Security (ICCWS), Towson Univ, Baltimore, MD.

Hausken, K. (2020). Cyber resilience in firms, organizations and societies [Review]. *Internet of Things*, *11*, 9. https://doi.org/10.1016/j.iot.2020.100204

ISACA. (2018). COBIT 2019 framework: Introduction & methodology.

Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions*, *33*(4), 471-476. https://doi.org/10.1007/s10669-013-9485-y

Linkov, I., & Kott, A. (2019). Fundamental Concepts of Cyber Resilience: Introduction and Overview. In (pp. 1-25). Springer International Publishing. https://doi.org/10.1007/978-3-319-77492-3_1

Linnenluecke, M. K. (2017). Resilience in Business and Management Research: A Review of Influential Publications and a Research Agenda [Review]. *International Journal of Management Reviews*, *19*(1), 4-30. https://doi.org/10.1111/ijmr.12076

Maes, R. (1999). Reconsidering Information Management Through A Generic Framework.

McAfee, A., & Brynjolfsson, E. (2008). Investing in the IT that makes a competitive difference. *Harvard Business Review*, *86*(7-8), 98-+. <Go to ISI>://WOS:000257047500024

Melville, N., Kraemer, K., & Gurbaxani, V. (2004). Review: Information technology and organizational performance: An integrative model of IT business value. *Mis Quarterly*, *28*(2), 283-322. https://doi.org/10.2307/25148636

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

Onwubiko, C. (2020, Jun 15-19). Focusing on the Recovery Aspects of Cyber Resilience. 2020 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), Dublin, Ireland.

Parent, M., & Reich, B. H. (2009). Governing information technology risk. *California Management Review*, *51*(3), 134-152. https://doi.org/10.2307/41166497

Riera, C., & Iijima, J. (2019). The Role of IT and Organizational Capabilities on Digital Business Value. *Pacific Asia Journal of the Association for Information Systems*, 67-95. https://doi.org/10.17705/1pais.11204

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity [Article]. *Sustainability*, *15*(18), 32, Article 13369. https://doi.org/10.3390/su151813369

Sarkar, A., & Wingreen, S. (2015, Sep 21-22). How CEOs of the Small Firms Make Decisions to Ensure Information Systems Resilience?*Proceedings of the European Conference on Information Management and Evaluation* [Proceedings of 9th european conference on is management and evaluation (ecime 2015)]. 9th European Conference on Information Management and Evaluation (ECIME), Univ W England, Bristol, ENGLAND.

Sarkar, A., Wingreen, S., Ascroft, J., & Assoc Informat, S. (2016). Top Management Team Decision Priorities to Drive IS Resilience: Lessons from Jade Software Corporation. [Amcis 2016 proceedings]. 22nd Americas Conference on Information Systems (AMCIS), San Diego, CA.

Schryen, G. (2013). Revisiting IS business value research: What we already know, what we still need to know, and how we can get there. *European Journal of Information Systems*, *22*(2), 139-169. https://doi.org/10.1057/ejis.2012.45

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Weill, P., & Broadbent, M. (1998). *Leveraging the new infrastructure—How market leaders capitalize on Information Technology*. Harvard Business School Press.

Williams, T. A., Gruber, D. A., Sutcliffe, K. M., Shepherd, D. A., & Zhao, E. Y. F. (2017). Organizational Response to Adversity: Fusing Crisis Management and Resilience Research Streams. *Academy of Management Annals*, *11*(2), 733-769. https://doi.org/10.5465/annals.2015.0134

Zmud, R. W., & Sambamurthy, V. (2012). *Guiding the digital transformation of organizations*. Legerity Digital Press.

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