Cybersecurity and Organisational Performance - the Interplay

Veena S Dorairajan [‡]

[‡] Ascensia Business School, Dubai, United Arab Emirates

Corresponding author: Veena S Dorairajan (veenasugu@gmail.com)

Abstract

The interplay between cybersecurity and organisational performance is multifaceted in nature, as it is related to how cybersecurity impacts and is impacted by various organisational activities and performance metrics. In the age of the rapid digitalization of organisations, cybersecurity emerges as an integral part of the health and effectiveness of an organisation. It includes not only preserving the confidentiality, integrity, availability of organisational digital assets but also establishing the organisational cybersecurity culture and, consequently, human behaviour. Cybersecurity and business are interdependent influencing each other significantly. This interplay shapes modern business.

The convergence of people, procedures, and technology to defend business, persons, or networks against digital attacks is known ascybersecurity. Cybersecurity is essential to protect organisational assets from risks such as but not limited to personal data breaches, unauthourised access leading to reputational and financial impact (Sandhu 2021).

Organisations that decide to implement digital technologies as part of their digital transformation journey are faced with increasing cyber threats and need to implement a reliable form of defence to protect their operations. In addition to digital transformation, organisations around the world are adopting artificial intelligence in their business process to reduce operating costs, boost productivity and improve customer experience. This introduces newer threats around artificial intelligence such as adversial AI attacks which involves attack vectors such as model poisoning. Artificial intelligence enabled cyber-attacks are also increasing and are contributing to the ever evolving complex threat landscape. Digital transformation and cybersecurity are intertwined elements crucial to today’s business. The strategic management of cybersecurity involves comprehensive understanding and measures against cybercrime, attacks, and terrorism to ensure organisational and business sustainability during digital transformation (Özsungur 2021). Effective cybersecurity practices are the cornerstone of successful digital transformation, protecting enterprises from evolving cyber threats and fostering a secure digital environment.

Effective cybersecurity management enhances business operations and reputation (Lopatova 2021). Businesses can turn cybersecurity into a commercial advantage by adopting proactive cybersecurity measures that not only protect assets but also assure business partners and customers of the firm's commitment to security. This can lead to smoother business transactions and partnerships, fostering trust across business networks . There is a shift in the perception about cybersecurity. It is now being viewed as a vital enabler for business growth fostering value creation and competitive advantage instead of being viewed as a cost burden. By mitigating cyber risks and fostering a secure information environment, businesses can enhance their operational efficiency, secure intellectual property, and maintain customer trust, thereby gaining a competitive edge.

Digital technologies shape the organisational design and brings cultural change. Digital transformation introduces cybersecurity challenges that necessitate a culture shift towards greater security awareness within organisations (Saeed et al. 2023). Human factors plays an important role in effective cybersecurity of the organisation. End users and IT professionals and cybersecurity personnel play pivotal role. A strong organisational culture enhances cybersecurity by aligning beliefs, values, and attitudes with security goals. Organisational leaders can foster a security-aware culture that supports the organisation’s overall cybersecurity objectives. The evolving business landscape requires continuous education on cybersecurity for all stakeholders within a company. This not only involves technical training but also understanding how cybersecurity impacts business strategies and operations. Educational initiatives need to cover the spectrum of risks and prepare businesses to handle emerging cybersecurity challenges effectively.

Cybersecurity must be managed strategically within an organisation to optimize performance and mitigate risks. This involves integrating cybersecurity into business strategy, recognizing it as a dynamic field that requires continuous adaptation and management. In short, cybersecurity strategy must align with business strategy and IT strategy. By integrating cybersecurity into the strategy and cultural fabric, organisations can increase their cyber resilience. The strategic approach of an organisation significantly influences its cybersecurity landscape. Firms focusing on innovation often face greater cybersecurity risks due to decentralized control systems and a variety of technologies that may introduce vulnerabilities. Conversely, efficiency-focused businesses may have more centralized and potentially more secure systems, though they also need to adapt to evolving cyber threats.

Effective cybersecurity practices are crucial for maintaining organisational integrity and performance. Cybersecurity influences various performance metrics, including risk management, compliance, and even financial performance.

Is there a connection between cyber security adoption and organisational performance? The organisation’s internal and external environmental elements need to be considered when studying the impact of the adoption of cybersecurity technologies. The three variables technology, organisation, and environment are used to identify the factors that affect on cybersecurity adoption. The technology-organisation-environment framework, referred to as the TOE framework, can be used for this analysis. Technological context considers the tenability, relative advantage, return on investment, cost, complexity, and compatibility. Organisational context considers the willingness to adopt, organisational readiness, knowledge and expertise, external support, communication process, and top management support. The environmental context considers competitiveness, external pressure, geopolitics and external events, fear of exposure, experience and laws and regulations.

In environments where system performance is prioritized over security, there might be a tendency to allocate fewer resources to security measures. This can leave systems more vulnerable to attacks. Rapidly deploying new features or updates to meet performance targets can sometimes lead to overlooking security best practices or conducting inadequate testing, creating potential vulnerabilities. Moving to the cloud and using third party services for improved performance also can increase the security risks if these services are not adequately vetted and managed.

The Security-Performance Tradeoff Model is a concept in cybersecurity that recognizes the balance between security measures that need to be implemented and the system performance that organisations need to maintain constantly. This model is important because both cybersecurity and the systems' performance can influence organisations' performance in terms of reputation, acceptance, etc. The Security-Performance Tradeoff Model is focused on the idea that there is usually a trade-off between cybersecurity and systems performance, and organisations need to manage a balance. It suggests that in some cases, the highest security levels can lower system performance, and vice versa. Organisations need to strike an appropriate balance by implementing tailored solutions that meet their security requirements without compromising operational efficiency or user experience.

The following approaches can be adopted to manage the trade-off:

- Risk-Based Prioritization to identify critical assets and potential vulnerabilities. Prioritize security measures based on the risk level and the organisation's risk appetite.
- Use optimization Techniques to reduce the impact of security measures.
- Design security controls with end user in mind (eg Single sign on, IP restriction)
- Implement continuous Monitoring and Testing
- Implement adaptive security frameworks that can dynamically adjust security measures based on the current threat landscape.

Presenting author

Veena S Dorairajan

Presented at

The Art and Science of Managing Performance” symposium, held on February 29th 2024, co-organized by Ascencia Center for Applied Business & Management Research (CABMR - France) and Gisma University for Applied Sciences (Germany), in collaboration with the Association for University Business & Economic Research (AUBER, United States).

Hosting institution

Ascencia Business School, Collège de Paris, International Campus, Paris - La Défense.

Conflicts of interest

The authors have declared that no competing interests exist.

References

- Lopatova N (2021) Cybersecurity as a driver of business growth. Science and Innovations 3 (217): 38-41. https://doi.org/10.29235/1818-9857-2021-3-38-41
- Özsungur F (2021) Business Management and Strategy in Cybersecurity for Digital Transformation. Handbook of Research on Advancing Cybersecurity for Digital Transformation144-162. https://doi.org/10.4018/978-1-7998-6975-7.ch008
- Saeed S, Altamimi S, Alkayyal N, Alshehri E, Alabbad D (2023) Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. Sensors 23 (15). https://doi.org/10.3390/s23156666
- Sandhu K (2021) Advancing Cybersecurity for Digital Transformation. Handbook of Research on Advancing Cybersecurity for Digital Transformation1-17. https://doi.org/10.4018/978-1-7998-6975-7.ch001