Navigating the Intersection of Innovation and Cybersecurity: A Framework

Danielle Botha-Badenhorst
CSIR, Pretoria, South Africa

DBotha3@csir.co.za

Abstract: Reliance on digital technologies for innovation management is unavoidable in current contexts. While digital processes and business models have been prioritised as key factors to drive innovation and value creation within firms, cybersecurity concerns are still rife. Increased levels and severity of cybersecurity breaches (CSBs) have had adverse effects on trust, caused significant revenue losses, and inflicted reputational damage on many firms. Further exacerbating these concerns is an observation made in the Global Risks Report of 2022, the World Economic Forum: cybersecurity measures taken by businesses are becoming increasingly obsolete. Many firms face severe consequences without implementing strategic objectives to limit the threats posed by CSBs. Cybersecurity breaches (CSBs) have a significant long-term impact on firm-level innovation and investment decisions. However, many firms are reluctant to examine or enhance their existing cybersecurity practices because of concerns that they may limit their innovation ability. Determining a method to limit CSBs and retain capabilities to perform necessary innovative processes is a delicate balance, with trade-offs to be considered within each process. This paper aims to address the delicate balance between limiting CSBs and preserving the ability to undertake necessary innovative processes. Building upon the Cyber Security Maturity and Innovation matrix introduced by Nelson and Madnick (2017), this paper expands the framework by providing specific suggestions for each quadrant. The matrix classifies firms into different quadrants based on their reliance on innovation and their assessment of cyber risk. We then detail measures to improve cybersecurity maturity for firms in each quadrant, incorporating the National Institute of Standards and Technology (NIST) Cybersecurity Framework Version 1.1 (CSF) as a reference. By making well-informed decisions and implementing appropriate measures, firms can effectively mitigate CSB risks while continuing to drive innovation and create value. This expanded framework serves as a valuable tool for firms seeking to align their cybersecurity practices with their innovation objectives, in accordance with the NIST CSF.

Keywords: Cybersecurity, Innovation, Digital technologies, Risk management, Framework.

1. Background and Introduction

In recent years, reliance on digital technologies for innovation has become an essential part of business operations. Innovation and cybersecurity are critical components of modern business operations, and their intersectionality has become increasingly relevant in recent years. With increasing use of digital processes and business models, cybersecurity concerns have become a prevalent issue for many firms. Cybersecurity Breaches (CSBs), cybercrime, ransomware attacks and other cybersecurity incidents have been increasing in frequency. More than 83% of organisations included in IBM's Data Breach Report have experienced more than one data breach (IBM, 2022). The report also highlights that the severity of these attacks, as well as associated costs, can have significant financial impacts on the business; the increase in severity and cost of these incidents can mean that it can take months or even years for a business to recover from the impact of a breach.

Cybercrime and CSBs are expected to incur a 15% increase in the associated costs, reaching $10.5 trillion by 2025. Annual costs are expected to reach $8 per annum by the end of 2023 (Cybersecurity Ventures, 2022). The report further highlights the growing threat of cybercrime and the increasing sophistication of cybercrime. Further issues compounding these concerns are stated in the Global Risks Report of 2022, the World Economic Forum: Cybersecurity measures taken by businesses are becoming increasingly obsolete (World Economic Forum, 2022). CSBs can influence future strategic decisions involving firm-level investment and innovation decisions; CSBs have been linked to a 10% decline in Research and Development, as well as decreasing investment efficiency for up to four years following a breach (He et al., 2020). Most firms are ill-equipped to deal with a CSB; this is further exacerbated by CSB contagion effects where managerial ability and internal control deficits within a firm in the same industry may ripple through to others once a CSB has taken place (Kelton & Yang, 2023).

Despite the clear adverse implications of a CSB, many firms are hesitant to enhance their cybersecurity posture because of the fear of limiting their ability to innovate (Auyporn et al., 2020). In surveys reviewed by Madnick and Nelson, firms tended to indicate one of three viewpoints regarding the intersection of innovation and cybersecurity. Some firms indicate that stringent cybersecurity has a negative and limiting impact on innovation; some believe that efforts can be well-balanced; and finally, some respondents indicated that firms are taking too many cyber risks in the name of innovation. Given the significant financial and reputational risks associated

with CSBs, businesses must adopt a proactive approach to managing their cybersecurity risks, preferably one that balances the need for innovation and cybersecurity. A carefully considered approach must be followed on a per-firm basis to develop a framework that considers the cybersecurity maturity of a firm along with its innovation requirements.

The framework proposed in this paper builds upon the finding in Nelson and Madnicks's work, "Studying the Tension between Digital Innovation and Cybersecurity" (Nelson & Madnick, 2017) and integrates it with the National Institute for Standards and Technology (NIST) Cybersecurity Framework Version 1.1 (CSF) (National Institute of Standards and Technology, 2018).

Nelson and Madnick's work relies on survey responses conducted from December 2015 to January 2016. The survey consists over 54 diverse organisations. The participants' demographics were diverse across regions: 21 participants were from Asia/Pacific, 10 from Europe/Africa, 2 from Latin America, and 21 from North America. Various industries were surveyed, 16 in total. Organisations ranged in size from small (<1000 employees), medium (1,000-9,999 employees) and large (>10,000). To address the lack of common metrics that define cybersecurity maturity and technological innovations in companies, the survey questions were designed as proxies for these measures. Two survey techniques were employed to enhance accuracy. Firstly, the questions focused on executives' activities within the past 12 months to ensure responses were based on recent experiences rather than perceptions. Secondly, specific examples were provided for each question to make them more concrete and encompass a wide range of possibilities. Figure 1 provides an indication of the number of companies per quadrant, as determined by the surveys conducted by Nelson and Madnick.

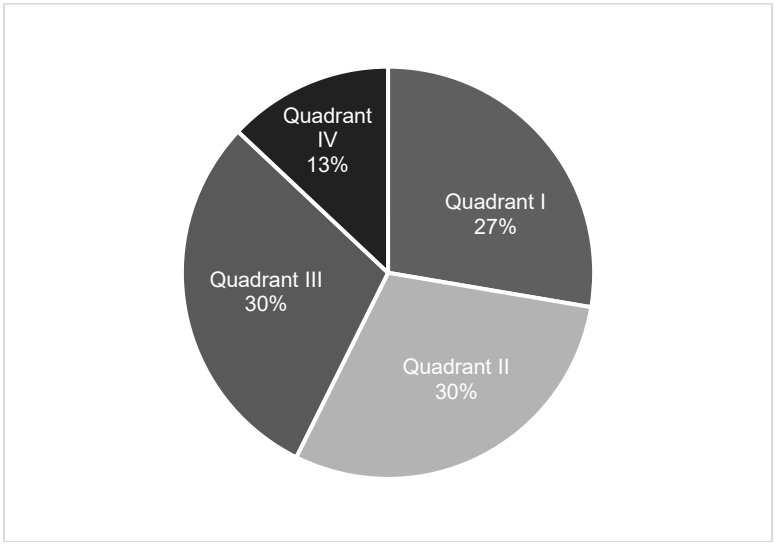

Figure 1 Proportion of companies per quadrant (Nelson & Madnick, 2017)

The paper is organised as follows: First, a brief background and introduction discuss the pertinence of developing a CSF that considers the intersectionality of innovation and cybersecurity. Next,
Both Madnick & Nelsons Innovation and Maturity matrix and the NIST CSF are detailed in Section **Error! Reference source not found.**. The CSF is detailed for each quadrant in Section 3. Section 4 discusses limitations and opportunities for future research4. Finally, Section 5 concludes the paper and discusses the implications and suggestions associated with the framework.

2. Framework introduction

Extending a framework to provide guidelines for firms according to their position on the Cybersecurity Maturity and Innovation matrix requires nuance and flexibility on a per-firm basis. This framework does not intend to be prescriptive per se, but provides a guideline that can be adapted according to the specific needs of the firm. The goal of the framework is to provide recommendations that can be implemented by firms depending on their identified quadrant, which can help mitigate the risks associated with CSBs.

ISO/IEC 27032:2012 defines *cybersecurity* as the preservation of confidentiality, integrity, and availability of information within complex environments, wherein people, services, and software interact on the Internet using technology devices and connected networks (ISO/IEC, 2012). Cybersecurity is often used interchangeably with other terminology in the field of security; it includes network security, information security, and Internet

security. Following the same approach as researchers (Azmi et al., 2018), this paper considers cybersecurity to mean "*securing a virtual digital environment by governance, management and assurance, including its assets (i.e. information assets and cyber assets), entities (such as end users, organizations, governments, societies, machines and software), and interactions (enabled by IT infrastructure, communications/networks, systems, and devices)".*

NIST CSF V1.0 is a voluntary framework that provides a set of guidelines and best practices or standards for improving cybersecurity risk management across various industries. This framework is a valuable resource for organisations seeking to improve their cybersecurity risk management processes and enhance their overall cybersecurity posture (Shen, 2014). The latest version, 2.0, is under review at the time of writing; thus, V1.1 CSF will be used in this paper. The NIST CSF has become the standard method of facilitating cybersecurity risk management within many organisations; The NIST CSF is popularly used as it emphasises organisation-specific recommendations within the framework (Gordon et al., 2020). NIST CSF includes five core functions: Identify, Protect, Detect, Respond and Recover.

The five core functions provided by the NIST CSF, when considered together, provide a comprehensive review of cyber risk management over its lifecycle. Each aspect represents a different element of risk management and can be broken down as follows (Mahn et al., 2023):

1. Identify: Developing an organisational understanding required to manage risk across relevant assets, data, and capabilities.
2. Protect: Developing and implementing appropriate safeguards to ensure the required service delivery.
3. Detect: Developing and implementing the appropriate activities required to identify occurrences of cybersecurity events.
4. Respond: Developing and implementing appropriate activities required to take action regarding detected cybersecurity events.
5. Recover: Developing and implementing appropriate activities required to restore any capabilities that have been impaired owing to the detected cybersecurity event, as well as maintaining plans for resilience.

Each core structure contains categories, subcategories, and informative resources. This is illustrated in Figure 2. The proposed framework focuses on the core functions and provides several categories. The highest level of organising basic cybersecurity activities was achieved through the functions described above. They help organisations manage cybersecurity risks by organising information, making risk-management decisions, addressing threats, and learning from previous activities. These functions also align with the existing incident management methodologies and demonstrate the impact of cybersecurity investments. Categories, however, are subdivisions of functions that group cybersecurity outcomes according to programmatic needs and specific activities. Examples of these categories include Asset Management, Identity Management and Access Control, and Detection Processes (National Institute of Standards and Technology, 2018).

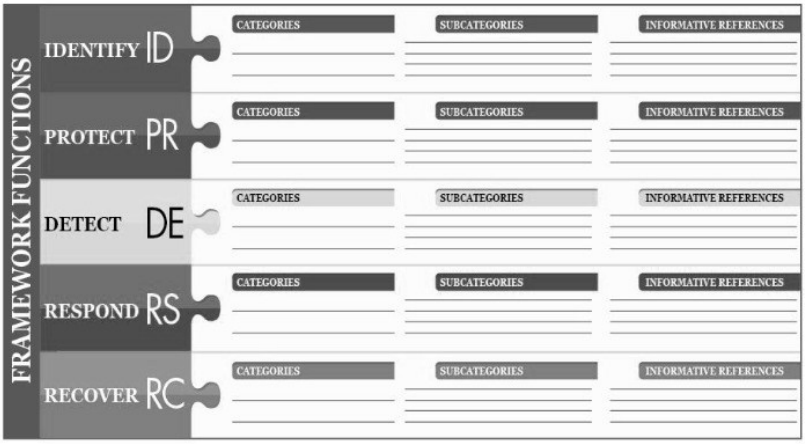

Figure 2 NIST CSF Framework Core Structure (National Institute of Standards and Technology, 2018)

The framework is intentionally broad and flexible. It provides a macro-overview of how cybersecurity risk management should be approached, while specific implementations and details must be determined by the firm

and its organisational requirements. The NIST CSF is also utilised in this study to provide recommendations in the context of Nelson and Madnick's Cybersecurity Maturity and Innovation matrix.

3. Proposed Framework

The proposed framework is divided into four categories: low innovation/low cybersecurity maturity (beginners), low innovation/high cybersecurity maturity (secure conservatives), high innovation/low cybersecurity maturity (reckless innovators), and high innovation/high cybersecurity maturity (secure digital innovators). This is illustrated in **Figure 3**.

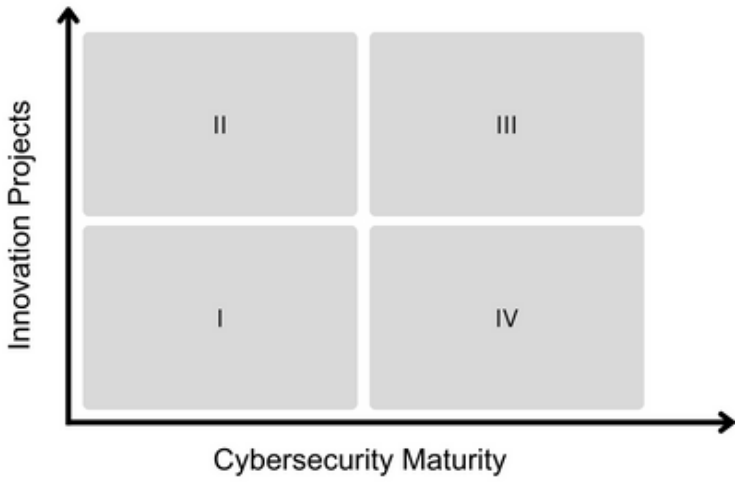

Figure 3 Cybersecurity Maturity and Innovation Matrix (Nelson & Madnick, 2017)

Quadrant I and IV firms would likely need to address all five core aspects of the NIST CSF, as discussed in sections 3.1 and 3.2. Recommendations for these quadrants describe the different approaches that both quadrants could follow. Quadrants II and III would likely have robust cybersecurity controls in place addressing the five core NIST CSF recommendations; however, each quadrant may have unique problems that may still need to be addressed. This is discussed in sections 3.3 and 3.4.

3.1 Quadrant I Firms

Quadrant firms are characterised by both low technology innovation and low cybersecurity maturity. Organisations in this quadrant are likely to have weaker cybersecurity controls in place, making them vulnerable to cyber threats, even if they have lower technological maturity. Firms with low technological innovation must still make use of various digitised processes; firms that use only basic utility technologies are increasingly scarce (Nelson & Madnick, 2017).

Many firms within this quadrant identify themselves as start-up firms. For start-up firms, it is essential to implement the necessary cybersecurity controls from the start. Startup firms working towards becoming a fully-fledged business often make similar cybersecurity mistakes that can result in costly CSBs (Starikova, 2022). Further, nascent firms face unique problems that are often easily overcome by their larger, more mature counterparts (Chandna & Tiwari, 2023).

The first step that firms within this quadrant must take is the implementation of robust, basic cybersecurity controls to protect digital and physical assets. Using NIST CSF, it is recommended that firms in this quadrant implement basic cybersecurity controls based on their specific risks and requirements. This can involve setting up security controls such as antivirus software, firewalls, and Intrusion Detection Systems (IDSs).

As the cybersecurity maturity for these firms is low, each of the NIST CSF's five core functions must be addressed (Mahn et al., 2023):

1. Identify classifying assets that need to be protected. This can include critical enterprise processes and assets, document information flows, maintaining hardware or software inventories, and establishing policies with relevant roles and responsibilities.
2. Protect: Implementing access control and firewalls to protect sensitive data, managing access to assets and information, and conducting regular backups.

3. Detect: Monitoring networks for potential security threats and testing or updating detection processes within the network.
4. Respond: Implement an incident response plan, which should include a procedure for detecting, containing, and responding to an incident. The plan must be updated and plans must be tested.
5. Recover: Develop a business continuity plan detailing steps to recover from an incident that may occur in a timely manner. Communication between internal and external stakeholders must be clearly defined.

Care must be taken during the response and recovery phases. Firms in this quadrant might struggle significantly more than others to recover from a cybersecurity incident, particularly if these measures have not been implemented.

When considering the risk-based approach recommended by NIST, ongoing assessments and continuous improvement of system implementation should be prioritised by firms within this quadrant. Additionally, organisations within this quadrant should consider awareness training, focusing on basic cybersecurity best practices. It is recommended that the training offered is appropriate for the target audience while still reaching the largest audience possible, while maintaining a favourable cost/performance ratio to ensure long-term sustainability (Gkioulos & Chowdhury, 2021). Essential skills and knowledge within this quadrant may include social engineering knowledge (protecting information from phishing, spoofing, ransomware, etc.) to mitigate financial losses, identity theft, and reputational damage. Various free or low-cost awareness training solutions are available (National Institute of Standards and Technology, 2020), which is a particular advantage for start-up firms.

3.2 Quadrant II Firms

Quadrant two firms are characterised by high technological innovation but low cybersecurity maturity. These firms may be highly innovative, but their cybersecurity posture may not be sufficiently mature to protect their assets. Such firms are particularly vulnerable to a wide range of cybersecurity threats.

Companies within this quadrant vary in size and comprise the smallest section of firms analysed by Nelson and Madnick (2017).

Nelson and Madnick indicate that firms within this quadrant may implicitly accept higher levels of risk and are prepared to deal with the consequences of a potential CSB. Another possibility is that companies may not fully understand the risks they accept. A study performed by Gartner researched the effectiveness of chief information security officers (CISOs) across four categories. Only 12% of the surveyed CISOs were deemed highly effective across all the categories. Gartner further indicated that only 66% of these top-performing CISOs collaborate with senior business decision-makers to accurately define the organisation's risk appetite (Gartner, 2020). If business decision-makers are unaware of acceptable risk levels, this may further exacerbate implicit, unwanted risk acceptance.

Like quadrant one firms, all aspects of the NIST CSF should be considered and implemented to improve the cybersecurity posture, as discussed below:

1. Identify classifying assets that need to be protected. This can include critical enterprise processes and assets, document information flows, maintaining hardware or software inventories, and establishing policies with relevant roles and responsibilities. A thorough risk assessment is required to identify vulnerabilities related to innovative technologies.
2. Protect: Implementing access control such as multi-factor authentication and firewalls to protect sensitive data, manage access to assets and information, and conduct regular backups.
3. Detect: Monitoring networks for potential security threats and testing or updating detection processes within the network. Implementing an intrusion detection and prevention system (IDPS) to monitor network traffic or security information and event management (SIEM) to centralise log monitoring and analysis.
4. Respond: Implement an incident response plan, which should include a procedure for detecting, containing, and responding to an incident. The plan must be updated and plans must be tested. Tabletops or simulated exercises can be performed to verify the efficacy of the response plan.
5. Recover: Develop a business continuity plan detailing steps to recover from an incident that may occur in a timely manner. Communication between internal and external stakeholders must be clearly defined.

Firms likely find themselves within this quadrant because of the friction between cybersecurity and innovation. A global survey found that various organisations may know how to improve their security position but choose to forgo the adoption of new applications or technologies to speed up core business processes (Ponemon Institute, 2016). Respondents indicated that while most organisations recognise the importance of adequate cybersecurity controls, access management and governance processes to support these digitisation practices are not yet in place.

3.3 Quadrant III Firms

Quadrant three firms are characterised by low technological innovation and high cybersecurity maturity. This quadrant comprises the lowest number of firms surveyed by Madnick and Nelson. Some of these firms either find themselves in an industry with less competitive pressure or where an intentional "slow follower" strategy is adopted. This method is employed especially in industries where the appetite is very low, such as nuclear power plants.

Some firms within the "slow follower" category were industrial firms. A study performed by Honeywell indicated that many organisations within this sector still have a long way to go regarding the adoption of current cybersecurity technologies. The majority of the surveyed firms only had a firewall between the plant and business systems. Less than a third of the respondents did not have proper access control or authentication methods implemented across their systems (Honeywell, 2017). The report stressed that many companies within these industries self-reported their cybersecurity posture to be higher than it may be in reality.

Although these firms may take the necessary precautions and have a well-rounded cybersecurity posture, cyber threats evolve faster than they can be assessed (Kettani & Wainwright, 2019). Adopting a slow follower approach may not be the correct approach in the current cybersecurity landscape. Organisations within quadrant two should focus on the continuous improvement of their cybersecurity posture. This could include adopting increasingly automated threat analysis and response. Artificial intelligence and machine learning technologies are essential for providing dynamic, automated, and up-to-date analytics by utilising data analysis. This can be leveraged to address the insufficient response of many traditional security systems when faced with the rapid proliferation of new cyber risks (Sarker, 2022).

In enterprise risk management, internal audits or user training can address issues of complacency regarding cybersecurity policies. Some technology users within a firm may deem themselves vulnerable to exploits or cyber risks, or engage in workarounds to side-step formal cybersecurity policies (Stafford et al., 2018). Considering the increased speed at which cyberthreats evolve, the two quadrants should focus on both the identity and protection functions of the NIST CSF.

3.4 Quadrant IV Firms

Quadrant three firms are characterised by both high technology innovation and cybersecurity maturity, consisting mostly of medium and large firms (Nelson & Madnick, 2017). In the surveys conducted, the firms noted the necessity of cyber-risk mitigation while building digital capacity and capabilities.

Medium-to-large firms are likely to have the correct procedures in place to respond to these threats when compared to small firms. Most large companies already have response plans in place; 81% of firms with more than $1 billion in revenue have a cybersecurity program in place, with a response plan forming part thereof (Sloan, 2020).

To improve the firm's capability to perform core functions (Identify), continuous improvement should be prioritised (Mahn et al., 2023). Learning goals and objectives for the cyber team or organisation should be defined and aligned with organisational needs and goals. Regular audits and gap assessments should be performed on both processes, as well as within the cyber team or organisation (Acartürk et al., 2021).

4. Discussion

Examining Nelson and Madnick's quantification of the tension between digital innovation and cybersecurity through the lens of the NIST CSF provides recommendations for improving the cybersecurity posture of various firms. A primary limitation of this framework is the assumption that firms are able to correctly determine their cybersecurity posture. Many firms struggle to accurately define their posture, often overestimating the effectiveness of cybersecurity solutions. Substantial investments in cybersecurity technology and a high level of

awareness among senior executives have led to the exploitation of vulnerabilities and CSBs. This is largely because of the fundamental intricacies of cybersecurity, and the rigorous steps required to achieve this are underestimated. Cybersecurity practices can devolve into an exercise of ticking specific boxes rather than building the strategic capabilities needed to have true cyber resilience (Ford & Ali, 2020).

This study does not aim to be prescriptive, but to provide some insight into the actions that could be taken by firms within different quadrants of Nelson and Madnick's work. It is essential for firms to determine their cybersecurity posture accurately. Various tools are available to assist in the assessment and auditing of an organisation's cyber posture. Some of these tools, such as *the Axio Cybersecurity Program Assessment Tool*, are available free of charge. Other tools, such as the Information Systems Audit and Control Association's *Implementation of the NIST Cybersecurity Framework and Supplementary Toolkit* or SACA's *Cybersecurity: Based on the NIST Cybersecurity Framework,* provide best practices for security audits, compliance, and communication (National Institute of Standards and Technology, 2022).

5. Conclusion

The intersection of cybersecurity and digital innovation has become increasingly relevant in recent years, and digital technologies play a crucial role in business operations (Nelson & Madnick, 2017). The rising adoption and use of digitised business models has brought about cybersecurity concerns as the prevalence, severity, and frequency of CSBs have increased. These incidents not only result in financial losses but may also impact a firm's ability to innovate or make strategic decisions in the years following a severe CSB.

Despite the clear risk associated with CSBs, many firms are hesitant to enhance their cybersecurity posture because of fear of limiting their innovation capabilities. However, it is crucial for firms to try to find a balance between these two concepts. Nelson and Madnick indicate that only 13% of companies surveyed believe that the have struck the correct balance between cybersecurity maturity and innovation.

This paper proposes a framework that integrates the Cybersecurity Maturity and Innovation matrix proposed by Nelson and Madnick with the National Institute of Standards and Technology (NIST) Cybersecurity Framework. The framework provides guidelines for firms based on their position in the matrix and recommends specific cybersecurity measures to mitigate the risks associated with breaches. Firms placed within quadrants I and II are in a precarious position with low cybersecurity maturity. These firms are likely to need to address all aspects of the NIST Cybersecurity Framework to improve their cybersecurity posture. Quadrant III and IV firms, with higher cybersecurity maturity, should continue to maintain a well-rounded cybersecurity posture and stay updated with evolving threats.

Both this paper and the work done by Nelson and Madnick assume that companies can correctly ascertain their cybersecurity posture. An area where further research is required is the proliferation and development of accurate cybersecurity posture assessments. Although many tools are available, most firms still struggle to accurately determine their posture. A Bain & Company survey indicates that only 43% of executives believe that their firms follow cybersecurity best practices. A deeper analysis indicated that only 24% of these firms met the bar, indicating that numerous executives or companies believe they have a better cybersecurity posture than they truly do (Ford & Ali, 2020).

In practice, various factors might affect the quadrant in which a firm is placed. This can include technology management practices (such as organisational structure or legacy architectures) or industry-related factors (such as regulatory environments or innovation pressures). The proposed framework is adaptable and allows firms to tailor their cybersecurity measures based on their specific needs. This emphasises the importance of ongoing assessments, continuous improvement, and employee awareness training.

References

Acartürk, C., Ulubay, M., & Erdur, E. (2021). Continuous improvement on maturity and capability of Security Operation Centres. *IET Information Security*, *15*(1). https://doi.org/10.1049/ise2.12005

Auyporn, W., Piromsopa, K., & Chaiyawat, T. (2020). Critical factors in cybersecurity for SMEs in technological innovation era. *ISPIM Conference Proceedings*, *March*.

Azmi, R., Tibben, W., & Win, K. T. (2018). Review of cybersecurity frameworks: context and shared concepts. *Journal of Cyber Policy*, *3*(2), 258–283. https://doi.org/10.1080/23738871.2018.1520271

Chandna, V., & Tiwari, P. (2023). Cybersecurity and the new firm: surviving online threats. *Journal of Business Strategy*, *44*(1). https://doi.org/10.1108/JBS-08-2021-0146

Cybersecurity Ventures. (2022). *2022 Official Cybercrime Report*.

Ford, F., & Ali, S. (2020). *Most Companies Overestimate Their Cybersecurity, but Resilience Is Possible*. https://www.bain.com/insights/most-companies-overestimate-their-cybersecurity-but-resilience-is-possible/

Gartner. (2020). *Gartner 2020 CISO Effectiveness Survey*.

Gkioulos, V., & Chowdhury, N. (2021). Cyber security training for critical infrastructure protection: A literature review. In *Computer Science Review* (Vol. 40). https://doi.org/10.1016/j.cosrev.2021.100361

Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost-benefit analysis into the NIST cybersecurity framework via the Gordon-Loeb model. *Journal of Cybersecurity*, *6*(1). https://doi.org/10.1093/CYBSEC/TYAA005

He, C. Z., Frost, T., & Pinsker, R. E. (2020). The impact of reported cybersecurity breaches on firm innovation. *Journal of Information Systems*, *34*(2). https://doi.org/10.2308/isys-18-053

Honeywell. (2017). *Overcoming the Industrial Cyber Security Skills Gap Facing the Process Industries*.

IBM. (2022). *Cost of a Data Breach Report*.

ISO/IEC. (2012). ISO 27032 Information technology - Security techniques - Guidelines for cybersecurity. *International Organization for Standardization*.

Kelton, A., & Yang, Y.-W. (2023). *Understanding cybersecurity breach contagion effects: The role of the loss heuristic, managerial ability, and internal controls*. https://ssrn.com/abstract=4379322

Kettani, H., & Wainwright, P. (2019). On the top threats to cyber systems. *2019 IEEE 2nd International Conference on Information and Computer Technologies, ICICT 2019*. https://doi.org/10.1109/INFOCT.2019.8711324

Mahn, A., Marron, J., Quinn, S., & Topper, D. (2023, January 23). *Quick Start Guide*. NIST Special Publication 1271. https://www.nist.gov/cyberframework/getting-started/quick-start-guide

National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. https://doi.org/10.6028/NIST.CSWP.04162018

National Institute of Standards and Technology. (2020, April 7). *Free and Low Cost Online Cybersecurity Learning Content*. NICE Program Office. https://www.nist.gov/itl/applied-cybersecurity/nice/resources/online-learning-content

National Institute of Standards and Technology. (2022, October 7). *Assessment & Auditing Resources*. National Institute of Standards and Technology Cybersecurity Framework. https://www.nist.gov/cyberframework/assessment-auditing-resources

Nelson, N., & Madnick, S. (2017). Studying the tension between digital innovation and cybersecurity. *AMCIS 2017 - America's Conference on Information Systems: A Tradition of Innovation*, *2017-August*.

Ponemon Institute. (2016). *Global Trends in Identity Governance & Access Management*.

Sarker, I. H. (2022). Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects. In *Annals of Data Science*. https://doi.org/10.1007/s40745-022-00444-2

Shen, L. (2014). The NIST Cybersecurity Framework Overview and Potential Impacts. In *The SciTech Lawyer* (Vol. 10, Issue 4).

Sloan, R. (2020, June 21). *Which Industries Aren't Ready for a Cyberattack?* The Wall Street Journal. https://www.wsj.com/articles/the-industries-most-vulnerable-to-cyberattacksand-why-11592786160

Stafford, T., Deitz, G., & Li, Y. (2018). The role of internal audit and user training in information security policy compliance. *Managerial Auditing Journal*, *33*(4). https://doi.org/10.1108/MAJ-07-2017-1596

Starikova, A. (2022, February 9). *Typical startup cybersecurity mistakes*. Kaspersky Daily. https://www.kaspersky.com/blog/startup-cybersecurity-mistakes/43559/

World Economic Forum. (2022). *The Global Risks Report 2022*. World Economic Forum.