Proceedings of the 6th International Conference on Computing and Data Science
DOI: 10.54254/2755-2721/71/20241658

Review on the application of data security in the enterprise management

Shiyou Nie

STEM college, University of South Australia, Adelaide, 5000, Australia

nsyleaist713@gmail.com

Abstract. In recent decades, cybersecurity has become a crucial topic in business management, centred around the three core elements of Confidentiality, Integrity, and Availability (C.I.A.) of information technology. Cybersecurity aims to protect IT systems and networks from cyberattacks, with data as the primary focus. In business management, strategies for addressing potential threats vary depending on the size and type of business. This writing explores the preferences for implementing cybersecurity strategies in business management and trends in the development of data security mitigation. It analyses the mitigation strategies adopted by different enterprises, identifies patterns between data security strategies and enterprise attributes, and examines the preferences and constraints faced by enterprises in developing cybersecurity programs. The study highlights trends in the implementation of data security strategies, emphasizes the importance of cybersecurity, and provides insights into future trends in digital security within enterprise management and development. It also addresses the challenges faced by businesses, particularly small and medium-sized enterprises, in implementing effective cybersecurity measures due to limited resources.

Keywords: Enterprise management, cybersecurity, data security, information security, information technology.

1. Introduction

Recently, the proliferation of digital technologies has changed the way businesses operate, making cybersecurity a critical component of enterprise management. Increasing cyber threats have underscored the demand for robust security tactics to secure sensitive information, maintain functional integrity, and ensure the availability of IT systems or services. The triad of C.I.A. forms the cornerstone of effective cybersecurity strategies [1].

As businesses become increasingly reliant on digital infrastructures, the risk of cyberattacks has grown, posing a significant threat to data security and overall business operations [2]. Cybersecurity is no longer a technical issue but a strategic imperative affecting all organisation levels. Protecting IT systems and networks from cyber threats is critical for safeguarding data and maintaining business reputations and financial stability [3].

Approaches to cybersecurity comprehensively vary among enterprises, differing by considerations such as scale, industry, and specific business requirements. Smaller businesses might focus on basic protective measures, while larger ones often implement comprehensive, multi-layered security measures.

DOI: 10.54254/2755-2721/71/20241658

It is crucial to understand these differences for developing customised cyber security solutions that effectively resolve the scenario-based challenges faced by diverse types of businesses [4].

The purpose of the review is to explore the preferences of business management in implementing cybersecurity strategies and to identify trends in data security mitigation measures by analysing the strategies adopted by different enterprises. The study attempts to reveal correlations between data security strategies and enterprise attributes. It also explores the constraints and preferences encountered by enterprises in developing security plans.

2. Literature Review

2.1. Concept of data security

Data security, which is referred to as information security, covers the practices and techniques that protect digital information from unauthorised access, destruction, or theft throughout its lifecycle. The primary purposes of data security are consistent with the principles of confidentiality, integrity, and availability (C.I.A.) [1].

Confidentiality ensures that only authorised individuals can access information. Ensuring that it includes encryption, access control, and authentication mechanisms [5]. Integrity consists of maintaining the accuracy and completeness of data. Mitigation like hashing, checksum, and data validation secure that data remain unchanged during transmission or storage unless properly authorised [5]. Availability Assures that authorised users can access resources when necessary. This has included implementing redundant systems, regular backups, and disaster recovery plans to minimise data loss or access disruption.

2.2. Significance of data security

The importance of data security in modern business environments should be considered as enterprises become more reliant on digital information, and cyber threats become increasingly sophisticated. In enterprise management, data security includes protecting sensitive information, maintaining business continuity, and regulating compliance and preventing economic loss and assuring the reputation and customer's trust.

Data security is critical to protecting sensitive information such as customer privacy, financial records, and intellectual property. Data breaches involving sensitive information can lead to profound consequences, including identity theft, credit card fraud and legal consequences [3]. Effective data security measures are also essential to maintain business continuity. Cyberattacks, such as ransomware can disrupt business operations and result in significant financial and reputational damage. Safeguarding data availability enables enterprises to minimise the chances of any unexpected downtime and maintain the efficiency of business operations and processes even when facing cyber incidents [6].

Businesses must comply with various data protection regulations and standards, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Ac (HIPAA). Noncompliance can lead to significant fines and legal ramifications. Implementing robust data safeguard practices provides organisations with aid in meeting those regulatory requirements and avoiding penalties [5].

Additionally, data breaches can lead to vital financial losses. It is not only in terms of immediate theft but also in spending on breach response, remediation, and lawsuits. According to research by Gordon in 2011, it has been shown that while companies invest in preventative data security measures, the costs are shifted downwards [2]. Business reputation and customer trust are directly affected by data security. High-profile data breaches can damage a brand long-term by eroding customers' trust and loyalty. In contrast, reliable data security strategies can increase customer confidence and differentiate an enterprise in a competitive market [7].

DOI: 10.54254/2755-2721/71/20241658

3. Research & Analysis

3.1. Results

Data security continues to be a vital concern for Australian Businesses, with the level of implementation and sophistication varying depending on the scale and type of the business. Table 1 and Figure 1 present the latest statistics on the adoption of specific data security strategies by Australian enterprises by the size of the organisation. Table 2 and Figure 2 are presented by the business sector, are sourced from authoritative research and reports.

Table 1. Adoption Rates of Data Security Measures by Business Size [8]

Security Strategy	Large Businesses (%)	Medium-Sized Businesses (%)	Small Businesses (%)
Multi-Factor Authentication (MFA)	85%	65%	50%
Data Encryption	75%	75%	N/A
Regular Security Audits	70%	N/A	40%
Firewall Usage	97%	88%	75%
Anti-Malware Software	92%	78%	65%
Employee Training	68%	55%	35%
Incident Response Plans	88%	N/A	55%
Data Backup and Recovery	N/A	78%	N/A
Access Controls	92%	N/A	60%

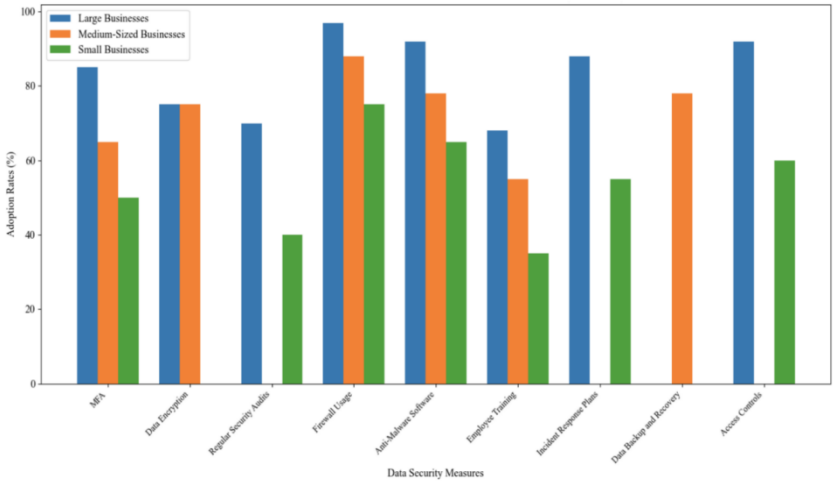

Figure 1. Adoption Rates of Key Data Security Measures by Business Size (2022-2023) [8]

Table 2. Adoption Rates of Data Security Measures by Business Sector [9]

Security Strategy	Financial Services (%)	Retail (%)	Healthcare (%)	Manufacturing (%)	Public Sector (%)
Security Information and Event Management (SIEM)	65%	65%	50%	N/A	N/A
Cloud Security	N/A	N/A	60%	40%	N/A
Zero Trust Architecture	N/A	N/A	N/A	N/A	25%

DOI: 10.54254/2755-2721/71/20241658

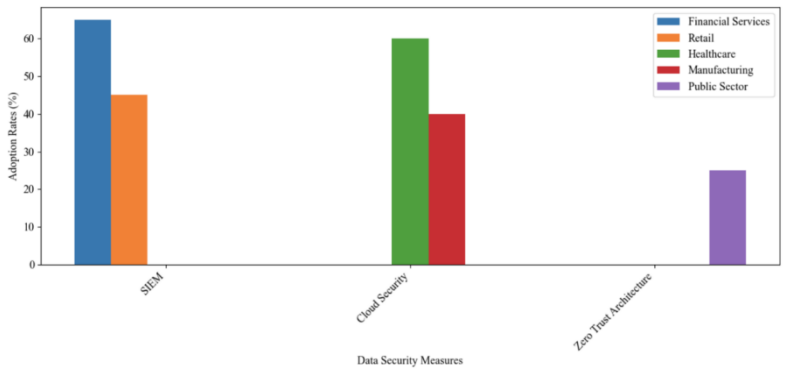

Figure 2. Adoption Rates of Key Data Security Measures by Business Sector (2022-2023)

3.2. Analysis

Based on the statistical data, multi-factor authentication (MFA), firewall, Anti-Malware software, and Employee training are commonly adopted by businesses in all scales.

Multi-factor authentication is becoming increasingly common in today's organisations of all sizes. MFA is an important security approach that reduces the risk of unauthorised access by requiring multiple forms of authentication. According to a 2023 report by the Australian Cyber Security Centre (ACSC), 85% of large enterprises, 65% of medium-sized enterprises, and 50% of small enterprises have implemented MFA [8]. Firewall is a basic defence mechanism that prevents unauthorised access and monitors incoming and outgoing network traffic. According to the Australian Cyber Security Centre, 97% of large businesses, 88% of medium-sized businesses and 75 % of small businesses use firewalls to protect their networks [8]. Anti-Malware software is essential for detecting and removing malware that could compromise data integrity and security. The Australian Cyber Security Centre reports that 92% of large businesses, 78% of medium-sized businesses, and 65% of small businesses use anti-malware software to protect against malware attacks [8]. Employee cybersecurity training is critical to reducing human risk. Training programs teach employees best practices and help prevent security breaches caused by human error. According to the Australian Cyber Security Centre, 68% of large businesses, 55% of medium-sized businesses, and 35% of small businesses conduct regular cybersecurity training for their employees [8].

SIEM solutions help organizations detect, monitor, and respond to security threats in real-time by analysing security events from a variety of sources. Deloitte Australia's Cybersecurity Report 2023 provides insight into the use of SIEM solutions. The report shows that 65% of financial services companies use SIEM solutions, compared to 45% in retail [9].

Cloud security ensures that data stored in a cloud environment is protected from corruption and unauthorized access. Cloud security measures are becoming increasingly important as organizations migrate to cloud environments. Deloitte reports that 60% of healthcare organizations have adopted cloud security measures, compared to 40% in manufacturing [9].

Zero-trust architectures recognize that threats can exist inside and outside the network and require continuous authentication of user access. The concept of zero-trust architecture is gaining traction, especially among technology companies. Deloitte also reports that 50% of technology companies have begun to implement zero-trust architectures, compared to 25% in the public sector by 2023 [9].

The data indicates a clear trend that larger enterprises are more likely to adopt comprehensive, advanced data security tactics than smaller ones. Businesses of all sizes commonly prioritise firewalls, anti-malware, and employee training. However, there are evident differences in the implementation of incident response plans and access controls, which might be caused by data loss or uncovering, considering partial data is in NA value. It can be speculated that small size businesses may concentrate more budget on developing marking and resources since they are less likely to be potential targets of cyber-attacks, but due to public awareness of cyber threat increase, a proportion of smaller-size

DOI: 10.54254/2755-2721/71/20241658

businesses are still willing to adopt minimum effort on the security strategy. Industry-specific adoption patterns also address resources in sectors such as financial services, healthcare, and manufacturing. The emerging trend of zero-trust architecture for technology companies suggests businesses are shifting to more proactive and comprehensive strategies in cybersecurity. In conclusion, the analysis underscores the importance of tailoring strategies to the specific needs and capabilities of varied sizes and industries.

4. Challenge

As speculation based on the former section, SMEs might need more financial and human resources, which are necessary to implement advanced and efficient cyber security measures, compared to large enterprises with comprehensive funding supporting information security infrastructures, and this may lead to higher vulnerability to cyber threats. There is also a huge gap between security awareness and training. While large organisations may be able to afford to train their staff regularly on cybersecurity practices, SMEs often neglect or spend minimum budgets on this critical aspect due to limited resources or lacking proficiency in CS. The continuous evolution of cyber threats poses a challenge to businesses of all sizes, and keeping track of the latest vulnerabilities and threats and developing mitigation strategies accordingly requires constant investment in cyber security technologies and expertise. In addition, maintaining compliance with various and often complicated data protection regulations, such as GDPR and HIPAA, can be especially challenging for new-started businesses. Failure to comply could result in severe financial fines and reputation damage.

Another challenge in data security of enterprise management is integrating innovative technologies with existing IT infrastructure, especially for legacy systems which may not be compatible with modern security solutions. Developing and maintaining an effective incident response plan is critical, but also extremely challenging, especially for SMEs that may not have dedicated cybersecurity staff [10]. Without proper planning and resources, ensuring a timely and effective response to security incidents can be difficult. This highlights the critical importance of a strong cybersecurity strategy in protecting the confidentiality, integrity, and availability (C.I.A.) of an organisation's information technology. As organisations become increasingly reliant on digital infrastructure and the risk of cyber-attacks continues to grow, cyber security has become an imperative.

5. Conclusion

Key findings highlighted by the study suggest differences in the adoption of cybersecurity measures between large enterprises and SMEs, with larger organisations tending to adopt a more comprehensive security strategy that includes multi-factor authentication, regular security audits and strict access controls. Industry-specific trends show that the adoption of advanced security solutions, such as SIEM and cloud security measures, varies widely across industries, with higher implementation rates in financial services and healthcare than in other industries. The trend towards zero-trust architectures shows a growing recognition of the need for ongoing authentication and verification to protect against internal and external threats.

Recommendations include raising awareness and training for all business sizes, especially SMEs, as regular training programmes can significantly reduce human factor-related security breaches. SMEs should invest in scalable cybersecurity solutions, such as cost-effective cloud security services and outsourced security operations centres (SOCs), which can evolve as the business grows. Enhancing compliance is also vital, as businesses should prioritise compliance with data protection regulations to avoid legal consequences and build customer trust. Incident response capabilities can be improved by developing and regularly updating incident response plans and conducting regular drills and simulations to ensure readiness for actual security incidents. Finally, it is important to leverage technology integration by seamlessly integrating new cybersecurity technologies with existing IT infrastructure, which may include updating legacy systems or adopting middleware solutions that promote compatibility. By addressing these challenges and adopting the recommended strategies, organisations can strengthen their cybersecurity posture and remain resilient in the face of emerging threats.

DOI: 10.54254/2755-2721/71/20241658

References

[1] Whitman, M. E., & Mattord, H. J. (2017). Principles of information security (6th ed.). Cengage Learning.

[2] Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? Journal of Computer Security, 19(1), 33–56. https://doi.org/10.3233/jcs-2009-0398

[3] Kaspersky Lab. (2020). The state of industrial cybersecurity 2020. https://ics-cert.kaspersky.com/publications/reports/2020/09/15/the-state-of-industrial-cybersecurity-2020/

[4] PwC. (2021). Global digital trust insights 2021. https://www.pwc.com/gx/en/services/consulting/cybersecurity.html

[5] Stallings, W., & Brown, L. (2018). Computer security: Principles and practice (4th ed.). Pearson.

[6] Symantec. (2019). Internet security threat report. https://docs.broadcom.com/doc/istr-24-executive-summary-en

[7] Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. International Journal of Electronic Commerce, 9(1), 70–104. https://doi.org/10.1080/10864415.2004.11044320

[8] 2022-2023 CYBER THREAT TRENDS FOR AUSTRALIAN BUSINESSES AND ORGANISATIONS. (2023). Australian Cyber Security Centre. https://www.cyber.gov.au/sites/default/files/2023-11/actr-2022-23-fact-sheets-businesses-organisations-2112023.pdf

[9] Deloitte Australia. (2023). Building long-term value by putting cyber at the heart of the business 2023 Global Future of Cyber Survey. https://www.deloitte.com/content/dam/assets-zone1/au/en/docs/services/risk-advisory/2023/deloitte-au-risk-2023-global-future-of-cyber-010223.pdf

[10] Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations. IEEE Access, 10, 85701–85719. https://doi.org/10.1109/access.2022.3197899