WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Assessing Costs and Preventative Strategies of Cloud Security Breaches on the U.S. Financial Services Sector

Obasuyi T Oghogho[1]*, Timilehin D Akano[2], Emmanuella O Erhabor[3], Steven C Ezeadi[4] and Bamidele T Akinyemi[5]

Department of Computing, East Tennessee State University, USA

ABSTRACT

Cloud security breaches represent a significant and growing threat to the U.S. financial sector, exposing institutions to financial losses, reputational damage, and regulatory penalties. Therefore, this study examined the costs and preventative strategies of cloud security breaches on the U.S. financial services sector, of which three specific research objectives were generated. This study employs a qualitative research approach with a case study design. It involves thematic analysis of three publicly available case study documents on financial institutions that have experienced cloud security breaches in the past decade. Additionally, interviews were conducted with two cybersecurity experts and one financial compliance officer, each with a minimum of five years of experience in the U.S. financial sector, selected through purposive sampling. The study found that vulnerabilities such as misconfigurations, compromised credentials, and weak third-party integrations are common entry points for attackers. While existing preventative measures have laid a solid foundation, they are often reactive rather than proactive, necessitating continuous investment in adaptive security technologies, comprehensive vendor oversight, and dynamic regulatory strategies to mitigate evolving risks effectively. The study recommended that financial institutions should continuously update and harden cloud configurations, implement real-time monitoring, and integrate advanced threat intelligence systems to quickly detect and respond to evolving cyber threats.

Keywords: *Cloud Security Breach, Financial Institutions, Cybersecurity, Case Studies, Compliance Regulations*

Introduction

Financial institutions are increasingly turning to cloud computing to enhance operational efficiency, reduce costs, and drive innovation. This is because, as asserted by Heng *et al.*, (2012), cloud computing enables banks and other financial entities to scale resources dynamically, improving service delivery while minimizing capital expenditure. The ability to access and analyze vast amounts of data in real time allows financial institutions to refine risk assessment, enhance customer experience, and streamline operations. As a result, cloud adoption has become a crucial component of digital transformation strategies across the financial sector (Vinoth *et al.*, 2022). Despite the numerous advantages of cloud computing, its adoption introduces significant security risks. The migration of sensitive financial data to cloud-based infrastructures increases exposure to cyber threats such as data breaches, ransomware attacks, and unauthorized access. Therefore, potentially shooting up the overhead cost of companies.

The financial impact of cyberattacks on financial institutions has been rising sharply. According a research conducted by Felce, Vedral and Tennie (2021), cyberattacks have become more frequent and sophisticated, with financial institutions among the primary targets due to the high value of their digital assets. Wuermeling (2017) found that cybercrimes cost the German economy approximately €55 billion annually, with financial institutions bearing a significant portion of this burden. Also, a cyberattack on Mexican financial institutions in 2018 resulted in losses exceeding $15 million due to vulnerabilities in third-party software (Oxford Analytical, 2018). These figures highlight the growing financial risks associated with inadequate cybersecurity measures in cloud-based financial systems.

Cloud Security Frameworks

To mitigate cloud security risks, various frameworks have been developed, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework, ISO 27001, and SOC 2.

NIST Cybersecurity Framework (NIST CSF): The NIST Cybersecurity Framework (NIST CSF) was developed by the U.S. National Institute of Standards and Technology to provide a comprehensive approach to managing cybersecurity risks. It is widely adopted in the financial sector due to its flexibility and emphasis on risk-based security strategies. The framework is structured around five core functions: Identify, Protect, Detect, Respond, and Recover (Almuhammadi and Alsaleh, 2017). NIST CSF allows financial institutions to assess their current security posture and implement controls that align with their risk tolerance. A study, conducted by

Möller, (2023), comparing NIST CSF to other security frameworks found that it provides comprehensive protection but may require supplementation with additional compliance measures for cloud security.

ISO/IEC 27001: The ISO/IEC 27001 is an international standard for information security management systems (ISMS). According to Humphreys (2016)It provides a systematic approach to securing data through policies, procedures, and risk management strategies. The standard requires organizations to conduct risk assessments, implement security controls, and continuously improve their security posture (Malatji, 2023). One key advantage of ISO 27001 is its global recognition and comprehensive security controls. A comparison of security frameworks, analyzed by Disterer (2013) found that ISO 27001 remains the most widely adopted standard for cloud security governance due to its structured risk management approach . However, financial institutions often need to supplement it with additional cloud-specific security measures.

Service Organization Control 2 (SOC 2): SOC 2, developed by the American Institute of Certified Public Accountants (AICPA), focuses on securing cloud-based services. It evaluates an organization's security, availability, processing integrity, confidentiality, and privacy controls. Unlike ISO 27001, which is a certification, SOC 2 is an attestation that demonstrates a company's adherence to best practices in cloud security (Zheng, Zheng and Liu, 2015). SOC 2 is particularly relevant for financial institutions that rely on third-party cloud providers, as it ensures these vendors maintain robust security measures. However, a study on security frameworks found that SOC 2 provides less comprehensive coverage compared to ISO 27001 and NIST CSF, making it more suitable as a complementary framework rather than a standalone solution (Syafrizal, Selamat and Zakaria, 2020).

Compliance Regulations

Regulatory compliance requirements play a crucial role in ensuring that financial institutions maintain stringent security controls while operating in cloud environments. As cyber threats continue to evolve, compliance frameworks such as the General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), and Federal Financial Institutions Examination Council (FFIEC) guidelines establish legal and industry-specific standards to protect sensitive financial and customer data. These regulations not only impose security requirements but also carry significant legal and financial implications for non-compliance.

The General Data Protection Regulation (GDPR), implemented by the European Union, is one of the most comprehensive data protection regulations, affecting financial institutions that process the personal data of EU residents, regardless of their geographical location. GDPR mandates strict data protection principles, including lawful processing, data minimization, and enhanced security measures such as encryption and anonymization (Protection Regulation, 2018). Financial institutions using cloud services must ensure that cloud providers comply with GDPR requirements, particularly concerning data transfer, storage, and breach notification. A major criticism of GDPR is its one-size-fits-all approach, which can impose excessive compliance burdens on financial institutions with robust existing security protocols (Almeida Teixeira, Mira da Silva and Pereira, 2019). Furthermore, while GDPR introduces heavy fines for non-compliance, up to €20 million or 4% of annual global turnover, studies suggest that enforcement remains inconsistent, leading to disparities in adherence among different jurisdictions (Khan and Daena, 2023).

The Payment Card Industry Data Security Standard (PCI DSS) is a global security standard specifically designed to protect payment card data. According the P. C. Industry (2010), financial institutions and cloud service providers that handle credit card transactions must comply with PCI DSS requirements, which include network security controls, data encryption, access restrictions, and continuous monitoring. Seaman (2020) asserted that PCI DSS compliance reduces the risk of payment fraud and data breaches; however, critics argue that the framework is reactive rather than proactive, as it primarily focuses on maintaining compliance rather than fostering a culture of cybersecurity resilience (Bonner, O'Raw and Curran, 2011). Additionally, achieving and maintaining PCI DSS certification is resource-intensive, making compliance challenging for smaller financial institutions that lack the necessary budget for advanced security infrastructure (Gross, 2012).

The Federal Financial Institutions Examination Council (FFIEC) guidelines are a set of U.S. regulatory standards that establish cybersecurity expectations for financial institutions, particularly those operating in the cloud. Unlike GDPR and PCI DSS, which focus on data protection and payment security, the FFIEC guidelines emphasize risk management, third-party oversight, and incident response (FFIEC, 2014). Financial institutions must conduct due diligence when selecting cloud providers, ensuring they adhere to robust security practices, including multi-factor authentication and real-time threat detection. While the FFIEC guidelines provide financial institutions with flexibility in implementation, a notable challenge is that they are not legally binding, which may lead to inconsistent application across different institutions (Council, 2016). Additionally, as cloud technology evolves rapidly, the FFIEC's periodic updates may struggle to keep pace with emerging threats, potentially leaving financial institutions vulnerable to sophisticated cyberattacks.

Financial Sector and Data Breaches

Assessing the financial costs and preventive strategies for cloud security breaches is crucial to mitigating risks and ensuring the resilience of financial institutions. The financial consequences of a breach extend beyond immediate remediation costs, including lost revenue, legal fees, regulatory fines, and increased cybersecurity investment (Wang et al., 2019). However, the full extent of these costs remains difficult to quantify due to the lack of standardized cost estimation frameworks. Without accurate assessment models, financial institutions cannot effectively allocate resources to strengthen their cybersecurity infrastructure (Huang & Wang, 2020). While various security measures exist, their effectiveness varies, and institutions often face inefficiencies in current security strategies, leading to gaps in protection. Identifying the most cost-effective and resilient security solutions is essential for financial institutions to optimize their cloud security investments while maintaining compliance with regulatory mandates.

The economic impact of data breaches in the financial sector is substantial. For instance, the work of Huang and Wang (2021) analyzed the financial consequences of data breaches, and found that breached firms face increased loan spreads, higher collateral requirements, and additional contractual covenants from banks. Another analysis of economic losses from data breaches showed that firms experience both direct and indirect costs, including legal penalties, operational disruptions, and loss of customer trust. In addition, stock market reactions to breach announcements, as presented in the work of Lange and Burger (2017) reveal that financial institutions often suffer short-term declines in share value, further exacerbating the financial toll of inadequate cybersecurity measures. Cloud security breaches in financial institutions continue to pose significant threats, necessitating stringent security frameworks and regulatory compliance measures.

Statement of the Problem

Cloud security breaches represent a significant and growing threat to the U.S. financial sector, exposing institutions to financial losses, reputational damage, and regulatory penalties. As financial institutions increasingly rely on cloud computing to enhance operational efficiency and scalability, the risks associated with cloud vulnerabilities continue to escalate. Cybercriminals exploit weaknesses in cloud-based infrastructures, leading to data breaches that compromise sensitive financial information. These breaches not only disrupt financial services but also undermine consumer trust, leading to long-term reputational harm. Regulatory bodies, such as the Federal Financial Institutions Examination Council (FFIEC) and Payment Card Industry Data Security Standard (PCI DSS), impose strict compliance requirements, and failure to meet these standards can result in substantial legal consequences (Khan and Daena, 2023). Despite the critical nature of cloud security, financial institutions often struggle to implement effective preventive measures, leaving them susceptible to evolving cyber threats.

Existing research on cloud security breaches in the financial sector remains fragmented and insufficient in addressing the full scope of economic and strategic implications. Studies often focus on specific breach incidents or general cybersecurity trends, but few provide a comprehensive analysis of cost estimation models and security framework efficiencies (Ford *et al.*, 2021). Furthermore, while regulatory guidelines exist, they lack uniform enforcement, leading to inconsistencies in security practices across financial institutions (Di Giulio *et al.*, 2017). Research is needed to develop a standardized approach to cost assessment and strategic cybersecurity planning, enabling financial institutions to enhance their cloud security resilience effectively. This study aims to bridge these research gaps by examining the economic impact of cloud security breaches, evaluating cost and current preventive measures on the U.S. Financial Services Sector.

Research Objectives

The main aim of this study is to assess the costs and preventative strategies of cloud security breaches on the U.S. Financial Services Sector. Specifically the study was structured;

1. To analyze the financial impact of cloud security breaches in the U.S. financial sector.
2. To examine common attack vectors in U.S cloud-based financial systems.
3. To assess the effectiveness of existing preventative strategies.

Research Questions

1. What are the direct and indirect costs of cloud security breaches in the U.S financial institutions?
2. What are the most common attack vectors in U.S cloud-based financial systems?
3. How effective are current cloud security measures in mitigating risks?

Methodology

Research Design

This study adopts a qualitative research approach using a case study research design to explore the financial, reputational, and regulatory implications of cloud security breaches in the U.S. financial sector. The qualitative approach is appropriate as it allows for an in-depth examination of real-world security incidents, providing context-rich insights into the costs and preventive measures associated with cloud security breaches.

Population, Sampling and Sampling Techniques

The study focuses on financial institutions in the U.S that have experienced cloud security breaches within the last decade, including cybersecurity experts and regulatory professionals who have worked in financial institutions in the US. Purposive sampling technique was employed to select three case studies of financial institutions that have encountered notable cloud security breaches and made public including; Capital One Cloud Security Breach of 2019, Bank of America Vendor Breach Cloud Security breach of 2023 and Bayview Asset Management Cloud Security Breach of 2021. In addition, two cybersecurity specialists and one financial compliance officers that have worked in the U.S financial institution for more than a decade were purposively selected for this study.

Instrumentation

The primary instruments for data collection including case studies documents i.e. publicly available reports on three financial institutions cloud security breaches in the U.S. As well as a semi structured interviews conducted with the selected cybersecurity experts and financial compliance officers. The interview was structured in line with the research objectives i.e. What are the direct and indirect costs of cloud security breaches in the U.S financial institutions? What are the most common attack vectors in U.S cloud-based financial systems? How effective are current cloud security measures in mitigating risks?

Data Analysis Techniques

Thematic analysis approach was used to examine the qualitative data from the case studies document and the semi-structured interviews.

Results

Thematic Analysis

Three key themes including, Direct and Indirect Costs, Most Common Attack Vectors and Effectiveness of Current Measures were generated.

Case Studies Documents

Three US Financial Institutions documents that experienced cloud security breaches in the past decade made public were reviewed and the result is presented in Table 1:

Table 1: Organized Review of the Case Studies Documents

Financial Institutions	**Direct and Indirect Costs**	**Most Common Attack Vectors**	**Effectiveness of Current Measures**
Capital One Cloud Security Breach of 2019 (Sources; web.mit.edu)	**Direct Costs** - Regulatory fines totaling $80 million. - Incident response and remediation expenses. **Indirect Costs** - Reputational damage leading to potential customer attrition. - Increased regulatory scrutiny.	- Exploitation of a misconfigured web application firewall. - Unauthorized access to sensitive data stored in the cloud.	- The breach highlighted vulnerabilities in cloud security configurations. - Emphasized the need for continuous monitoring and proper implementation of security controls.
Bank of America Vendor Breach Cloud Security breach of 2023 (Source; metomic.io)	**Direct Costs** - Costs associated with notifying affected customers. - Legal fees and potential settlements. **Indirect Costs** - Reputational harm affecting customer trust. - Potential loss of business due to diminished confidence.	- Compromise of third-party vendor systems (NCB Management Services). - Exposure of sensitive customer information due to vendor vulnerabilities.	- Incident underscored the risks associated with third-party vendors. - Highlighted the necessity for stringent vendor management and oversight.

Bayview Asset Management Cloud Security Breach of 2021 (Source; wsj.com)	**Direct Costs** - $20 million settlement due to cybersecurity weaknesses. - Expenses related to enhancing cybersecurity programs. **Indirect Costs** - Reputational damage among clients and partners. - Increased regulatory oversight and mandatory independent assessments.	- Deficiencies in IT practices leading to vulnerabilities. - Potential exploitation of weak security protocols by attackers.	- The breach revealed significant gaps in existing security measures. - Led to mandated improvements and regular assessments to ensure compliance and security.

Participants Interview Response

Three experts including two cybersecurity experts and one financial compliance officer with at least 5 years of work experience participated in this study and the participants coded response were presented in Table 2:

Table 2: Organized Participants Coded Response

Participants	Direct and Indirect Costs	Most Common Attack Vectors	Effectiveness of Current Measures
Cybersecurity Expert 1	Direct costs include immediate incident response, remediation expenses, and regulatory fines. Indirect costs often involve reputational damage, customer attrition, and long-term business disruption.	Phishing schemes, misconfigured cloud storage, and exploited API vulnerabilities are the primary vectors. Credential theft remains a major factor.	Current measures establish a good baseline; however, they can lag behind sophisticated, targeted attacks. Continuous investment in adaptive security and threat intelligence is crucial.
Cybersecurity Expert 2	Beyond remediation and legal fees, direct costs cover technical recovery while indirect costs extend to lost revenue, prolonged operational downtime, and diminished trust.	Social engineering tactics, unauthorized access via compromised credentials, and weak configurations in cloud environments are prevalent attack paths.	Although many institutions deploy robust security frameworks, these measures sometimes prove reactive. Proactive monitoring and regular security updates are necessary to outpace emerging threats.
Financial Compliance Officer	Costs are not only financial, encompassing fines and increased regulatory scrutiny, but also reputational, affecting investor confidence and market position.	Data misconfigurations, vulnerabilities in third-party integrations, and supply chain risks serve as key attack vectors that expose sensitive financial data.	Security measures have improved, yet many remain reactive rather than anticipatory. Enhanced, integrated strategies that align with evolving regulatory standards are needed for better risk mitigation.

Discussion of Findings

Theme 1: Direct and Indirect Costs

The reviewed case studies documents of cloud security breaches in U.S. financial institutions reveal a complex mix of direct and indirect costs. For example, the Capital One breach in 2019 incurred immediate expenses such as incident response, remediation, and regulatory fines reportedly totaling around $80 million. As Cybersecurity Expert 1 explained, *"Direct costs include immediate incident response, remediation expenses, and regulatory fines. Indirect costs often involve reputational damage, customer attrition, and long-term business disruption*". Similarly, the Bayview Asset Management incident, which led to a $20 million settlement, further illustrates how technical recovery costs are compounded by prolonged operational downtime and lost revenue. Cyber Security Expert 2 asserted that, *"Beyond remediation and legal fees, direct costs cover technical recovery while indirect costs extend to lost revenue, prolonged operational downtime, and diminished trust"*. In addition to these quantifiable expenses, the broader impact on brand reputation and customer confidence can be even more damaging over time. A Financial Compliance Officer noted, "*Costs are not only financial, encompassing fines and increased regulatory scrutiny, but also reputational, affecting investor confidence and market position*". This perspective underscores that while

direct costs such as fines and remediation are immediately measurable, the indirect costs, like erosion of customer trust and long-term damage to market reputation, can significantly impede future business prospects.

Theme 2: Most Common Attack Vectors

Cloud-based financial systems in U.S. financial institutions face a range of common attack vectors, as evidenced by the case studies documents reviewed in this study. For example, the Capital One breach of 2019 demonstrated how misconfigured cloud security, specifically, a poorly configured web application firewall, can be exploited to gain unauthorized access. As Cybersecurity Expert 1 explained, *"Phishing schemes, misconfigured cloud storage, and exploited API vulnerabilities are the primary vectors. Credential theft remains a major factor"*. This example highlights that even well-resourced organizations can fall prey to basic configuration oversights, enabling attackers to leverage technical vulnerabilities to compromise sensitive data stored on cloud platforms. Furthermore, vulnerabilities arising from third-party integrations and weak security protocols significantly compound these risks. The Bank of America vendor breach and Bayview Asset Management's incident illustrate that attack vectors are not limited to direct technical flaws but also include compromised vendor systems and deficiencies in IT practices. Cybersecurity Expert 2 articulated that "*Social engineering tactics, unauthorized access via compromised credentials, and weak configurations in cloud environments are prevalent attack paths"*. A Financial Compliance Officer reinforced this view by noting, *"Data misconfigurations, vulnerabilities in third-party integrations, and supply chain risks serve as key attack vectors that expose sensitive financial data"*.

Theme 3: Effectiveness of Current Measures

Cloud security measures in U.S. financial institutions have evolved considerably, establishing a solid baseline of defense; however, recent case studies indicate that these measures often struggle to keep pace with sophisticated threats. After the Capital One breach, for instance, experts pointed out that existing security frameworks, while robust, can lag behind targeted attacks. As Cybersecurity Expert 1 remarked, *"Current measures establish a good baseline; however, they can lag behind sophisticated, targeted attacks. Continuous investment in adaptive security and threat intelligence is crucial"*. Cybersecurity Expert 2 noted, "*Although many institutions deploy robust security frameworks, these measures sometimes prove reactive. Proactive monitoring and regular security updates are necessary to outpace emerging threats"*. These insights underline that while current protocols help mitigate risk, they often require significant updates and proactive enhancements to address evolving cyber threats. From a regulatory and operational standpoint, the financial compliance officer highlighted that improvements in cloud security have been substantial, yet many defenses remain reactive rather than anticipatory. The officer stated, *"Security measures have improved, yet many remain reactive rather than anticipatory. Enhanced, integrated strategies that align with evolving regulatory standards are needed for better risk mitigation"*. This perspective underscores that while existing measures provide a necessary defense, ongoing refinements and coordinated efforts, both technical and regulatory, are essential to reduce vulnerabilities.

Conclusion

This research underscores that cloud security breaches in the U.S. financial services sector result in significant costs, both immediate and long-term, impacting financial performance, customer trust, and market reputation. The analysis reveals that vulnerabilities such as misconfigurations, compromised credentials, and weak third-party integrations are common entry points for attackers, indicating critical gaps in current security infrastructures. While existing preventative measures have laid a solid foundation, they are often reactive rather than proactive, necessitating continuous investment in adaptive security technologies, comprehensive vendor oversight, and dynamic regulatory strategies to mitigate evolving risks effectively**.**

Recommendations

1. Financial institutions should continuously update and harden cloud configurations, implement real-time monitoring, and integrate advanced threat intelligence systems to quickly detect and respond to evolving cyber threats.
2. Institutions must enforce rigorous security standards and comprehensive risk assessments for third-party vendors, ensuring that any external integrations meet strict security and compliance requirements to reduce vulnerabilities.
3. A strategic shift towards dynamic and integrated cybersecurity frameworks is crucial. This includes aligning security practices with evolving regulatory standards and continuously investing in adaptive technologies that can preemptively address both known and emerging threats.

REFERENCES

Almeida Teixeira, G., Mira da Silva, M. and Pereira, R. (2019) 'The critical success factors of GDPR implementation: a systematic literature review', Digital Policy, Regulation and Governance, 21(4), pp. 402–418.

Almuhammadi, S. and Alsaleh, M. (2017) 'Information security maturity model for NIST cyber security framework', Computer Science & Information Technology (CS & IT), 7(3), pp. 51–62.

Bonner, E., O'Raw, J. and Curran, K. (2011) 'Implementing the payment card industry (PCI) data security standard (DSS)', TELKOMNIKA (Telecommunication Computing Electronics and Control), 9(2), pp. 365–376.

Council, F.F.I.E. (2016) 'Federal Financial Institutions Examination Council'. Obtenido de Federal Financial Institutions Examination Council: https://www ….

Disterer, G. (2013) 'ISO/IEC 27000, 27001 and 27002 for information security management', Journal of Information Security, 4(2).

Felce, D., Vedral, V. and Tennie, F. (2021) 'Refrigeration with indefinite causal orders on a cloud quantum computer', arXiv preprint arXiv:2107.12413 [Preprint].

FFIEC, E.C. (2014) 'Federal Financial Institutions Examination Council', Bank Secrecy Act/Anti-Money Laundering Examination Manual [Preprint]. FDIC.

Ford, A. et al. (2021) 'The impact of data breach announcements on company value in European markets', in WEIS 2021: The 20th Annual Workshop on the Economics of Information Security.

Di Giulio, C. et al. (2017) 'Cloud standards in comparison: Are new security frameworks improving cloud security?', in 2017 IEEE 10th International Conference on Cloud Computing (CLOUD). IEEE, pp. 50–57.

Gross, T.R. (2012) 'Card-reader apparatus'. Google Patents.

Heng, S. et al. (2012) 'Cloud computing', Freundliche Aussichten für die Wolke, Deutsche Bank DB Research, Economics. Digitale Ökonomie und struktureller Wandel, Frankfurt am Main [Preprint].

Huang, H.H. and Wang, C. (2021) 'Do banks price firms' data breaches?', The Accounting Review, 96(3), pp. 261–286.

Humphreys, E. (2016) Implementing the ISO/IEC 27001: 2013 ISMS Standard. Artech house.

Khan, I. and Daena, M. (2023) 'Navigating Data Protection Regulations: Impacts on AI Innovation and Deployment'.

Lange, R. and Burger, E.W. (2017) 'Long-term market implications of data breaches, not', Journal of Information Privacy and Security, 13(4), pp. 186–206.

Malatji, M. (2023) 'Management of enterprise cyber security: A review of ISO/IEC 27001: 2022', in 2023 International conference on cyber management and engineering (CyMaEn). IEEE, pp. 117–122.

Möller, D.P.F. (2023) 'NIST cybersecurity framework and MITRE cybersecurity criteria', in Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices. Springer, pp. 231–271.

Oxford Analytical (2018) 'Cybersecurity risks will rise in Mexico', Emerald Expert Briefings [Preprint]. Oxford Analytica.

P. C. Industry (2010) 'Data security standard', Requirements and Security Assessment version, 3.

Protection Regulation (2018) 'General data protection regulation', Intouch, 25, pp. 1–5.

Seaman, J. (2020) PCI DSS: An integrated data security standard guide. Apress.

Syafrizal, M., Selamat, S.R. and Zakaria, N.A. (2020) 'Analysis of cybersecurity standard and framework components', International Journal of Communication Networks and Information Security, 12(3), pp. 417–432.

Vinoth, S. et al. (2022) 'Application of cloud computing in banking and e-commerce and related security threats', Materials Today: Proceedings, 51, pp. 2172–2175.

Wuermeling, J. (2017) 'Digitalization and cyber crime–" opportunity makes the thief"', EFL quarterly: an E-Finance Lab publication, 2017(3), p. 3.

Zheng, H.-B., Zheng, X.-G. and Liu, B.-P. (2015) 'miRNA-101 inhibits ovarian cancer cells proliferation and invasion by down-regulating expression of SOCS-2', International journal of clinical and experimental medicine, 8(11), p. 20263.