NOLEGEIN Journal of
Management Information Systems

ISSN: 2581-6810
Volume 6, Issue 1, 2023
DOI (Journal): 10.37591/NJMIS

http://mbajournals.in/index.php/JoMIS/index

Case Study NJMIS

Measures for Securing Information Systems in a Multinational Company to Protect Sensitive Data

Barkha*

Abstract

This case study focuses on the importance of securing information systems for companies, using the example of a large multinational company in the multi-service financial and manufacturing services sector. The study highlights the potential risks involved in securing information systems, including the financial and reputational harm that data breaches may cause, as well as the rising danger of cyberattacks. The report explores steps that businesses can take to secure their information systems, such as implementing strict password policies, network security measures, data encryption, employee training, and incident response plans. According to the study's findings, businesses may reduce their risk of cyberattacks and safeguard the security of their sensitive data by taking the necessary steps to secure their information systems.

Keywords: information systems, sensitive data, data protection, password policies, network security

INTRODUCTION

Securing the information systems of a company is one of the most important aspects of modern-day business operations. Companies rely significantly on digital technologies to store, handle, and send sensitive data in today's linked world. This information may include personnel files, client information, monetary information, intellectual property, and other trade secrets. As such, it is crucial that companies take appropriate measures to secure their systems to protect information against unauthorized access, data breaches, and other cybersecurity incidents. This case study will discuss the importance of securing information systems, the potential risks involved, and how a company can take measures to secure its information systems [1].

Background

Securing information systems has emerged as a crucial concern for firms across a range of industries in the current digital era [2]. Companies must put in place strong safeguards to protect their sensitive data from cyberattacks, data breaches, and other information security risks given the growing threat they pose. Failure to do so could lead to monetary losses, harm to one's reputation, and legal obligations [3].

***Author for Correspondence**
Barkha
E-mail: barkhaa9601194@gmail.com

Student, Department of Political Science, Lakshmi Bai College, Ashok Vihar, Delhi, India

Received Date: April 28, 2023
Accepted Date: May 07, 2023
Published Date: May 20, 2023

Citation: Barkha. Measures for Securing Information Systems in a Multinational Company to Protect Sensitive Data. NOLEGEIN Journal of Management Information Systems. 2023; 6(1): 6–9p.

Because financial data is handled by businesses on a daily basis in such large quantities, the financial services industry is particularly susceptible to information security risks. Furthermore, this sector is governed by strict data protection laws like the General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS) [4].

Given the potential risks involved, it is essential for companies in the financial services sector to take appropriate measures to secure their information

systems. However, despite the importance of information security, many companies struggle to implement effective measures due to various challenges, such as a lack of resources, insufficient expertise, and changing threat landscapes [5].

Consequently, this study aims to provide a thorough understanding of the significance of information system security for businesses, using the case of a sizable multinational corporation in the financial services industry. The study will highlight the potential risks involved in securing information systems, the measures that companies can take to secure their information systems, and the benefits of implementing effective information security practices [6].

METHODOLOGY

1. *Research design*: This study would use a qualitative case study approach as its research design. Data from numerous sources, including interviews, business reports, and other documents pertaining to information security, are collected. The case study would focus on a large multinational company in the financial services sector, known as HCL Technologies
2. *Data collection*: The data collection process would involve collecting data from a variety of sources, including key person interviews involved in information security, review of internal company documents related to information security policies, and analysis of external reports related to cyber threats and best practices in information security. The data collection process would be ongoing, and data would be collected over a period of several months.
3. *Data analysis*: A thematic analysis strategy would be used to examine the data that was gathered. Using the study questions and objectives as a guide, the data would be arranged into themes. Finding patterns and trends in the data as well as comparing it with external standards and best practices are all part of the analysis.
4. *Ethical considerations*: The study procedure would take ethical factors into account. Participants' informed consent would be obtained before the study was carried out, and all information gathered would be kept private and anonymous. The researcher would also make sure that the study was carried out in accordance with ethical standards and laws.
5. *Limitations*: The study has a number of restrictions. First, because the study would only focus on one case study, the results might not be as broadly applicable. Second, the data collected would be based on self-reported information, which could contain bias. Along with publicly available data, the study would also rely on. available data and may not include all relevant information related to information security.
6. *Conclusion*: A summary of the findings would be presented at the end of the study, including the measures that HCL Technologies has taken to secure its information systems, the potential risks involved in securing information systems, and recommendations for other companies to improve their information security practices. The publication would also include a description of the study's shortcomings and suggested research areas.

Importance of Securing Information Systems

Securing information systems is crucial for companies like HCL Technologies for several reasons. It primarily assists in preventing unauthorized access, theft, and misuse of sensitive information. A data breach can result in severe financial loss, harm to a company’s brand, and even legal obligations and fines. Moreover, companies are increasingly facing cyber threats from sophisticated hackers who are constantly looking for ways to exploit vulnerabilities in their information systems. Due to this, organizations must implement robust security measures to prevent cyberattacks [7].

Risks Involved in Securing Information Systems

Securing information systems is not without risks. It can be expensive and time-consuming to implement security measures, and there is always a chance of false positives, which can result in legitimate users being denied access to critical data. Additionally, security measures can also be

intrusive and affect employee productivity if they are not properly implemented. Finally, implementing security measures can lead to complacency among employees, who may rely too heavily on the security measures to protect their data, rather than being vigilant and proactive in protecting their information [8].

Measures to Secure Information Systems

HCL Technologies has implemented several measures to secure its information systems. These measures include the following:

1. *Implementing strict password policies*: One of the most basic yet effective measures to secure information systems is to enforce strong password policies. This can entail mandating that workers use secure, complicated passwords that are updated frequently. The company could also implement multi-factor authentication for added security. Employees at HCL Technologies are required to set secure passwords and to update them frequently in accordance with the company's strict password standards. The firm also uses multi-factor authentication to make sure that only permitted users have access to sensitive data [9].
2. *Network security*: As part of its network security measures, the company may employ firewalls, intrusion detection and prevention systems, and virtual private networks (VPNs). These precautions can help guard against malware and other online risks and help prevent unauthorized access to the company's network. A network security system that the corporation has put in place consists of firewalls, intrusion detection systems, and antivirus software. This technology guards against malware and other online dangers and assists in preventing unauthorized access to the company's network [10].
3. *Data encryption*: Data is encoded through the process of encryption so that unauthorized people cannot read it. The organization may encrypt all sensitive data, both in transit and at rest. This can shield sensitive data in the case of a security breach and help avoid data breaches. When transmitting and storing sensitive data, HCL Technologies uses encryption to keep it secure. Additionally, the business has strict data retention guidelines that make sure that data is only kept as long as is required [11].
4. *Employee training*: A key aspect of securing information systems is ensuring that staff are knowledgeable about potential risks and ideal practices related to information security. The company could conduct regular employee education programs to convey the significance of information security, the risks involved, and best practices for securing their devices and data. The company provides regular training to Educate staff members on good cybersecurity practices, including how to spot phishing emails, secure passwords, and safeguard private information. This encourages a culture among employees that values security [12].
5. *Incident response plan*: Security breaches can still happen despite the best efforts to stop them. The firm could develop and implement a comprehensive incident response plan to lessen the effect of security issues. Procedures for recognizing and responding to security events, contacting affected parties, and resuming normal operations could all be part of the plan. HCL Technologies has an incident response strategy in place that specifies the steps to take in the case of a cybersecurity incident or data breach. The strategy calls for actions to stop the situation, look into what caused it, and alert others who might be affected [13].
6. *Regular security assessments*: The business could carry out routine security evaluations, such as penetration testing and vulnerability scanning, to make sure its information security procedures are effective. These evaluations can aid in locating any gaps or vulnerabilities in the business's information systems, allowing it to take preventative measures before a security breach happens.
7. Overall, implementing these measures can help a company in the financial services sector secure its information systems and protect its sensitive data from cyber threats [14].

CONCLUSION

Companies in the financial services industry must priorities protecting their information systems to safeguard their private information and guard against liability, financial loss, and reputational harm.

This study aimed to provide a comprehensive understanding of the significance of protecting information systems, utilizing the example of a large multinational company in the financial services sector.

The study identified several measures that the company could take to secure its information systems, including implementing strong password policies and multi-factor authentication, network security measures, data encryption, frequent security audits, incident response strategies, and personnel training.

The study's conclusions showed that putting these steps in place can greatly increase the security of the business's information systems and lower the danger of cyber threats. Failure to take these actions could lead to large monetary losses, reputational harm, and legal consequences.

Overall, this study emphasizes the importance of securing information systems for companies in the financial services sector and provides guidance on measures that they can take to protect their sensitive data from cyber threats. Businesses must invest in information security if they want to protect their assets and maintain the trust of their stakeholders and clients.

REFERENCES

1. Kesan JP, Hayes CM. Strengthening cybersecurity with cyberinsurance markets and better risk assessment. Minn. L. Rev. 2017; 102: 191.
2. Kavak H, Padilla JJ, Vernon-Bido D, Diallo SY, Gore R, Shetty S. Simulation for cybersecurity: state of the art and future directions. Journal of Cybersecurity. 2021; 7 (1): tyab005.
3. Lohana S, Roy D. Impact of demographic factors on consumer's usage of digital payments. FIIB Business Review. 2021. DOI: 10.1177/23197145211049586.
4. Liu X, Wang S, Yao K, Sun R. Opportunistic behaviour in supply chain finance: a social media perspective on the "Noah event." Enterpr Inf Syst. 2021; 15 (10): 1607–1634.
5. Donalds C, Barclay C. Beyond technical measures: a value-focused thinking appraisal of strategic drivers in improving information security policy compliance. Eur J Inf Syst. 2022; 31 (1): 58–73.
6. Almudaires F, Almaiah M. Data an overview of cybersecurity threats on credit card companies and credit card risk mitigation. In 2021 International Conference on Information Technology (ICIT); 2021 Jul 14–15; Amman, Jordan: IEEE; 2021. 732–738 pp.
7. Bailey T, Banerjee S, Feeney C, Hogsett H. (2020). Cybersecurity: emerging challenges and solutions for the boards of financial-services companies. [Online] Available at https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-emerging-challenges-and-solutions-for-the-boards-of-financial-services-companies
8. Comizio VG, Dayanim B, Bain L. Cybersecurity as a global concern in need of global solutions: an overview of financial regulatory developments in 2015. J Invest Compliance. 2016; 17 (1): 101–111. DOI: 10.1108/JOIC-01-2016-0003.
9. Camillo M. Risks and management of risks for global banks and financial institutions. J Risk Manag Financ Inst. 2017; 10 (2): 196–200.
10. Dincer H, Hacioglu U, Tatoglu E, Delen D. A fuzzy-hybrid analytic model to assess investors' perceptions for industry selection. Decis Support Syst. 2016; 86: 24–34. DOI: 10.1016/j.dss.2016.03.005.
11. Hamzah RB. (2014). The determinant factors for a successful risk culture in banking sector: Malaysian case. [Online] Available at https://etd.uum.edu.my/4082/2/s812327_abstract.pdf
12. Mwamba N, Massawe N, Komba K. Financial sector development and financial inclusion. In Tanzania: the path to prosperity. Oxford, England: Oxford University Press; 2016. pp. 271–290.
13. Tamjidyamcholo A, Bin Baba MS, Shuib NLM, Rohani VA. Evaluation model for knowledge sharing in information security professional virtual community. Comput Sec. 2014; 43: 19–34. DOI: 10.1016/j.cose.2014.02.010.
14. Baldwin LP, Irani Z, Love PED. Outsourcing information systems: drawing lessons from a banking case study. Eur J Inf Syst. 2001; 10 (1): 15–24. DOI: 10.1057/palgrave.ejis.3000372.

