Spring 2023

Evaluating the Effectiveness of Cyber Security Regulations

Siraj Uddin Syed

EVALUATING THE EFFECTIVENESS OF CYBER SECURITY REGULATIONS

By

SIRAJ UDDIN SYED
B.S Computer Science, 2019

THESIS

Submitted in the partial fulfillment of the requirements

For the Degree of Master of Science,
With a Major in Information Technology

Governors State University
University Park, IL 60484

2023

Table of Contents

ABSTRACT

The rapid advancement of technology has led to an increase in the volume and sensitivity of personal and professional data stored and shared online. As a result, there is a growing need for effective cyber security regulations to protect against data breaches and ensure the confidentiality and integrity of sensitive information. The Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), and General Data Protection Regulation (GDPR) are three such regulations that have been implemented to address this need. This thesis aims to evaluate the effectiveness of these regulations in protecting sensitive information and preventing data breaches. A comprehensive literature review of existing research on the topic is conducted, and case studies of the implementation and enforcement of these regulations are analyzed. The study finds that while these regulations have been successful in raising awareness and establishing standards for cyber security, there is still room for improvement in their implementation and enforcement. Additionally, the study identifies the challenges and limitations in evaluating the effectiveness of cyber security regulations. Finally, recommendations for future research are provided in this area. The study concludes that while these regulations are important steps towards improving cyber security, more research is needed to fully understand their effectiveness and potential for improvement.

Keywords: Cyber security regulations, HIPAA, PCI DSS, GDPR, Data breaches, Implementation, Enforcement, Evaluation.

INTRODUCTION:

The rise of technology has led to an increase in the amount and sensitivity of data that is stored and shared online. Consequently, cyber security has become increasingly important to both individuals and organizations. Data breaches can lead to financial losses, damage to reputations, and even legal liability when personal information is stolen. There have been several regulations implemented to ensure the confidentiality and integrity of sensitive information in order to address these concerns. The Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), and General Data Protection Regulation (GDPR) are three such regulations that aim to protect sensitive information and prevent data breaches.

The effectiveness of these regulations in achieving their objectives is an important issue that has been widely discussed in literature. While these regulations have been successful in establishing standards and raising awareness of cyber security, there are still concerns regarding their implementation and enforcement. This thesis aims to evaluate the effectiveness of these regulations in protecting sensitive information and preventing data breaches, while also identifying the challenges and limitations in evaluating their effectiveness.

LITERATURE REVIEW:

The literature review is conducted to provide an overview of the existing research on cyber security regulations and to identify the key findings and research gaps. The review covers studies published between 2010 and 2022 and includes academic articles, reports, and case studies. The review is structured around three main themes: the effectiveness of cyber security regulations in preventing data breaches, the challenges and limitations in evaluating the effectiveness of cyber security regulations, and the potential for improvement in the implementation and enforcement of cyber security regulations.

EFFECTIVENESS OF CYBER SECURITY REGULATIONS IN PREVENTING DATA BREACHES:

One of the primary objectives of cyber security regulations is to prevent data breaches and ensure the confidentiality and integrity of sensitive information. Data breaches can have severe consequences, including financial losses, damage to reputation, loss of customer trust, and even legal liabilities. Therefore, evaluating the effectiveness of cyber security regulations in preventing data breaches is crucial.

Several studies have shown that cyber security regulations can have a positive impact on reducing the incidence of data breaches. For instance, a study by Ponemon Institute found that companies complying with the Payment Card Industry Data Security Standard (PCI DSS) had fewer data breaches and lower costs associated with such incidents than non-compliant companies.

However, cyber security regulations alone cannot guarantee the prevention of data breaches. Implementation and enforcement of these regulations are crucial to their effectiveness. According to a study by the National Institute of Standards and Technology (NIST), the failure to properly implement and enforce cyber security regulations can result in data breaches and other security incidents. Barrett (2018). For instance, a company may have implemented all the necessary security measures but failed to train its employees properly or failed to monitor third-party vendors who have access to its sensitive data.

Moreover, cyber threats are constantly evolving, and cyber criminals are becoming more sophisticated. This means that cyber security regulations must be continuously updated and improved to address new and emerging threats. For instance, the General Data Protection Regulation (GDPR) introduced new requirements such as the right to be forgotten, data portability, and mandatory breach notification, to address the changing nature of cyber threats (European Union Agency for Network and Information Security, 2019).

In conclusion, while cyber security regulations can be effective in preventing data breaches, their implementation and enforcement are crucial to their effectiveness. Furthermore, the constantly evolving cyber threat landscape requires continuous improvement and updating of these regulations to ensure their relevance and effectiveness in preventing data breaches.

QUANTITATIVE ANALYSIS:

PCI DSS (Payment Card Industry Data Security Standard):

The PCI DSS is a set of security requirements created to make sure that all businesses that receive, process, store, or transmit credit card information do so in a safe manner. According to a report by Verizon, in 2020, only 27.9% of organizations globally were fully compliant with all 12 requirements of PCIDSS, while 51.9% of organizations had less than 75% compliance with the requirements. This highlights the need for more stringent compliance measures and better enforcement of the standard (Verizon, 2020).

HIPAA (Health Insurance Portability and Accountability Act):

HIPAA, A set of Regulations designed to safeguard the confidentiality and security of patient health information. A study conducted by the US Department of Health and Human Services found that in 2019, there were 418 healthcare data breaches affecting more than 39 million individuals. Of these breaches, 51% were caused by hacking or IT incidents, while 35% were caused by unauthorized access or disclosure. The report also notes that the number of reported breaches has steadily increased over the years, indicating the need for stricter security measures (HHS, 2020).

GDPR (General Data Protection Regulation):

GDPR is a set of regulations that aim to protect the privacy and personal data of individuals in the European Union. A survey conducted by the Ponemon Institute found that in 2020, the average cost of non-compliance with GDPR was $3.86 million, up from $3.33 million in 2019. The survey also found that organizations that had a high level of GDPR compliance spent an average of 43% less on data breaches than non-compliant organizations (Ponemon Institute, 2020).

THE CHALLENGES AND LIMITATIONS IN EVALUATING THE EFFECTIVENESS OF CYBER SECURITY REGULATIONS:

1. **Lack of standardized metrics:** There is a lack of standardized metrics for measuring the effectiveness of cyber security regulations. Different regulations have different objectives, and measuring their effectiveness requires different metrics. For example, measuring the effectiveness of the General Data Protection Regulation (GDPR) would require different metrics than measuring the effectiveness of the Payment Card Industry Data Security Standard (PCI DSS). This lack of standardized metrics makes it challenging to compare the effectiveness of different regulations and identify best practices.
2. **Time lag:** Cybersecurity regulations are relatively new, and their effectiveness may not be immediately observable. It takes time for organizations to implement the necessary changes to comply with the regulations, and it may take even longer for the regulations to have an impact on the reduction of cyber risks. As a result, evaluating the effectiveness of cyber security regulations in the short term may not be an accurate representation of their long-term impact.
3. **Lack of data:** Evaluating the effectiveness of cyber security regulations requires data, both quantitative and qualitative. However, obtaining relevant data can be challenging due to issues such as data privacy concerns, the lack of reporting requirements, and the reluctance of organizations to share data. Without adequate data, it is difficult to measure the impact of cyber security regulations accurately.

4. **Complexity of the cybersecurity landscape:** Cybersecurity is a complex field, and the effectiveness of cyber security regulations is influenced by various factors, such as the size of the organization, the industry sector, and the threat landscape. The complexity of the cybersecurity landscape makes it challenging to isolate the impact of cyber security regulations from other factors that may influence an organization's cybersecurity posture.

Despite these challenges, several studies have attempted to evaluate the effectiveness of cyber security regulations. A study by Mitropoulos and Akkaya (2020) evaluated the effectiveness of the General Data Protection Regulation (GDPR) in reducing data breaches. The study found that while the GDPR had a positive impact on reducing the frequency of data breaches, it had a limited effect on the severity of the breaches. Another study by Huang et al. (2019) evaluated the effectiveness of the Payment Card Industry Data Security Standard (PCI DSS) in reducing credit card fraud. The study found that the PCI DSS had a significant positive impact on reducing credit card fraud.

In conclusion, evaluating the effectiveness of cyber security regulations is a challenging task due to various factors such as the lack of standardized metrics, time lag, lack of data, and the complexity of the cybersecurity landscape. However, despite these challenges, several studies have attempted to evaluate the effectiveness of cyber security regulations, providing valuable insights for policymakers, regulators, and practitioners.

THE POTENTIAL FOR IMPROVEMENT IN THE IMPLEMENTATION AND ENFORCEMENT OF CYBER SECURITY REGULATIONS:

The implementation and enforcement of cyber security regulations are critical factors in ensuring the protection of sensitive information and preventing data breaches. While regulations such as HIPAA, PCI DSS, and GDPR have been successful in raising awareness and establishing standards for cyber security, there is still room for improvement in their implementation and enforcement. In this section, we will discuss the potential areas of improvement in the implementation and enforcement of cyber security regulations.

One area where cyber security regulations can be improved is through the use of technology. The use of advanced technology such as machine learning and artificial intelligence can help organizations to identify potential threats and vulnerabilities in their systems in real-time, thus allowing them to take proactive measures to prevent cyber attacks. For example, machine learning algorithms can be used to identify patterns of suspicious behavior that may indicate a potential cyber attack, while AI-based security tools can be used to detect and respond to threats in real-time.

Another potential area for improvement is through the use of risk assessments. Risk assessments can help organizations to identify potential vulnerabilities in their systems and develop a comprehensive strategy to mitigate those risks. By conducting regular risk assessments, organizations can ensure that their cyber security measures are up-to-date and effective in preventing cyber attacks.

Furthermore, the implementation and enforcement of cyber security regulations can be improved by providing training and education to employees. Employees are often the weakest link in cyber security, and many cyber attacks are the result of human error or lack of awareness. By providing regular training and education on cyber security best practices, organizations can ensure that their employees are equipped with the knowledge and skills to prevent cyber attacks.

In addition, cyber security regulations can be improved by ensuring that they are regularly updated to reflect changes in technology and emerging threats. Cyber threats are constantly evolving, and regulations that were effective in the past may not be sufficient to protect against current and future threats. By regularly updating regulations to reflect these changes, policymakers and regulators can ensure that organizations are equipped with the necessary tools and guidelines to protect against cyber attacks.

Overall, the potential for improvement in the implementation and enforcement of cyber security regulations is vast. By leveraging technology, conducting regular risk assessments, providing training and education, and ensuring that regulations are regularly updated, organizations can improve their cyber security posture and protect against cyber attacks.

LIMITATIONS OF THE STUDY:

This study has several limitations. First, the evaluation of the effectiveness of cyber security regulations is a complex and multidimensional issue that requires a comprehensive and holistic approach. Although this study has conducted a comprehensive literature review and analyzed case studies of the implementation and enforcement of the regulations, there may be other factors that have not been considered or included in the analysis. Moreover, the study is limited to the three selected regulations (HIPAA, PCI DSS, and GDPR) and may not be generalizable to other regulations or contexts.

Second, the evaluation of the effectiveness of cyber security regulations is often hindered by the lack of reliable and comprehensive data. Many organizations are reluctant to disclose information about data breaches or cyber attacks due to fear of reputational damage or legal liability. Additionally, there is no standardized approach or metric for evaluating the effectiveness of cyber security regulations, which makes it difficult to compare and aggregate data across organizations or sectors.

Finally, this study is limited to a qualitative analysis of the effectiveness of cyber security regulations. Future research could use quantitative methods, such as surveys or experiments, to measure the impact of cyber security regulations on data breaches or other cyber security outcomes.

RECOMMENDATIONS FOR FUTURE RESEARCH:

Based on the findings and limitations of this study, several recommendations for future research can be made.

First, future research should aim to develop a standardized approach or metric for evaluating the effectiveness of cyber security regulations. This would enable more reliable and comparable data to be collected and analyzed, which would in turn facilitate a more accurate evaluation of the effectiveness of cyber security regulations.

Second, future research should aim to evaluate the effectiveness of other cyber security regulations beyond the three selected in this study (HIPAA, PCI DSS, and GDPR). This would enable a more comprehensive and nuanced understanding of the effectiveness of cyber security regulations across different sectors and contexts.

Third, future research should aim to identify and address the factors that hinder the implementation and enforcement of cyber security regulations. This would enable a more effective implementation and enforcement of the regulations, which would in turn enhance their effectiveness in protecting sensitive information and preventing data breaches.

Fourth, future research should aim to evaluate the effectiveness of cyber security regulations using quantitative methods, such as surveys or experiments. This would enable a more precise and rigorous evaluation of the impact of cyber security regulations on data breaches or other cyber security outcomes.

Finally, future research should aim to evaluate the long-term effectiveness of cyber security regulations. This would enable a more comprehensive and sustainable evaluation of the effectiveness of cyber security regulations over time, which would in turn facilitate a more effective and adaptive regulatory approach to cyber security.

CONCLUSION:

The rapid advancement of technology has led to an increase in the volume and sensitivity of personal and professional data stored and shared online. As a result, there is a growing need for effective cyber security regulations to protect against data breaches and ensure the confidentiality and integrity of sensitive information. The Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), and General Data Protection Regulation (GDPR) are three such regulations that have been implemented to address this need.

This thesis aimed to evaluate the effectiveness of these regulations in protecting sensitive information and preventing data breaches. A comprehensive literature review of existing research on the topic was conducted, and case studies of the implementation and enforcement of these regulations were analyzed. The study found that while these regulations have been successful in raising awareness and establishing standards for cyber security, there is still room for improvement in their implementation and enforcement. Additionally, the study identified the challenges and limitations in evaluating the effectiveness of cyber security regulations.

However, there are limitations to this study that should be acknowledged. First, the analysis is limited to three specific regulations - HIPAA, PCI DSS, and GDPR - and may not be generalizable to other cyber security regulations. Second, the study relied primarily on secondary sources of information, such as case studies and existing research, which may not provide a comprehensive picture of the effectiveness of these regulations. Future research could address these limitations by expanding the analysis to include other regulations and by incorporating primary data collection methods, such as surveys and interviews, to provide a more nuanced understanding of the effectiveness of cyber security regulations.

In conclusion, cyber security regulations play a crucial role in protecting sensitive information and preventing data breaches. The three regulations examined in this study - HIPAA, PCI DSS, and GDPR - have been successful in raising awareness and establishing standards for cyber security. However, there is still room for improvement in their implementation and enforcement. By addressing the challenges and limitations identified in this study, policymakers, regulators, and practitioners can work towards improving the effectiveness of cyber security regulations and better protecting the confidentiality and integrity of sensitive information stored and shared online.

REFERENCES:

1. Barrett, M. (2018). Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, NIST Cybersecurity Framework Retrieved from https://doi.org/10.6028/NIST.CSWP.04162018
2. European Union Agency for Network and Information Security. (2019). Cybersecurity Regulation and Standardization. https://www.enisa.europa.eu/topics/cybersecurity-regulation-and-standardisation
3. Huang, H., Chen, M. Y., Huang, Y. H., & Tzeng, G. H. (2019). Evaluating the effectiveness of the Payment Card Industry Data Security Standard in reducing credit card fraud. Information & Management, 56(3), 370-383.
4. Mitropoulos, S., & Akkaya, K. C. (2020). Evaluating the effectiveness of the GDPR in reducing data breaches. Computers & Security, 88, 101640.
5. 2012 Payment Security Practices Survey: United States by Ponemon institute. https://www.ponemon.org/local/upload/file/US_Cybersource_WPFinal.pdf
6. Verizon. (2020). Payment Security Report 2020. https://www.verizon.com/business/resources/T38/reports/2020-payment-security-report.pdf
7. HHS. (2020). Healthcare Industry Cybersecurity Task Force Report.
8. Ponemon Institute. (2020). The Cost of a Data Breach report Retrieved from https://www.ibm.com/downloads/cas/QMXVZX6R?mhsrc=ibmsearch_a&mhq=cost%20of%20data%20breach%202020