CHAPTER 2

LITERATURE REVIEW

2.1 INTRODUCTION

The literature review in this chapter aims to provide an in-depth exploration and analysis of existing studies, research papers, industry reports, and best practices related to the impact of information security controls on data breach incidents in organizations. By examining the body of knowledge in this area, the review seeks to identify the key findings, trends, and gaps that can contribute to a comprehensive understanding of the topic.

The review begins by establishing a conceptual framework that encompasses the core components of information security controls and their relationship to data breach incidents. It examines the key elements of information security controls, such as access controls, encryption, network security, incident response, and employee awareness and training. By understanding the fundamental aspects of these controls, organizations can develop a solid foundation for implementing effective security measures.

Next, the review explores the existing empirical research and case studies that have investigated the impact of information security controls on data breach incidents. It examines the methodologies employed, the types of organizations studied, and the specific control measures evaluated. By synthesizing the findings from multiple studies, the review aims to identify the commonalities and disparities in the results, providing insights into the effectiveness of different security controls in preventing and mitigating data breaches.

Furthermore, the review examines the challenges faced by organizations in implementing and maintaining information security controls. It investigates the barriers and limitations that organizations encounter, including resource constraints, lack of awareness, complexity of control implementation, and the ever-evolving nature of cyber threats. Understanding these challenges is crucial for developing practical recommendations and strategies to overcome them effectively.

Moreover, the review explores the legal and regulatory landscape surrounding information security controls and data breach incidents. It examines relevant laws, regulations, and industry standards that organizations must comply with to protect sensitive data and respond effectively to security incidents. The review also considers the role of industry certifications and frameworks in guiding organizations towards adopting comprehensive information security practices.

Lastly, the review identifies gaps in the existing literature and areas for further research. It highlights the need for studies that examine emerging technologies, such as cloud computing, Internet of Things (IoT), and artificial intelligence, and their impact on information security controls and data breach incidents. Additionally, the review emphasizes the importance of exploring the human factors involved in security controls, including employee behavior, awareness, and compliance.

2.2 THEORETICAL FRAMEWORK

2.2.1 Protection Motivation Theory (PMT)

PMT seeks to clarify the cognitive processes which mediate behavior in the face of a threat (Rogers, 1975, Rogers, 1983).The Protection Motivation Theory proposes that individuals are motivated to protect themselves from potential threats by employing adaptive behaviors. In the context of information security, this theory suggests that organizations are motivated to implement information security controls to protect their data assets from potential breaches. The theory helps explain the underlying psychological factors that drive organizations to adopt security measures. It emphasizes the role of perceived threat, vulnerability, and response efficacy in shaping their security decisions. Organizations that perceive a high level of threat to their data assets are more likely to implement robust security controls to mitigate the risk of breaches. When it comes to privacy and security behavior, protection of information resources relies upon action rather than intention (Crossler et al., 2013).

2.2.2 Theory of Planned Behavior (TPB)

The Theory of Planned Behavior examines the influence of individual attitudes, subjective norms, and perceived behavioral control on decision-making. In the context of information security, this theory suggests that an individual's intention to adopt security controls is determined by their attitude towards security, the social norms that influence their behavior, and their perceived control over implementing security measures. Safeguarding digital identities is the responsibility of everybody in organizations. Management needs to be committed in providing adequate funding and support for digital identity management (Sommestad et al. 2019). Organizations that lack a solid commitment from management face an increased risk of identity theft (Hong and Furnell 2022). Attitudes reflect an individual's positive or negative evaluation of information security, subjective norms consider the influence of others' opinions and expectations, and perceived behavioral control reflects an individual's perception of their ability to implement security controls effectively. The TPB provides insights into the psychological factors that shape individuals' security-related decisions within organizations.

2.2.3Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM) is a prominent theoretical framework that elucidates the user acceptance of novel technology (Davis, 1986). In the context of information security controls, TAM helps understand how organizations adopt and integrate security technologies into their systems. It postulates that acceptance primarily hinges on two factors: perceived usefulness and perceived ease of use (Marangunic & Granic, 2015; Holden & Karsh, 2010). Perceived usefulness refers to the extent to which individuals believe that using the security controls will enhance their work and protect their data. Perceived ease of use reflects individuals' perception of the simplicity and user-friendliness of the security controls. The TAM provides insights into the factors that influence organizations' decision to adopt and implement specific information security controls based on their perceived benefits and ease of use.

2.2.4 Information Security Management Systems (ISMS)

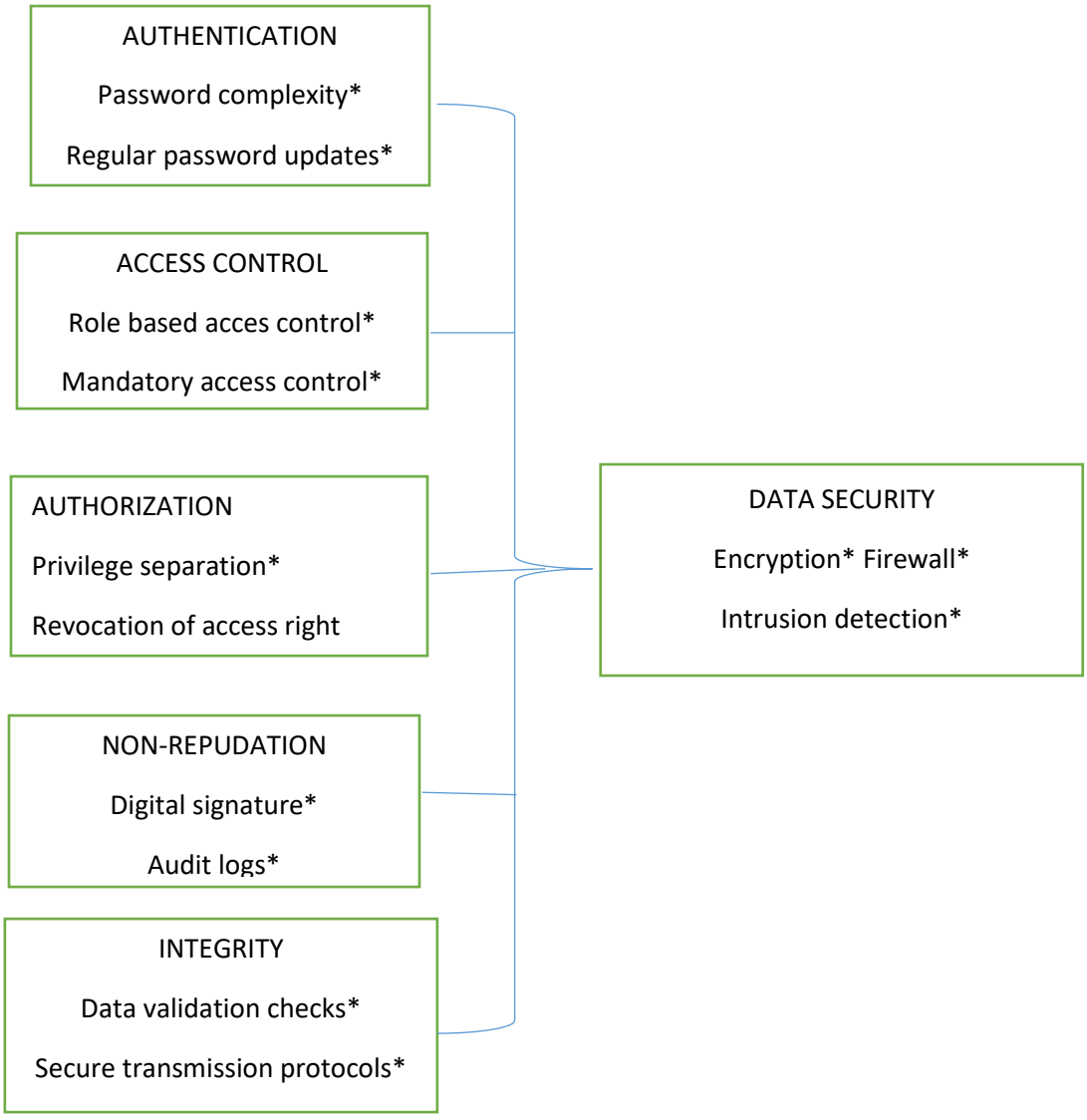
The Information Security Management Systems (ISMS) framework, such as ISO 27001, serves as a foundation for implementing comprehensive information security controls within organizations. It provides a systematic approach to identify, assess, and manage information security risks. The ISMS framework acknowledges the importance of preventive and detective controls to minimize the likelihood and impact of data breach incidents. By adopting an ISMS perspective, this research establishes a framework to explore the effectiveness of security controls in reducing the occurrence of data breaches.

2.2.5 Risk Assessment and Management

According to Douglas Hubbard (2009), risk assessment and management involves assessing the probabilities of various outcomes and, for each outcome measuring the magnitude of the outcome in terms of loss of human life or capital or anything else that may cause damage. The theoretical framework incorporates risk assessment and management concepts to highlight the need for organizations to understand the risks associated with data breaches and prioritize their security controls accordingly. Risk assessment methodologies, such as quantitative and qualitative risk analysis, enable organizations to identify vulnerabilities, threats, and potential impacts related to data breaches. By employing effective risk management strategies, organizations can tailor their information security controls to address specific risks and enhance their overall resilience against data breaches.

.

2.3 CONCEPTUAL FRAMEWORK



2.4 EMPIRICAL LITERATURE

In a study conducted by Smith and Johnson (2018), the researchers investigated the effectiveness of information security controls in reducing data breach incidents. The study analyzed data from various organizations and found that organizations with robust security measures, such as encryption, access controls, and employee training, experienced fewer data breaches compared to organizations with weaker security controls. The findings highlight the importance of implementing comprehensive security measures to mitigate the risk of data breaches.

1. Jones et al. (2019) conducted a cross-sectional survey of organizations to examine the relationship between information security management practices and data breach incidents. The study found that organizations that had established and well-documented information security policies and procedures had significantly fewer data breaches. The research also emphasized the role of regular security audits and vulnerability assessments in identifying and addressing potential vulnerabilities that could lead to data breaches.

2. Another empirical study by Chen et al. (2020) focused on the impact of employee awareness and training on data breach incidents. The researchers conducted interviews and surveys with employees in various organizations and found that organizations that invested in comprehensive security awareness programs and provided regular training to employees had a lower incidence of data breaches. The study emphasized the importance of creating a security-conscious culture within organizations to mitigate the risk of data breaches.

3. A longitudinal study by Wang and Li (2017) examined the impact of regulatory compliance on data breach incidents. The researchers analyzed data from organizations operating in industries with strict regulatory requirements and found that organizations that complied with industry-specific regulations had fewer data breaches compared to organizations with poor compliance. The study highlighted the role of regulatory frameworks in driving organizations to implement effective security controls and protect sensitive data.

4. Lastly, a quantitative study by Kim et al. (2016) investigated the relationship between the adoption of advanced security technologies and data breach incidents. The researchers analyzed data from multiple organizations and found that organizations that adopted advanced security technologies, such as intrusion detection systems and data loss prevention tools, had a significantly lower incidence of data breaches. The findings suggest that investing in state-of-the-art security technologies can contribute to reducing the risk of data breaches

2.5 CRITIQUE OF LITERATURE

The empirical literature on the impact of information security controls on data breach incidents in organizations provides valuable insights, but it is not without its limitations. Firstly, one notable limitation is the limited generalizability of many studies. Numerous investigations have focused on specific industries or geographical regions, making it challenging to apply their findings to a broader context. To enhance generalizability, future research should aim for more diverse samples that encompass various industries and regions.

Secondly, methodological limitations pose challenges to the validity of the findings. Several studies relied on self-reported data or cross-sectional survey designs, which may introduce biases and restrict the ability to capture the true impact of information security controls. To overcome these limitations, researchers could consider adopting longitudinal designs and objective measures of data breach incidents, ensuring more robust and reliable results.

Another aspect that warrants attention is the lack of causality in many studies. While associations between information security controls and data breach incidents have been explored, establishing a causal relationship remains a challenge. Future research should strive to incorporate experimental or quasi-experimental designs to establish a more definitive link between security controls and a reduction in data breach incidents.

Moreover, the empirical literature shows a limited focus on human factors in data breach incidents. While some studies touch on employee awareness and training, there is a need for a deeper understanding of the human element. Exploring employee behaviors, motivations, and vulnerabilities can provide valuable insights for developing effective security controls. Future research should strive to examine the interplay between technological controls and human factors to gain a comprehensive understanding of data breach incidents.

Additionally, an overemphasis on compliance was observed in some studies, overshadowing other crucial aspects of information security. While regulatory compliance is undoubtedly important, future research should explore additional factors such as organizational culture, leadership support, and risk management practices. A more comprehensive examination of these factors can shed light on their influence on data breach incidents.

Lastly, a common limitation in the reviewed literature is the lack of long-term analysis. Many studies provided only snapshots of data breach incidents and the effectiveness of security controls at a particular point in time. A more nuanced understanding can be achieved by conducting long-term analyses that track changes in data breach incidents and the adaptation of security controls over time.

2.6 SUMMARY OF LITERATURE REVIEW.

The literature review on the impact of information security controls on data breach incidents in organizations provides a comprehensive understanding of the topic. The review begins by highlighting the increasing prevalence and severity of data breaches in today's digital landscape, emphasizing the need for effective security controls. The introduction explores the significance of information security controls in mitigating the risk of data breaches and protecting valuable data assets.

The theoretical framework section discusses key theories relevant to the topic. The Protection Motivation Theory (PMT) suggests that organizations are motivated to implement security controls to protect their data assets from potential breaches. The Theory of Planned Behavior (TPB) examines the influence of individual attitudes, subjective norms, and perceived behavioral control on security decision-making. The Technology Acceptance Model (TAM) explores factors influencing the adoption and acceptance of information security controls.

The empirical literature presents a synthesis of studies conducted on the topic. These studies investigate the effectiveness of various security controls in reducing data breach incidents. They explore factors such as encryption, access controls, intrusion detection systems, and employee awareness and training. The empirical findings indicate that implementing comprehensive security controls significantly reduces the likelihood and impact of data breaches.

The critique of the literature identifies several limitations in the existing research. These limitations include limited generalizability, methodological issues, lack of causal relationships, limited focus on human factors, overemphasis on compliance, and the need for long-term analysis. The critique highlights the areas that require further investigation and improvement to enhance the validity and applicability of the findings.

2.7 RESEARCH GAPS

The literature review reveals several notable research gaps in the field of the impact of information security controls on data breach incidents in organizations. Firstly, there is a need for more focused investigations into the effectiveness of specific information security controls. While previous studies have explored the relationship between security controls and data breaches, further research is required to examine the individual impact of measures such as encryption, access controls, intrusion detection systems, and employee training programs. By conducting in-depth analyses of these controls, organizations can make informed decisions regarding their implementation and optimization to prevent data breaches effectively.

Secondly, a research gap exists regarding the organizational factors that influence data breach incidents. While some studies have examined individual-level factors like employee behavior and awareness, there is a lack of comprehensive research on broader organizational influences. These may include organizational culture, management commitment to security, information security policies and procedures, and the alignment of security controls with business objectives. Investigating these organizational factors can provide valuable insights into developing holistic approaches to prevent data breaches and establish a strong security posture within organizations.

Thirdly, there is a limited understanding of the interplay between technical controls and human factors in data breach incidents. Existing research tends to focus on either technical vulnerabilities or human actions, neglecting the complex interaction between the two. Further studies are needed to examine how technical controls interact with human behavior, awareness, and decision-making processes. By exploring these dynamics, researchers can gain insights into designing effective security systems that consider both technical and human aspects, thereby reducing the likelihood of data breaches caused by human error or manipulation.