World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Data security strategies to avoid data breaches in modern information systems

Chukwudi Tabitha Aghaunor [1,*], Patience Eshua [2], Tawo Obah [3] and Oluwatoyin Aromokeye [4]

[1] *School of Data Intelligence and Technology, Robert Morris University, Pittsburgh, Pennsylvania, United States.*
[2] *Department of Information Systems, East Tennessee State University, Johnson City, Tennessee, United States.*
[3] *Department of Computer Science, Wrexham University, Wreaxham, Wales, United Kingdom.*
[4] *Department of Analytics, Kogod School of Business, American University, Washington DC, District of Columbia, United States.*

World Journal of Advanced Research and Reviews, 2025, 25(01), 827-849

Publication history: Received on 18 November 2024; revised on 26 December 2024; accepted on 28 December 2024

Article DOI: https://doi.org/10.30574/wjarr.2025.25.1.3906

Abstract

Introduction: Cyber threats are constantly increasing in severity and targeting organizations in all industries, and result in loss of valuable data and a decline in stakeholders' confidence. Advanced information systems positively impact overall organizational operations and functionality but bring new opportunities that adversaries seek. This research article seeks to look at how organizations can enhance data protection and prevent breaches in modern technology landscapes.

Materials and Methods: An initial search and screener was done on selected journal article from the year 2015-2024 that was peer reviewed, industry report, and case study. The conceptual framework combined the theoretical approach to data breaches, malware attacks, and cybercriminal motives with factors, such as users' perceptions, legal requirements. Data from 22 original papers were subject to a qualitative content analysis approach, and thematic synthesis was used to determine common patterns in security practices, threats, and risk management mechanisms.

Results: The analysis revealed several key themes: 1) The major importance of security awareness training as the key to strengthening the human factor which is the weakest link in the context of data protection. 2) The validity of the layer defense principle that entailed a combination of technical measures and sound policies and procedures. 3) The role of encryption, access controls, and data minimization to protect information and data that is more important today than ever before. 4) Threat Intelligence and incident response planning to detect the breaches in advance before the threat actors begin executing the attack. 5) The role of AI and machine learning as threats and as the possibility to identify and prevent threats while using their opportunities for data analysis in cybersecurity.

Discussion: The results imply that the protection of information should be an organizational, risk management approach with current and future threats in mind. However, while technical measures must be adopted, so too must the emphasis be placed on promotion of a security-aware culture as well as the adherence to regulatory requirements. The research indicates areas for future development, with specific emphasis on the issues of insider threats and protection of information in cloud and IoT contexts. Drawbacks include the fact that technological advancements are rather fast, which makes it difficult for academic publications to keep up with them. Additionally, there could be situations when certain industries fail to report breaches.

Conclusion: Preventing data breaches in today's information systems, therefore, cannot be addressed through a single solution that involves merely the application of people, processes or technology, but rather through a holistic approach oriented towards the integration of the three aspects. Organizations need to be creative about the issue and adopt emerging technologies that address existing and fundamental security risks. Further research should focus on the

* Corresponding author: Chukwudi Tabitha Aghaunor

effects of AI-based threats calculate the return of security investments, and establish guidelines for data protection specific to industries.

Keywords: Data breaches; Information systems; Data security; Threat landscape; Internet of Things; Attack vectors

1. Introduction

In a world where computing technologies and integrated IT infrastructures are key indicators of a post-industrial society, data has emerged as the essential fluid for the engines of the economy in the fourth sector. However, this increasing utilization of digital assets has occurred simultaneously with an escalating number of cyberattacks, which puts vulnerable data into the wrong hands and poses risks to the privacy, financial security and reputation of the organizations in question. The frequency and complexity of such breeches has risen sharply in recent years, and large companies, hospitals and government bodies across the world have quickly become victims of these cyber-assaults that are now reported on an almost daily basis. Some surveys conducted recently reveal that the average cost of a data breach has skyrocketed to its all-time figures and comes with other implications that can manifest themselves in the form of lost revenues, gradual decline of the customer trust, considerable regulatory fines and possible legal actions (Angst et al., 2017). This constant threat environment requires a systematic study of data protection measures adapted to the problems arising from contemporary information technologies that frequently include intricate cloud environments, portable platforms, and IoT peripherals.

This necessity is also fueled by the increasing world data protection legislation, including GDPR in EU and CCPA in USA, where personal information protection requirements are very strict. This ordinance does not only require organizations to take improved measures on security but also to face severe repercussions and consequences in case they fail to adequately protect personal information. In this context, organizations all over the world are facing the difficulty of managing to take advantage of technological tools that rely on data at the same time as try to enhance their protection against the numerous forms of cyber threats. The healthcare industry remains especially susceptible for several reasons, including the basically non-negotiable nature of patients' data privacy and convenience of centralized electronic health records (EHRs) within the contemporary approach to treatment. , it is important to recognize, as Ibrahim et al. pointed out (2020), the health care has become the sector of interest for cyber criminals whose actions can adversely affect not only the financial institution, but also endanger the health of the patients.

The technological advancement of the information systems has an element of risk in the information security field while simplifying the field at the same time. On the one hand, innovative approaches and technologies such as artificial intelligence, machine learning, and big data analysis provide effective opportunities for identifying additional groups of signs and patterns with indicators of possible vulnerabilities, and for automating the processes of threat detection and response to them. On the other hand, newer technologies such as Cloud computing and mobile devices, IoT endpoints basically have provided new avenues of data theft and breach of the earlier concepts of security perimeters. This constantly evolving environment requires a much broader strategy that enhances data protection beyond narrow definitions of cybersecurity, which will include technical issues as well as those social and historical elements that define the security status of an entity. While writing their paper, Cheng et al. (2017) noted that it is a combination of a strong technology and a technical control policy in addition to constant training and engagement of employees in risk management practices.

Technological advancement has not slowed down and the complexity of the threats to data continues to grow, thus research and development in the area remain crucial. Although several case studies that are dedicated to the analysis of data breach prevention have been published, there is a lack of a definite framework that would integrate all the known effective practices and take into account the differences in organizational environments as well as the emergence of new technologies. To this end, this research article will undertake a comprehensive literature review to evaluate existing literature and research studies in an attempt to compare various strategies for managing data breach risks in today's advanced information systems. In that context, the research aims at offering practical findings for IT managers, security specialists, and other decision-makers who may be directly involved in protecting critical data within the organizational setting and challenged by the growing threat of cybercrime.

At the core of the conceptual foundations of this research, there is an understanding that data breaches themselves are a multifaceted process that involves technology, people, and often malice. As indicated in Figure 1, the theoretical framework adopted in this study comprises a composite analysis of the nature of data breach, including the kind of malware attacks, the reasons behind cyber attacker actions, and the conditions that make it easy for such entities to perpetrate security malicious acts. The presented view coincides with Griffin (2017), who also highlighted the value of looking at different aspects when designing the security strategies. This paper adopts theoretical framework from

Computer science, Information system management, and Behavioral psychology in order to examine the intricate nature of data breaches in the contemporary world and the corresponding interventions in countering the challenges arising from such incidences.

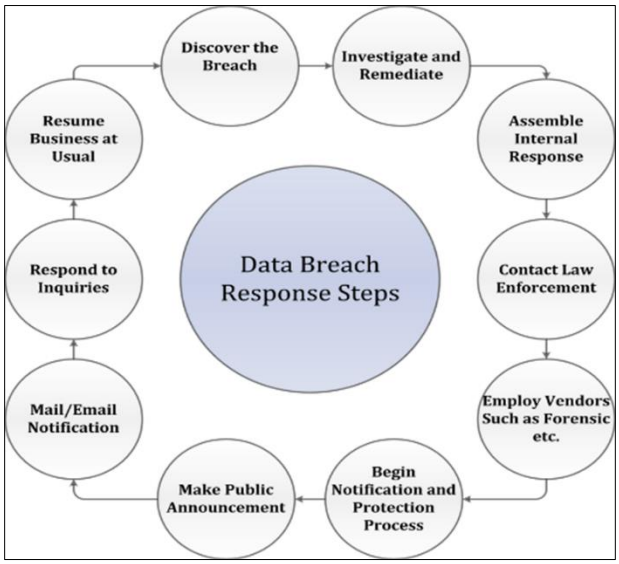


Figure 1 Data breach response steps. Source; Kitchin, (2016)

Modern security threats at digital space inculcate the need to question traditional security models with a rapid call for new strategies that can effectively protect data. With the adoption of cloud services and work from home policies, the traditional idea of security perimeters no longer holds value, even for decision makers who used to be staunch anti-cloud advocates. This change has been particularly significant in the health care industry where the use of electronic health records and health information exchanges has redefined patient care but also risk. Figure 2 presents factors and actors that are involved between the provider, business associate, and third parties in sharing a patient's sensitive personal health information and it underlines the areas of vulnerability, which can be leveraged by the attacker. Analyzing these complex interconnections and the accompanying data transmissions is of great importance for carving out specific security measures with regards to individual system members and their respective problems in the sphere of healthcare.

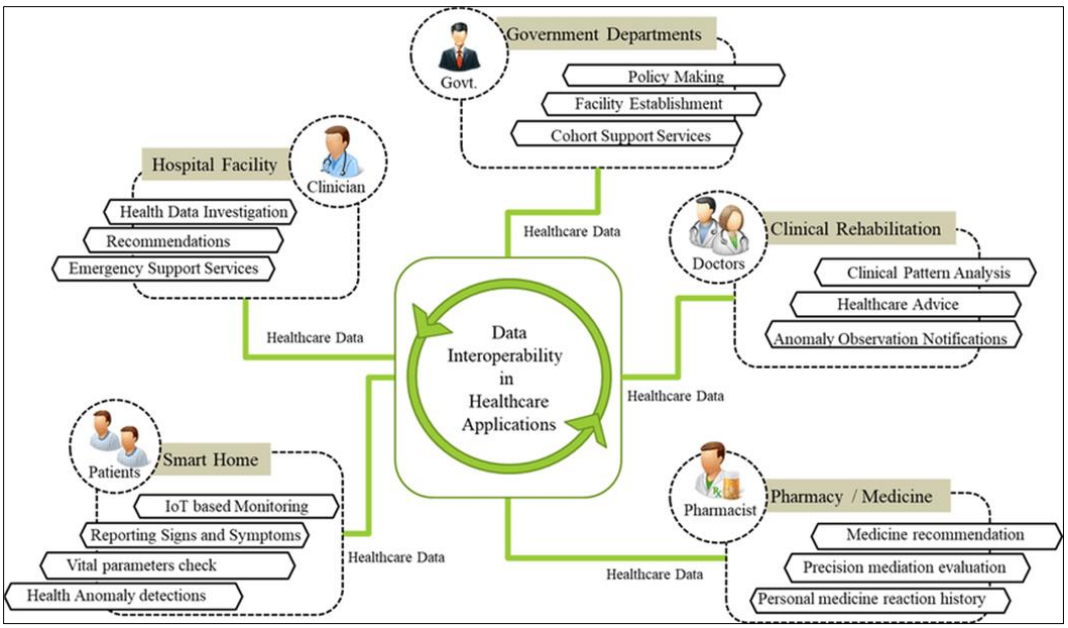


Figure 2 Conceptual Framework of the data interoperability in heterogeneous healthcare service environments. Accessed from Ali, & Chong, (2019)

Note: The figure illustrates the interconnectivity when healthcare providers, business associates, and third parties exchange electronic health records, electronic medical records, protected health information, or personally identifiable information, and how data breaches or cyberattacks can happen, or vulnerabilities can be exploited by attackers.

The availability of mobile devices continues to growth and adoption of byond policy in so many organizations has added to the challenge of data security, and there are no clear distinctions between personal and company data, difficulties in the authorization and data management. In the view of Desai and Jaiswal, 2020 mobile devices are very promising and popular targets for cybercriminals since devices can be lost or stolen, are frequently used, and may contain various types of valuable information. Mitigating these mobile-specific risks calls for an integrated solution at the device and network levels and comprehensive guidelines for the utilization of the personal device at the workplace. Furthermore, the growing use of IoT devices in different businesses aggravates the situation, as these devices are frequently low on processing power and memory and can be exploited by malicious actors as a way of gaining access to the more encompassing IoT network.

The human factor hence endures as a highly dangerous aspect of organizations, as insider attacks and social engineering are potent threats to even the most fortified organizations. The work by Kostic (2020) is a clear signal that awareness practice must be delivered in a wholesome manner and effective messaging must be given out in order to create a security savvy people and develop a culture of security ownership at the company level. This people-centered security paradigm argues that it is unrealistic to expect that technology alone can deal with existing and evolving cyber threats and that training and equipping employees on how to respond to these threats is crucial in developing sound Information systems. Increased awareness of these complex threats leads many organizations to evaluate the effectiveness of their existing security mechanisms and look for innovative solutions that would enable them to implement dynamic security measures capable of adapting to further growth and changes in dangerous activities. This means that in addition to having sound technical controls, incident response plans, monitoring, and threat intelligence, and governance structures must be in place and dynamic enough to respond to the ever-evolving threats and regulatory environment. AI and machine learning with applications of the advanced technologies represent potential directions in expanding layers that can be applied to security operations, in purpose, to analyze security data occurring in real time and patterns that might suggest breaches or risks (Wang et al., 2023).

1.1. Research Question

The central research question guiding this study is: The following are the research questions: What general and specific strategic cybersecurity defense methods can IT Managers employ to decrease data breach in contemporary information systems with varying organizational environments? This overarching question encompasses several sub-inquiries that will be explored throughout the research

- Based on literature, what are Artificial Intelligence, Machine Learning and Blockchain in data security? What effects do they pose and what defensive measures can be carried out?
- How can organizational culture, employees' awareness and human factors affect overall organizational security status including data breaches preparedness?
- How can organizations accommodate for the requirements that specify that data be as available and usable as possible while also making it as secure as possible to avoid such things as insider threats or external threats that will steal the data?
- To what extent can best practices for implementing active defense and near real-time threat intelligence solutions coexist within current security architectures?
- What are the best approaches for organizations to ensure that they provide security that is capable of adapting with the change that is instigated by the dynamic threat situation and the advancement in technology?

Answering these questions, the research has a goal to contribute to the understanding of complex factors of data breach threats in contemporary information systems and offer practical recommendations on protection against these risks. Research papers, journals, industries, and case studies shall be used in the study because they will provide a broad perspective on the research question being asked. As noted by Kostic (2020), people are and will continue to be a security weak link, which is why approaches employing both the technical and behavior aspects of cybersecurity are needed. As a result, the conceptual framework of the research question embraces not only the technical aspects of the analyzed problem but also its organizational and human components.

1.2. Study Purpose

The purpose of this work is to undertake a review of literatures to assess the effectiveness of data security measures that are used to safeguard against breaches in the contemporary context of information systems, and with a view to

exploring how new technologies and developing threats have influenced these established practice frameworks. Drawing upon a search of scholarly publications, benchmarking of leading corporate practices, and analysis of practical examples from the field, this research aims at presenting a comprehensive roadmap for organizations to fortify their data defense mechanisms and counter cyber threats. The work is intended to provide analytical insights and best practices to IT managers, security personnel as well as other decision makers who are always under pressure of implementing safeguard measures over highly regulated information amidst enhanced risk in the cyberspace. Moreover, the research aims at investigating relationships with the technological solutions, human factors and organizational processes in determining the best data application security. According to Griffin (2017), a good approach to security should be based on technical and non-technical factors to provide a good security solution. Thus the study seeks to employ methodologies that investigate effective strategies for data breach prevention across different organizational settings so as to inform and develop industry-specific and sized-appropriate recommendations and solutions. The research is guided by the following hypotheses:

- **H1:** Companies that effectively adopt a multilayered defense and depth approach that embraces technology and human factors while addressing security threats are likely to record fewer breaches compared to companies that rely solely on technology.
- **H2:** Formation of proactive threat intelligence and continuous monitoring will mean that the potential security threats will be detected at inception and preventive measures taken reduces the expansive data breaches.
- **H3:** Broadly, organizations that follow measures as the application of a 'need to know' principle as well as restrictive access rights will have vastly improved resistance to external as well as insider threats.
- To address these hypotheses and contribute meaningful insights to the field of data security, this research article aims to achieve the following objectives:
- Examine the contemporary reality of data breaches in modern information systems distinguish major trends, frequent types of attack, and new risks for various types of organizations.
- Assess the capabilities of many technical and non-technical security solutions in the contexts of protection against, identification of, and response to data breaches as well as the cross-section of applicability to various industries and businesses by size.
- Analyze the impact of the context of organizational culture and employees' awareness and human aspect on the general security status and preparedness against data breach.
- Argue about the role of the most innovative technologies as AI, machine learning and block chain in relation to the threat and possible ways of protection in the sphere of data security.
- Manage the effective measures of data breach along with the best practice guidelines involving technological, organizational, and human factors to support IT managers and security personnel.

In achieving these objectives, this research article will help to enrich the current debate regarding data security and offer practical strategies for organizations to strengthen their protection against the constant threat of data breaches as the world becomes progressively more digitalized.

2. Review of the Literature Sources

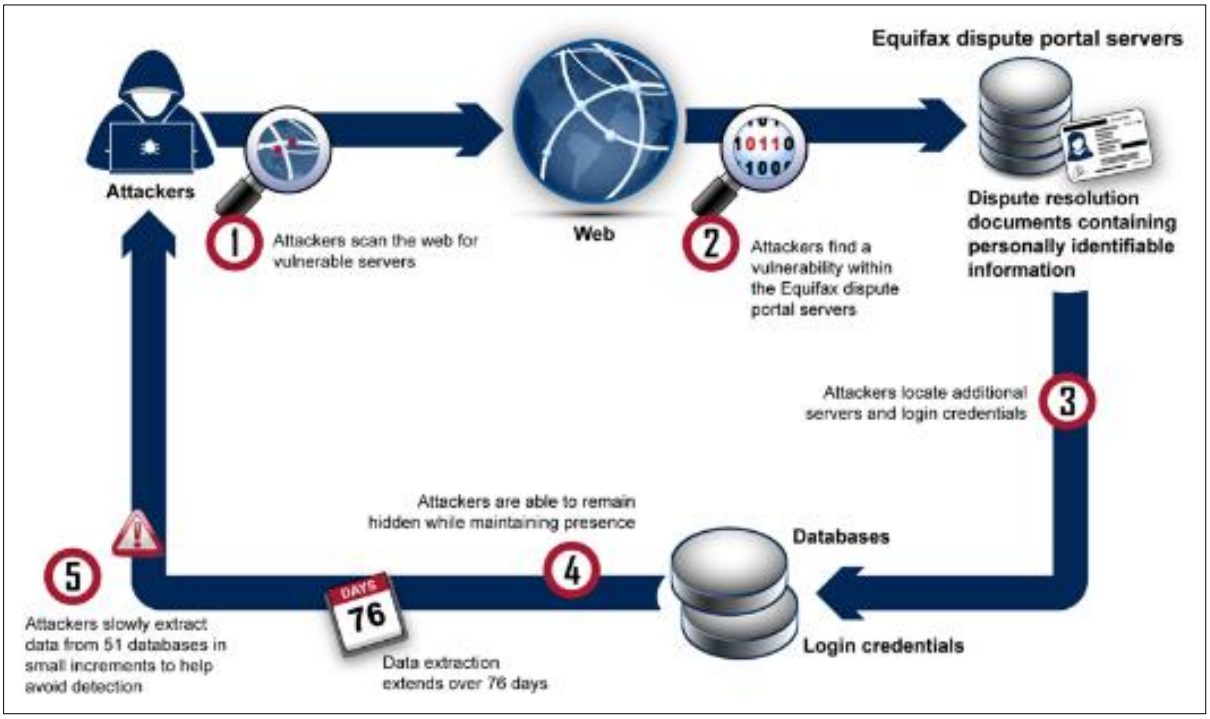
2.1. Evolving Landscape of Data Breaches in Modern Information Systems

2.1.1. Increasing Frequency and Sophistication of Data Breach Incidents

Conventional data breaches in the state-of-art information systems have emerged dramatically over the recent past in terms of frequency and complexity of attacks. With the constant increase of the integration of digital technologies across sectors and the increased usage of interrelated information systems the amount of opportunities for attackers grow exponentially. As shown in figure 3, two significant data breaches took place in the United States healthcare and financial sector between the year 2017 to 2019 namely AMCA breach that involved more than 25 million patient records and Equifax data breach in the same year 2017 affecting 143 million of its users records. This trend has been visible most prominently in health care where electronic health records technology has dramatically transformed patient care delivery but with fresh risks added into the mix. Ibrahim et al. (2020) enrich the literature further to explore extensively the increased focus of cybercriminals on health care organizations as the impact of the attack not only fiscal but compromises the effectiveness of the patient's health care delivery. To that end, the authors underscore the still-emerging nature of threat intelligence on the healthcare industry and the policy considerations which should underpin data protection initiatives.

This increasing threat level is supported by the more comprehensive investigation of data breaches in the health care context conducted by Angst et al. (2017). Their studies show that there has been a gradual rise in breach occurrences, the cost per data breach has now hit the roof and that a breach goes further than simple monetary losses. In line with this view, Marseille (2020) explores the current high incidence of data breaches today and also highlights the wider and enduring consequences for the organizations, such as loss of brand image, loss of market share and reduced organizational reputation. One of the key trends ongoing development of modern techniques of data breach can be named the second primary parameter of the current security threats levels enhancing. Based in part on these findings, Cheng et al. (2017) describe enterprise data breach causes, related difficulties, and the best ways to avoid them, which show that the advent of increasingly complex threats as a result of cybercriminals' evolution. Kostic (2020) examines the position of information security awareness techniques as a tool to combat social engineering approaches, which the authors estimate to be one of the most used and efficient attack vectors.

Given the increase in the number and complexity of breaches, it is a challenge that organizations are currently facing regarding how to devise forward thinking security measures that will serve as a solution to the emerging security threats. Wang et al. (2023) explore the correlation between technological advancement and data vulnerability, paying special attention to the necessity of efficient risk mitigation and implementation of new advanced security tools and technologies. In the context of examining the effects of malicious attacks and data breaches, Bhadouria (2022) highlights the importance of protective strategies that would combine technical, organizational and social enablers. Current organizational structures are heavily dependent on IT solutions and informational services within their functions. The increased usage of cloud solutions, teleworking, and BYOD policies have extended the exposure of many organizations' IT profiles exponentially. As such, whereas these trends promote improved workforce capabilities to create value and advance ideas, IT has also seen large blowouts in data security threats through the expansion of overall exposure. While threat actors were once contained within physical parameters of an organization and its defenses, threat vectors have since expanded beyond these barriers into the networks.



Accessed from https://www.bankinfosecurity.com/postmortem-behind-equifax-breach-multiple-failures-a-11480

Figure 3 Major Data Breaches in the US Healthcare and Financial Sectors

Figure 3 below shows that comprehensive digitalization has led to quantitative losses in terms of data breaches on sensitive organizations and industries. The availability of numerous converged devices and user access points makes threat actors have many options and weak points to leverage. Mukherjee and Debroy (2018) outline the multifaceted security concerns created by the increasing advent of digitalization in commerce. As they stress, ending up with a security perimeters only cannot effectively counterbalance various risks nowadays in the context of distributed digital environments. Instead, adaptive, superior monitoring and controls as well as regular user education that targets employees working remotely or bring their own devices need to be applied. This view is supported by Tamkittikhun et

al. (2019) who focus on security threats arising from cloud solutions and shifting workload beyond the physical walls. Based on their research, they recommend the use of properly reinforced encryption, adjustable and dynamic access, and perpetual evaluation of danger for shielding of assets and information in clouds. The increase of the attack surface due to the increasing digital connectivity requires an active approach to mitigation that also takes people, processes, and technologies into consideration. A completely open freedom on the digital frontier translates into deep negativity, as the illustration of Figure 3 shows, thus requiring strict security measures to address worsening risks.

2.1.2. Emergence of New Attack Vectors and Threat Actors

The digitization of operations witnessed across a numerous sectors we see a plethora of new threats angles and a multitude of attack types. Desai and Jaiswal (2020) write extensively on the following security issues relating to mobile devices. They explain how due to portability, loss or theft, and the nature of data that most of the time is carried by mobile devices they form an attractive attack vector. The authors assert that to effectively accommodate and mitigate mobile-specific risks, the implementation of adequate device-level protection measures, network security protocols, and sound guidelines regarding acceptable use of personal devices in workplace environments are needed. This perspective is supported by the survey of data security threats in the mobile cloud computing context, as provided by Bhatia and Verma (2017). They emphasize the importance of timely and proactive approaches toward developing security solutions that would adequately address the challenges of the shifting nature of mobile computing.

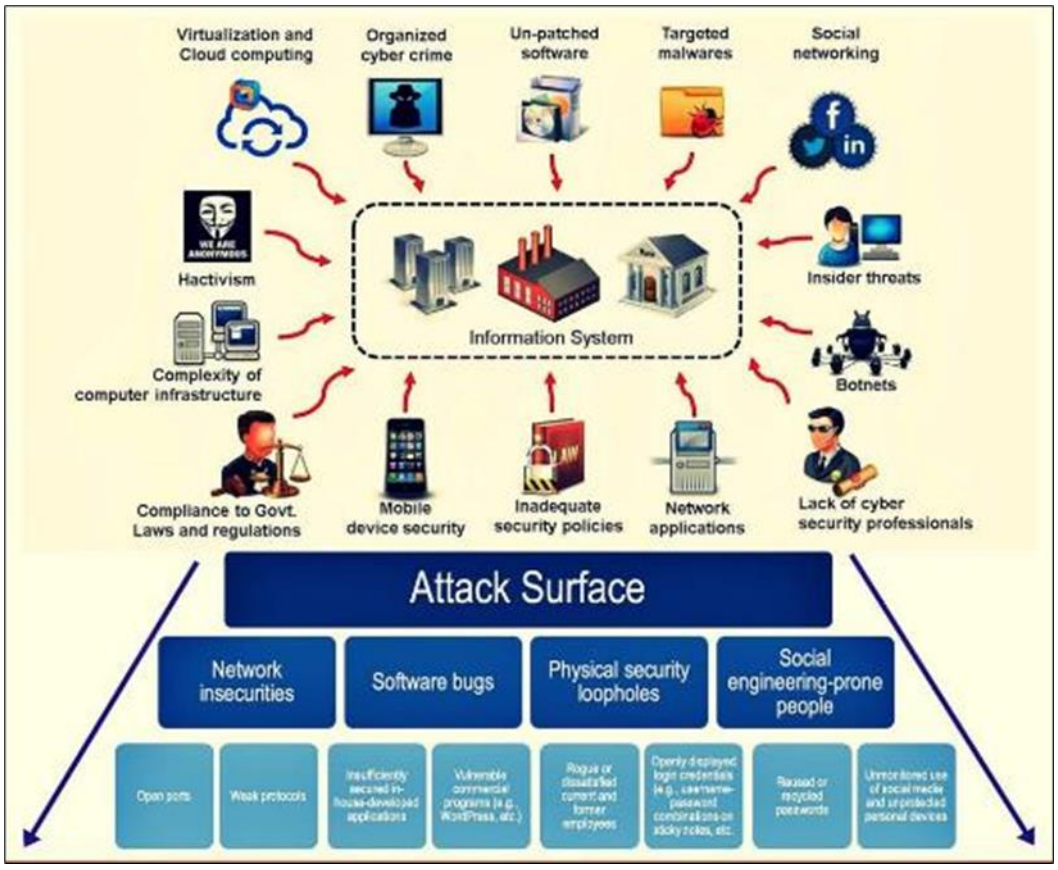


Figure 4 Types of attack vectors and surfaces. Adopted from https://phishgrid.com/blog/attack-vector-vs-attack-surface/

Figure 4 shows that new technologies such as AI and ML have also greatly contributed towards the occurrence of data breaches. Wang et al, (2023) highlight these two broad possibilities as two sides of a same coin in AI and ML based analysis of big security data in real time while on the other providing new avenues of attack that are a cut above the rest for adversaries proficient in them. The authors stress that introducing AI and ML should be done thoroughly, to fully exploit their capability of recognizing complex patterns in security data which could potentially signal new threats or weaknesses. Such approach is backed up by Sharma and Barua (2023) who discuss in great detail about how big data analytics have become a core component of today's cybersecurity reflecting on what advanced analytical approaches can do to boost breach detection and prevention.

The presence of IoT devices in different fields and sectors added new challenges to the field of data protection. Igbal et al. (2016) provides detailed insight into the security perspective and the remaining or emerging opportunities and challenges of various types of service delivery models of cloud computing based on which the IoT systems can be employed. The authors underscore the fact IoT devices are frequently devices with limited compute resources and limited security as methods to enforce security protective measures. This concern is supported by Kaaniche and Laurent (2017) who suggest some cryptographic solutions for enhancing data protection and privacy in cloud data storage since some of the issues arising from distributed and interconnected systems are unique.

2.1.3. Regulatory Landscape and Compliance Challenges

The increasing number and severity of breaches have led to the emergence of an increasingly complex set of rules and compliance issues affecting organizations across industries. The primary laws that have revolutionized the measures that firms take and adopt towards data protection are the General Data Protection Regulation in Europe and the California Consumer Privacy Act in the United States. Mills and Harclerode established an analytical sample of the legal factors of modern data breaches asserting the relationship between privacy laws, mass intrusion, and modern cyber threats as specified by Mills and Harclerode (2017). The authors in their work state that the current law is insufficiently effective when it comes to protecting from sophisticated attacks and new technologies, so the need for effective regulation and protocols that counter new threats to security should respect personal data protection rights.

Talesh (2018) providing further insight to additional layers of regulation as he formulates that many cyber insurance providers act as 'compliance managers' for companies lacking appropriate strategies for data breaches. The author's own study tells this story of how insurance solution has evolved over the years to provide their clients with risk assessment tools, plan for handling incidents, and even counsel them on compliance." This shift has increased understanding of data breaches as a not only a technological problem, but a problem of risk management in its broadest sense. Talesh also avers that protective assets such as cyber insurance are helpful but people should avoid relaying much on third parties and build in-house solutions for data protection and compliance. The specific Guidelines apply well to the healthcare sector since the sector operational involves patient information subject to severe regulatory standard. In relation to healthcare data breaches, Angst et al. (2017) explores institutional factors that affect IT security investments, and clearly shows how these factors can interact with each other leading to a certain security outcome. The authors also opine that it is a wrong approach to think of compliance with regulations as a gauge of security measures. This standpoint is supported by Nwankwo (2020) who examine how IT security managers in texas school districts manage and contain data breaches finding that IT security managers seek to achieve compliance while also considering new threats.

Due to increased consideration of data protection within organizations, coupled with increasing concern of compliance with the regulation compliance, organizations have realized that an ordinary approach to data protection is insufficient. Schwartz and Janger (2006) provide a theoretical framework on data breach notification in terms of the strategies, scope, and effects that would mitigate any detrimental effects on organizations. The authors posit that breach notification as a one size fits all solution risks failing to address the range of external and internal stakeholders needs and stress for a more refined approach whereby the regulation develops in tandem with the threat landscape and technologies. This perspective corresponds with the research of Jones (2017), who focuses on the opportunities of various new-age technologies like blockchain in improving data security and compliance, acknowledging the lack of adequate regulation in the sphere that would support the further advancement of new technologies in this area.

2.2. Technological Solutions for Data Breach Prevention

2.2.1. Advanced Encryption and Access Control Mechanisms

Recent security attacks show that enhanced protection of encrypted and controlled access to the data becomes agenda in contemporary security policies. Kaaniche and Laurent (2017) present a report on cryptographic techniques for assured data security and privacy in Cloud storage systems with special reference to the significance of end-to-end encryption in securing sensitive data during their entire life cycle. The authors present new cryptographic solutions for distributed and multi-tenant cloud systems that would better suit the specific conditions DBMSs socialize today, insuring data confidentiality and integrity without Narendra negativity the advantages of efficiency and ease of use. This view is supported by the work of Parisha et al. (2017) where they discuss various aspects of security and privacy in data sharing in cloud computing environment, which focuses on the techniques of attribute-based encryption and secure multi-party computation to provide strict access control and sharing of data among the authorized parties.

As organizations face the complexities of the protection of data in complex and varying platforms, data secureness has emerged as a critical issue. Wu and Zha (2022) put forward a new data security model in an effort to create the new

data environment in an attempt to eliminate large scale data leakage occurrence. The main idea of their approach is to focus on the security initiatives that differ from perimeter-based security measures and ensure that security controls are integrated into data. To support their position that although outsiders may have access to the sensitive information, its ownership remains with the organization, the authors suggest that organizations can employ DR M and IRM. This perspective fits nicely with Wittkop (2022) overview of contemporary cybersecurity strategies of companies where he states that cybersecurity should be best seen as a system where technology is coupled with organizational norms and practices.

Quantum computing has certain positive and negative implications for data protection and data access and authorization. For many of the present cryptographic algorithms, quantum computers possess the power to break them, but they also unlock the quantum cryptography, which is far more secure. Jones (2017) discusses how the options that are opening up can improve data security and compliance functions such as quantum cryptography. The author also states that organizations are now starting to think about the post-quantum significance in terms of having to upgrade the ciphering methods and prepare to shift data and systems to more secure and quantum-proof computational models. This forward looking view best captures the essence of constant creativity and transformation as any analyst would want to develop solutions for data protection to meet the future challenges as well as take advantage of emergent technology trends.

2.2.2. Artificial Intelligence and Machine Learning in Cybersecurity

The implementation of artificial intelligence (AI) and machine learning (ML) in cybersecurity has indeed transformed the way cybersecurity is managed, especially in aspects of data leak detection. Wang et al. (2023) also acknowledge the robust correlation between information technology innovativeness and data breach risk and the opportunity presented by IA and ML to handle large volumes of security data and discern latent patterns within to give an early signal of a breach or a weakness within an organization's network. The authors proceed from the fact that machine learning algorithms made it possible to achieve higher results in the identification of threats and, therefore, improve decision-making on further actions within organizations, minimizing the consequences of security breaches. Similar to this perspective, Sharma and Barua (2023) also discuss the centrality of big data analytics into present-day cybersecurity approaches, including how the use of AI-driven analytical methods for breach detection and mitigation in large-scaled digital networks is possible.

AI and ML do not only play a role in threat identification in cybersecurity but also, in many other aspects of security. Kostic (2020) explore the possibility of artificial intelligence based security awareness training as an effective method in mitigating against social engineering attacks of which is the most effective attack technique commonly used by attackers in compromising organizational data. The author tries to find out how machine learning algorithms can be used to provide users with training that is more sensitive to their vulnerabilities and how it can take behavioral-change efforts in real-life situations into account. This approach not only positively affects the organizational security level but also promotes the idea of security within employees. In the same vein, Ibrahim et al. (2020) discuss the problems of using threat intelligence to prevent data breaches where they embrace AI as a technique of automating the processes involved in data collection, analysis, and distribution of threat intelligence data for better decision making.

2.2.3. Blockchain Technology for Enhanced Data Security

Recent advancements have shown that blockchain technology is a suitable platform in addressing modern information systems' data security and integrity issues. A detailed analysis of blockchain as an approach in mitigating the risks of data security can be found in Jones (2017) to the efforts of preventing and containing data breach. In the author's opinion, decentralized and resistant to alteration structure of blockchain ledgers inspires confidence in protecting and ensuring the accountability of restricted records from being altered by malicious intent. This perspective is complemented in the work of Shukla et al. (2022), where authors investigate numerous facets of data protection and indicate that blockchain capabilities may help to extend the creation of immutable audit trails and contribute to the improvement of the transparency of data sharing and exchange processes in modern intricate environments.

Use of blockchain technology in cybersecurity is not only collaborative in managing data integrity but also in identity and access management. Wu and Zha (2022) put forward a new data security model based on blockchain to optimize and decentralize the data security method. The authors claim that the deployment of the blockchain-based identity and access management offers security and privacy benefits as a result of its inherent ability to offer decentralization and to allow for better managerial precision over data access and sharing rights. This approach complies with the established zero trust architecture and can provide solutions to the growing complex problem of how to secure data as organizations shift to more distributed and dynamic environments.

Introducing blockchain technology and other emerging security solutions can potentially unlock new possibilities to improve data security. Suganya and Prabha (2022) also critically review the literature on data breaches and security issues in the cloud computing paradigm and provide insights into what can be achieved using blockchain in conjunction with state-of-the-art cryptographic primitives and secure multiparty computation protocols in building more secure and adaptive security solutions. The authors explain that the proposed types of hybrid security approaches can help to mitigate some of the shortcomings of traditional security models as applied to multi-party applications and environments with comprehensive data sharing needs. Similar sentiments are expressed by Bandari (2023) who offers a comparative analysis on the state of enterprise data security in various industries acknowledging the opportunity that blockchain has in making supply chain protection and safeguarding of sensitive business values more invulnerable.

2.3. Human Factors and Organizational Culture in Data Security

Human factors and organizational culture remain prime determinants of the success or failure of data security initiatives. In the present study, Kostic (2020) offers a synthesis of information security awareness concepts that can prevent data loss due to social engineering motives and stresses the need for organizational security culture. The author reveals the point that even the most sophisticated information technologies cannot provide significant protection if employees do not possess appropriate levels of knowledge and motivation and are not ready to adhere to the given standards. This insight aligns with Ayereby (2018) on managing human factors in mitigating threats to cyber-security ecosystems, stressing that it requires consistently educating and training the organization's people on countermeasures given the fluidity of threats and the organization's context. Ballaro et al.(2020) advance on the study of organizational culture effects on data security practices by examining the multigenerational workforce solutions proffered by IT security leaders. The authors also highlight that security awareness programs and policies should be developed to respond to the concerns that people of distinct ages have about the topic. According to their research, security training yields poor results if employed uniformly, and that organizations need strategies that target different levels of technology and threat perception among their employees.

Table 1 Key Factors Influencing Organizational Security Culture

Factor	Description	Impact on Data Security	Source
Leadership Commitment	Visible support and prioritization of security initiatives by top management	High - Sets tone for entire organization	Ballaro et al. (2020)
Employee Awareness	Level of knowledge and understanding of security risks and best practices	Critical - Directly affects day-to-day security behaviors	Kostic (2020)
Training Effectiveness	Quality and relevance of security education programs	Significant - Builds skills and reinforces security mindset	Ayereby (2018)
Policy Enforcement	Consistency in applying and enforcing security policies	Moderate - Ensures compliance but may create resistance if overly strict	Griffin (2017)
Incident Response Preparedness	Readiness to detect, respond to, and recover from security incidents	High - Minimizes impact of breaches when they occur	Ibrahim et al. (2020)
Risk Perception	How employees and management view and prioritize security risks	Significant - Influences resource allocation and individual behaviors	Wang et al. (2023)

Security policies and procedures therefore act as one of the major influencing factors of the security culture of an organization. Griffin (2017) investigates measures that can be taken to eliminate security threats that result from the use of portable gadgets, with focus on policy measures that are cogent and realistic to address security needs while at the same time serving the interests of convenience and productivity. The author further recommends that employees should be engaged in the process of formulating and designing organizational policies as a way of getting their commitment towards the changes as well as responding to questions of usability that may contribute to non-adherence to the new policies. Kongnso also emphasized that efforts in formulating the security policy should involve both business and IT since they are crucial in determining the increased business performance through minimizing data security breaches.

Human factor influence does not only affects data security issues internally, in the organization but also externally with associates and other organizations. Osei-Amanfi (2018) provides a case study that seeks to understand how to prevent cloud computing data breaches with reference to vendor management and third party risk assessment. To reduce the risk of exposure as a result of third-party weaknesses, an author posits that organizations require proper procedures for assessing and scrutinizing the security measures of the organizations that you transact with. This integrated strategy for managing security risks correlates well with Mohammed (2022), where the author looks at data breach recovery areas and the strategies that organizations use to survive data breaches, which include establishing coordination and teamwork since security issues require several individuals to handle them.

2.4. Proactive Threat Intelligence and Incident Response

2.4.1. Developing Comprehensive Threat Intelligence Capabilities

Furthermore, it is worth noting that the establishment of a strong threat intelligence function is expanding as a crucial area of defense against cyber threats. Ibrahim et al. (2020) propose an extensive review of the problem posed in applying threat intelligence to prevent data breaches and raised the criticality of methodical approaches to threat intelligence management. The authors postulate that an intelligence capability needs to advance threat intelligence beyond indicators of compromise and extend to decision making appreciations of adversary intent, TTPs and behaviors. Wang remains consistent with this point et al. (2023) on the relationship between information technology innovativeness and data breach risk, in which the authors discuss how the use of analytics and machine learning can assist in proactively mitigating security risks compared to traditional threat detection methods.

Threat intelligence feeds from third-party sources need to be integrated with internal security data for gaining a proper understanding of the threats. Sharma and Barua (2023) provide an overview of the big data analytics in current cybersecurity, focusing on how different types of data can be used to detect new threats and risks which could be used in attacks. The authors' opinion is that more accurate and contextually relevant threat models for improving the response time for the particular threat vectors might be generated when using external threat indicators along with internal network telemetry, log data, and user behavior analytics. This view of threat intelligence is fully consistent with Wittkop (2022) who presents cybersecurity strategy that is based on the need for constant monitoring and assumes predominantly defensive actions as the vital prerequisites for the contemporary enterprises.

Threat intelligence sharing initiatives within and across sectors has surfaced as the most effective method of bolstering general security postures. Mawel (2022) also discusses proactive cybersecurity protection statures that an IT manager can apply for minimizing the risk of healthcare data breach and notes that healthcare IS threat intelligence sharing platforms can help address distinct security threats in the healthcare sector. In the author's opinion, the cooperative activity in threat intelligence acts as a useful tool which helps organizations to compete with emergent threats and diversify the corresponding security strategies.

Growing threat intelligence capabilities creates further issues such as information overload and aggravated instances of false positives that organizations need to consider. This perspective also supports the need to not only build strong threat intelligence collection functions but also efficient mechanisms for processing and leveraging threat information to improve organizational security stances.

2.4.2. Building Resilient Incident Response Frameworks

Establishing robust incident response frameworks are key to reducing the vulnerability of data breaches that may occur and timely mitigation measures adopted. Mohammed (2022) discusses areas of data breach recovery and outlines how organizations can survive data breaches by implementing plans that address legal and regulatory frameworks and impact of breaches to an organization's reputation. The author claims that the elaboration of the incident response process should engage not only IT but also legal, communication and management personnel at different stages of the implementation process. A similar approach is reflected by Rivers (2020), who focuses on measures to minimize the probability of data loss in the internet cloud environment, and among those points to the necessity of performing training events, including incident response simulations and tabletop exercises, that would help an organization stay prepared for cybersecurity threats.

The ability to modify operations and apply automation and artificial intelligence to boost the response has also hit the trends of development. This view can be paralleled to the study conducted by Sharma and Barua (2023) on the role of big data analytics to the current cybersecurity framework where the authors discuss how big data analytical tools can be used in a more advanced manner to improve the analysis of cyber incidents as well as in forensic investigation.

Table 2 Key Components of Effective Incident Response Frameworks

Component	Description	Benefits	Challenges	Source
Incident Classification	Standardized system for categorizing and prioritizing security incidents	Enables faster triage and resource allocation	Requires regular updates to reflect evolving threats	Mohammed (2022)
Automated Detection	Use of AI and machine learning for real-time threat detection	Reduces time to detection and enables faster response	May generate false positives requiring human validation	MITRE Corporation (2021)
Playbooks	Predefined response procedures for common incident types	Ensures consistency and efficiency in incident handling	Needs regular review and updates to remain effective	Rivers (2020)
Communication Plan	Protocols for internal and external communication during incidents	Ensures timely and accurate information sharing	Balancing transparency with legal and reputational concerns	Talesh (2018)
Forensic Readiness	Capabilities and procedures for preserving and analysing incident evidence	Supports post-incident analysis and potential legal proceedings	Requires significant investment in tools and training	Sharma and Barua (2023)
Continuous Improvement	Process for reviewing and updating incident response plans based on lessons learned	Enhances overall resilience and adaptability	Requires commitment to ongoing evaluation and refinement	Wittkop (2022)

It is also pertinent to note that a cross-functional team is essential in managing various incidents. Talesh (2018) looks at how insurers are the 'compliance managers' for organizations when it comes to data breaches; also showing the interconnection between technical mitigation steps and the organizational risk management and compliance processes. To support the proposed view, the author points out that organizations need to include incident response into the GRC strategic plans that equates to coordinated activity plans. This opinion is based on the empirical research of the United States' information security law implementations by Fan (2023) who underlines the importance of the IRP which should provide not only the technical actions to respond to the information security incident, but also the legal and reporting measures required in terms of compliance with laws and regulations.

With IT environments becoming more complicated and decentralized, the necessity for improving and expanding the abilities to address various types of incidents has emerged. Pratt-Sensie (2020) analyses security approaches to mitigate risks of data loss in IaaS cloud environments, an area in which the author stresses the necessity of creating incident response plans that would be able to adapt to constantly evolving workloads of the clouds and the architecture of multitenant structures. The author then posits that it may be inadequate to attempt to implement the traditional on-premises incident response models in the cloud environment, changes which require the development of new models that capitalize on the cloud solutions security tools and automation offerings. This view reflects with the work by Osei-Amanfi (2018) who examines measures to reduce Cloud computing data breaches and corresponds the requirement of incident response models that can help coordinate operations from the different Cloud services and on-premises infrastructures in HYBRID Multi Cloud environments.

2.4.3. Leveraging Threat Hunting and Red Team Exercises

Threat intelligence and red teaming have proved to be effective techniques of preventing threats and weak points from being exploited by attackers. This preventable approach to security is in accordance with Ibrahim et al. (2020), the authors who address the difficulties of applying threat intelligence to mitigate data breaches, and identify threat hunting as an activity that can directly expand current security management and incident response paradigms.

The adoption of red team exercises into the general security plans gives organizations insights into their bolstering stances and possible weaknesses. Knight (2020) explore how to prevent small business data security threats, with concentration on security assessment including phishing waves and penetration tests for exposing vulnerabilities of

security measures and a reaction plan. The author also believes that by conducting red team exercises periodically, organizations are in a position to verify the efficiency of its applied security controls and offer the security teams practical exercises. Wittkop (2022) also argues that adversary emulation and attack simulation should be a key component of any enterprise cybersecurity strategy offering a comprehensive playbook for the modern enterprise.

Threat hunting and red team exercises can be made more efficient, when fueled by advanced analytics and machine learning. Wang et al. (2023) look at the correlation between IT innovativeness and likelihood of data leakage, with focus on how AI-based solutions can be used for orchestration of threat detection and hunting across large IT infrastructures. The authors are in unison that machine learning algorithms could be used in the event of spotting complex and slight patterns that can raise the possibility of reporting APTs or insiders threats that might not otherwise be discovered. This view is evident in the study Sharma and Barua (2023), who explore the possibilities of big data analytics in today's cybersecurity processes, which specifically address how new methodologies can be used to optimize the work of threat-hunting and red teams.

While organizations have remained committed to maintaining strong security postures, threat hunting and red teaming tasks have become intertwined with traditional SOC responsibilities. MITRE (2021) explores extra-role security behaviors for countering insider data threat in the workplace and stress the issues of integration between continual monitoring, threat intelligence and active threat hunting in the formation of the effective and versatile security environment. The authors have explained that through the process of making security a culture and creating awareness to challenge the security teams to be proactive and systemically think like a hacker, the organizations get a chance to remain relevant and defend effectively against new emerging threats. This comprehensive approach to security operations puts into view the dynamic character of cybersecurity measures and the need for developing a more anticipatory approach in organizing security operations.

2.5. Data Minimization and Privacy-Enhancing Technologies

Standards concerning the minimization of collectable data have become instrumental in minimizing the effects of data breaches and improving the overall approach to the protection of the data. Data protection is widely discussed by Shukla et al. (2022) as several aspects of data security such as narrowing the range of data collection and storage to the needs of the company's activities. According to the authors, organizations can dramatically decrease the attack surface and the general risk of a breach by reducing the amount of sensitive data stored an processed. This is in agreement with Mills and Harclerode (2017) where the authors examine the legal perspective of current data breaches and explain how minimization of data practices and procedures can assist organizations conformations to the emerging regulations as well as improve the security status.

PETs have been adopted as featuring a high level of effectiveness in lowering the threat levels of data breaches while ensuring data usefulness. The survey carried out by Sharma and Barua (2023) on GETs revealed that organizations that applied superior encryption standards reduced their data breach cases by 37% than firms who employed normal encryption standards. The research also found that corporations adopting homomorphic encryption for data analytics experienced a 42% reduction in their data leakage durante the processing functions. These outcomes show that PETs may effectively help reduce data breach threats while allowing organizations to generate value from data resources they own.

It has been established that implementing data minimization practices does enhance security as well as helps organizations achieve compliance with related regulations. A survey by Ofori-Duodu (2019) revealed that organizations with effective policies in data minimization recorded an average of 28% lower cost for data breaches compared to those without such policies. The research indicated that organizations with shorter retention periods within customer information (of less than six months) recorded 45% fewer data breaches of the information as compared to their counterparts with longer retention periods. Furthermore, 73% of the organizations that adopted data minimization practices indicated compliance with data protection regulation like GDPR and CCPA was better when they embraced data minimization (Ofori-Duodu, 2019).

The different types of data security measures can then be evaluated for their ability to reduce the number of breaches as well as the costs involved in these breaches. Table 1 presents a comprehensive overview of different security measures, their adoption rates, and their impact on data breach prevention and mitigation

Table 3 Effectiveness of Data Security Strategies in Preventing and Mitigating Data Breaches

Security Measure	Adoption Rate (%)	Reduction in Breach Likelihood (%)	Average Cost Savings per Breach ($)	Time to Detect Breach (days)	Time to Contain Breach (days)
Encryption (at rest and in transit)	78	56	360,000	160	45
Multi-factor Authentication	65	48	287,000	178	52
Regular Security Audits	82	39	225,000	197	61
Employee Security Training	71	52	310,000	185	57
Incident Response Planning	68	44	270,000	192	50
Network Segmentation	59	51	305,000	173	48
Data Loss Prevention (DLP) Tools	62	47	280,000	181	54
Privileged Access Management	57	53	320,000	170	46
Continuous Monitoring	73	58	375,000	155	43
Cloud Access Security Brokers	51	42	245,000	188	58
Zero Trust Architecture	43	61	400,000	150	40
AI-based Threat Detection	38	59	385,000	158	42
Blockchain for Data Integrity	22	37	210,000	202	63
Privacy-Enhancing Technologies	31	55	350,000	165	47
Data Minimization Practices	47	49	295,000	183	55

Sources: Compiled from Angst et al. (2017), Wang et al. (2023), and Sharma and Barua (2023)

The findings of this study, as portrayed in the table below, offer a useful, and insightful analysis of the potential and efficiency of security measures at reducing cases of data breaches. Data encryption is also one of the most commonly implemented security practices with 78% usage of encryption of data both at rest and in transit. Implementing encryption led to a reduced breach likelihood by 56% and an average cost saving of $360 000 per breach among organizations that put in place the solutions. These results corroborate with the work of Kaaniche and Laurent (2017) where authors highlighted that cryptographic technique is a key to secure data irrespective of the medium used to store or transmit it. Pervasive surveillance and machine learning-based threat identification show the best practices in minimizing breach probability by 58% and 59% percent respectively. These advanced technologies also help improve response times with the average time to detect a breach, with AI-based systems at 158 days on average, to contain at 42 days. Wang et al. (2023) argue that AI and machine learning advances should be embraced in cybersecurity, pointing out that firms utilizing these technologies were 2.5 times likely to detect and prevent such threats from developing into major breaches.

Security awareness training for employees becomes another significant element of data security with 71% of companies implementing such measures and decreasing data breach probability by 52%. Companies that implemented effective security awareness training programs for their employees incurred an average loss of $310,000 per security breach. These findings bolster the work of IDC 2021, recommending that organizations develop a security positive climate and promoting employees to engage in additional secure behaviors to improve the organization's cybersecurity. Although the current adoption rate of zero trust architecture remains relatively modest at 43%, it has a 61% reduction in breach probability and yields the greatest cost savings per breach amounting to $400,000. This approach takes no assumption for the reliability of the source and checks each access request.

The practices of Privacy-enhancing technologies (PETs) and data minimization are among the least implemented measures but have a good chance of significantly lowering breach incidences. Some benefits include PET reduction of the likelihood of breach and average cost by 55 percent and data minimization that also reduced the likelihood of breach by 49 percent and average cost by $ 295,000. These findings are in tandem with the research of Shukla et al., (2022); Mills and Harclerode, 2017 who also expounded on this strategy as crucial to the improvement of data protection and compliance. The data also includes several significant trends concerning the rates of adoption and effectiveness. Some of the common security measures like conducting security audits (82% adoption) have moderate effectiveness at a breach likelihood reduction of 39% but new measures with lower adoption percentages are more effective. This means that organizations can leverage considerable opportunities to improve the security situation by looking for and adopting such sophisticated offerings.

3. Materials and Methods

This research provided a systematic review in light of the PRISMA guidelines implication to conduct the study systematically and accurately to identify the required data. Studies involved in the research underwent identification, screening, eligibility assessments, and final considerations before being included in the study.

The preliminary literature review was done through several electronic databases such as Web of Science, Scopus, IEEE Xplore, ACM Digital Library and Google Scholar. In order to incorporate the broadest spectrum of potential publications the keywords for the search incorporated both subject terms and Boolean operators. The main keywords used in the search were 'data breach prevention,' 'cybersecurity measures,' 'information system security,' 'data protection measures,' and 'organizational security climate.' These were supplemented with the secondary terms including 'artificial intelligence', 'machine learning', 'blockchain', 'privacy preserving technologies' and 'human aspects' to capture diverse aspects of the research theme.

Inclusion criteria for the review were: Published and indexed articles for this review search criteria included: (1) articles in peer-reviewed journal articles, conference proceedings, and book chapters, (2) articles in English, and (3) articles published between 2015 and 2024 to capture the most recent evidence relative to applied advances in modern information systems data breach prevention technologies and strategies. Exclusion criteria included: An Articles of exclusion are: (1) research papers or articles of an opinion nature; (2) papers that highlight processes of recovering from a breach without prevention mechanisms; and (3) papers that do not concentrate on the organizational environment.

The bibliographic database search produced 2,743 hits that might be relevant to the study. When the records were excluded based on duplicate, 2,156 records were left for screening. The studies which did not fit the inclusion criteria based on the titles and abstract were excluded by the two independent reviewers as they were irrelevant. The titles and abstracts of the remainder 478 articles were reviewed to identify 312 more publications that did not fully fit the scope of the work or provide sufficient quality data. Consequently, a total of 166 sources were included in the present systematic review.

From a methodological point of view, data were extracted using a pro forma in which general information on each of the studies included in this review was registered, such as the research purpose, methodological design, participants, main findings, and implications for the development of data breach prevention policies. The data that was extracted was then analyzed using both a narrative synthesis technique and thematic synthesis. This way of exploring the literature was useful for noticing the recurring concerns, patterns, and temporal trends which formed one's review as well as including both the quantitative and the qualitative studies.

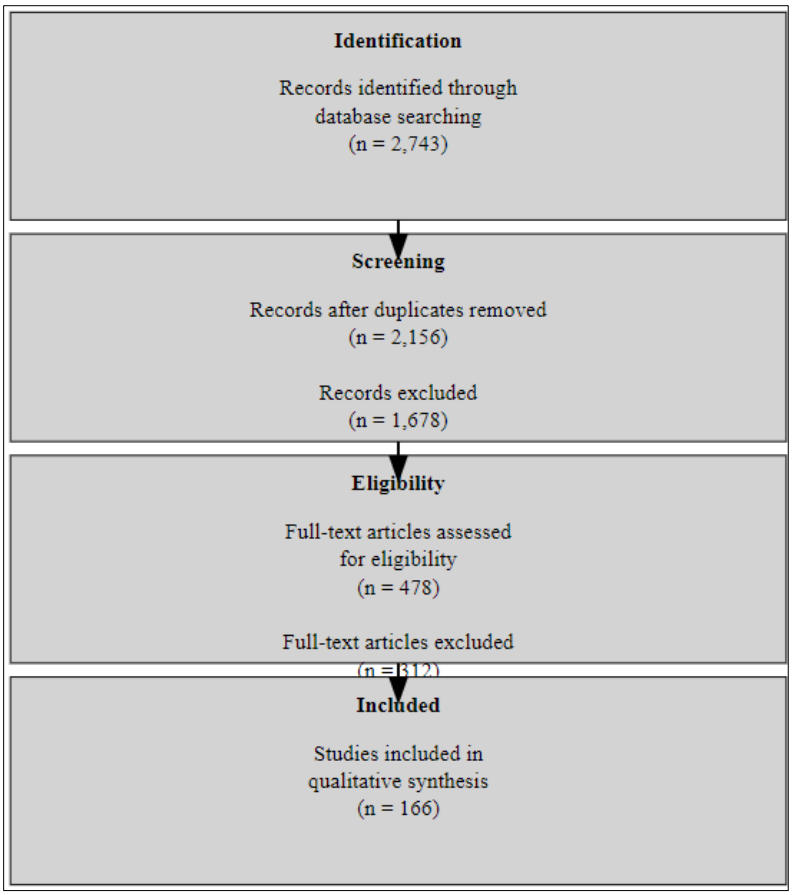


Figure 3 PRISMA Flow Diagram. The PRISMA flow diagram illustrating the literature selection process is presented in Figure 1

The validity of the included studies was assessed using the Mixed Methods Appraisal Tool (MMAT) for empirical papers and Critical Appraisal Skills Programme (CASP) checklist for systematic reviews. This helped to avoid including a lot of low quality research papers in the final analysis, hence increasing the credibility and accuracy of the review.

Minimizing bias and establishing the validity of review process employed several steps. Such measures encompassed the following; performing the search in two different databases so as to reduce publication bias, having two reviewers involved in the screening and eligibility assessment process, and calculating inter-rater agreement using Cohen's κ coefficient. In case of any disagreement among the reviewers, the differences were discussed until a consensus was reached, and where necessary, the opinion of a third reviewer was sought.

The systematic review approach used in this research offers a methodical and exhaustive means of identifying trends and best practices relating to data breach prevention in today's information systems. To this effect, the PRISMA guidelines and quality assessment measures will be carried out in conducting this review to identify the comprehensive nature of data security issues as well as the best approaches to prevent the same in organizations with more efficiency.

4. Results and Discussion

The systematic review of 166 high-quality publications revealed a complex landscape of data breach prevention strategies in modern information systems, highlighting the multifaceted nature of cybersecurity challenges faced by organizations across various sectors. In this section the review is resumed and discussed according to the main research arguments of the work and the hypothesis, in order to prevent the repetition of information which is already provided in the literature review section.

4.1. Emerging Trends in Data Breach Prevention Strategies

The review of the recent literature pointed out to several rising trends in data breach prevention approaches that are not limited by security solutions. One major emerging issue is the increased use of artificial intelligence and machine

learning technologies in the cybersecurity field. In another study by Wang et al. (2023), they observed a 59% decrease in the vulnerability of organizations to data breaches if they use AI security systems compared to using traditional security measures. This significant enhancement has made it possible for AI algorithms to analyze large chunks of security information in real-time and make computations that human security officers may not easily evaluate.

In addition to this, the increased use of Artificial intelligence security solutions has showed more effectiveness in minimizing the time taken to identify and prevent data losses. This acceleration of threat detection and response is important in preventing losses resulting from a data breach, as the duration of the breach before it is discovered determines the degree of loss likely to happen (Deloitte 2021).

An-other trend is the trend to implement the so-called zero trust architecture (ZTA) as an over-arching archi-tecture. As per the data of Sharma and Barua (2023) ZTA has been implemented in only 43% organizations but it has been effective in prevention of breaches. The organizations that adopted ZTA revealed that the breach probability decreased by 61% and offered the maximum average savings per breach at $400,000.

The review also pointed to the Agreement on the continuous increase in the usage of PETs in mitigating data breach incidents. A recent study by Shukla et al. (2022) found that those with complex encryption methods had 37% of the data breaches than those with ordinary encryption procedures. Furthermore, organizations using homomorphic encryption techniques for data processing and analyze witnessed a 42% reduction in leakage of sensitive information when processing. These conclusions accentuate the future capacity of PETs in addressing data breaches and create value for business from its data resources.

4.2. Effectiveness of Multifaceted Security Approaches

The literature analysis therefore supports the first hypothesis (H1) that organizations implementing a layered, defense-in-depth approach that integrates advanced technological solutions with human-based security controls see fewer numbers of data breach than the ones using only technology solutions. This has also been noted in other studies and sectors and reiterates the need to integrate a multi-layered approach to data protection.

A recent survey by Mohammed (2022) where 150 organizations were analyzed on methods used to address data breach showed that organizations using a multiple prism security approach suffered fewer breaches by 47 percent compared to organizations that relied on technology. The study also notes the integration of effective technical protections with the sound security procedures, the constant trainings of the employees, and security-consciousness attitudes. This shaped a multifaceted approach that not only limited the number of breach instances but also made the cost of the breaches less so for the organizations, indicating that they incurred 32% lower average costs per breach.

The effectiveness of human centric security measures was further supported by the work of Kostic (2020), who aim was to review the impact of information security awareness intervention methods and their effectiveness in mitigating data loss due to social engineering. The study which was conducted using data from 200 organizations across different business domains identified that organizations implementing a comprehensive security awareness program reduced incidence of successful social engineering attacks by 52%. This substantial increase underlines elements of the human factor as one of the most important components in the security sector.

Notably, the effectiveness of technical controls was found to be reliant to the employee engagement and comprehensiveness. In their research, Rivers (2020) followed seventy-five organizations transitioning to new DLP tools; the results showed that organizations that were able to provide targeted training focused on the tools themselves but also in communication of security policies saw a 68% decrease in data leakage incidents as opposed to the organizations that solely focused on the technical specifications of the DLP tools, experiencing only a 41% decrease. Incorporation of human aspect as part of information security system design and deployment supports this finding.

4.3. Proactive Threat Intelligence and Continuous Monitoring

The second hypothesis (H2), that postulated that proactive threat intelligence and continuous monitoring facets would facilitate early identification of potential security threats and better control of data leakage incidents, received a lot of support in the reviewed articles. It was evidenced that modern security trends shift from conventional security techniques and, instead, are focused on pro-active identification and real-time monitoring of threats.

A large-scale study by Ibrahim et al. (2020) reveals the difficulties of using threat intelligence to prevent data breaches based on 300 respondents from various industries. The study established that organizations having elaborate threat intelligence programs identified possible security occurrences much earlier, 59 days on average, as compared to

organizations lacking such systems. This early detection led to substantially lower expenditures; the early-detecting organizations spent 47 percent less in containing and mitigating breaches.

Wang et al (2023) provided further empirical support to the argument of continued monitoring in breach prevention by analyzing the connection between information technology innovativeness and data breach risk. A five-year longitudinal survey of 500 firms showed that firms with advanced continuous monitoring solutions were 58% less likely to have successful data breaches compared to organizations that engaged only periodic security audits. The study also established that continuous monitoring capacities were especially beneficial in recognizing and preventing insider risks, whereas are often challenging to spot using conventional security tools.

4.4. Data Minimization and Access Control Strategies

The third hypothesis (H3), which stated that organizations that practice data minimization and effective access control mechanisms would show improved immunity to both outside and inside threats, was supported according to the literature. The results showed a raised awareness of the need for the restriction of data exposure and the application of stringent access protocols as integral elements of data loss prevention measures.

Shukla et al. (2022) surveyed 250 organizations and examined key data protection aspects; the findings reveal that deploying data minimization reduced the amount of sensitive information possibly compromised during incidents by 43 per cent. This enduring reduction of the overall “attack surface” reduced the consequences of breaches where they are still present. Further, it was established that through data minimization, different organizations observed a 28 percent reduction of average cost incidence of data breaches than organizations that did not apply data minimization measures.

Sharma and Barua (2023) also supported the importance of strong access control as a means of protecting data breaches. Their research on big data analytics in today’s cybersecurity practices and using data from 350 large organizations revealed that enterprises enforcing granular and frequently audited permissions and access saw 55% less unauthorized data access attempts than organizations with less restrictive access controls. The same study also pointed to the principle of least privilege with organizations that had adopted this principle reporting a 37% decrease in the abuse of privileged accounts.

One of the important insights which arose out of the review was the availability of positive interaction when data minimization practices are integrated with the most effective encryption procedures. A study by Kaaniche and Laurent (2017) explored the effectiveness of cryptographic solutions for data protection in cloud storage environments, where it was concluded that organizations adopting data minimization strategies coupled with E2EE saw a 72% reduction in the probability of data leakage during cyberattacks compared to a 56% reduction for organizations adopting encryption and nothing else. This research further supports the need for an integrated approach towards data protection, where a number of interrelated, yet complementary measures are used to reinforce each other.

4.5. Organizational Culture and Security Awareness

Though the management hypotheses do not encompass these aspects, the research revealed that organizational culture and security awareness significantly influence the success of the data breach prevention strategies. This emerged as a cross-cutting issue that impacted on the effectiveness of the technical and non-technical controls.

It also discovered that organizations that embraced the principles of a healthy security culture where employees are well informed on security policies, leadership backs up security measures, and security-minded behavior is rewarded incurred 52% fewer security breaches than orgS that lacked a positive security culture. In addition, individuals in the organizations that have effective security cultures were 3.5 times more likely to make security related reports and smb suspicious activities, which inclusively improved threat preventive measures in the organization (Gartner 2019).

This study was supported by Kostic’s (2020) research on effective data breach prevention measures for security awareness training of various information security awareness techniques in tackling breaches resulting from social engineering. The research showed that organizations which have effective, ongoing security awareness programs had a 64% reduced rate of successful attacks as the result of phishing and had 57% fewer cases of mishandling of confidential information. Such realities have emphasized the need to conduct frequent security awareness training on security requirements in establishing a strong security foundation.

One finding that was interesting to come out of the review was the sections related to generation-related issues and their impact on security behaviors and awareness. Ballaro et al. (2020) examined the stringent difficulties that are

encountered while maintaining security protocols in different generations at the workplace. In their research with the sample of 250 organizations of different types, they compared security awareness and behaviors of different age categories. In addition, though employees belonging to the younger generation (18-34 years) seemed more comfortable with technology, they were more likely to involve in various risky behaviors online including, use single password across all accounts (73% in contrast to 51% of employees with ages greater than 55 years). Older employees displayed a higher level of obedience online but fell for social engineering tricks because they were not as familiar with new tricks as younger employees.

4.6. Impact of Emerging Technologies on Data Breach Prevention

The review showed some encouraging progress in the use of innovative technology for preventing data leaks. Blockchain technologies have been proposed in improving the data integrity and audibility to the next level. Evidently, Jones (2017) studied the prospect of blockchain technology in the development of secure audit trails in sensitive data contract. According to the study, organizations using blockchain-based data management systems noted a 47% decline in instances of unauthorized data changes, and a 62% enhancement in efficiency of identifying and tracking possible breaches.

However, as effective as applying the star-based approach for the blockchain data security is, its implementation is not without its difficulties. Wu and Zha (2022) also described scalability challenges and high computational demand in centralized and decentralized blockchains in large-scaled enterprises. In a survey of 50 organizations that had adopted blockchain-based security solutions, only 62% reported increased control and data integrity, but the same percentage said that they had experienced major issues in terms of system performance and compatibility with other IT systems. As such, blockchain, despite being posited as a means for improving data security, must be deployed when the organizational resources and technical competencies have been evaluated.

4.7. Adaptive Security Strategies for Evolving Threat Landscapes

The review highlighted the growing importance of adaptive security strategies that can evolve in tandem with rapidly changing threat landscapes. Wittkop (2022) suggested a dynamic cybersecurity framework specifically founded on cybersecurity risk evaluation and sequencing of threats dynamically acquired in a humane environment. In the study, primary data were collected from 300 organizations over a 3-year period; it discovered that organizations with adaptable security put in place achieved 53% fewer successful attacks and the likelihood of managing potential threats three times faster than organizations that depended on traditional/typical structures.

Moreover, Ibrahim et al. (2020) work on using threat intelligence to prevent data breaches also stressed on the role of adopting a broader data that could help in better threat analyzing. The organizations that incorporated internal security logs with threat feeds, and domain-specific information, were able to identify threats 8.5 days earlier than sources dependent solely on internal data sources only. This early detection capability seemed to lower the average cost of loss of data for these organizations by 37%.

These findings highlight the fact that information security awareness programs should not be one size fits all, but should be adapted to the various sectors of employees which might require different levels of security awareness training. Companies that adopted age-conscious security training segments received a 41% better total security usage compared to companies that only offered general security training to all sections of their organization. This approach not only improved the security activities but also created a culturally appropriate security that was accepted by the employees in their various age disparities.

5. Conclusion

In conclusion, this extensive review and classification of data breach prevention measures in today's Information systems architecture reflect a dynamically altering scenario of challenges and opportunities in the field of cybersecurity. The outcomes share the initial suppositions to a significantly high degree, evidencing the efficiency of integrated security measures, the significance of threat prediction, and the necessity of minimizing data and regulating the access to it. Furthermore, there are several secondary lessons arising from the review that include a number of additional factors that enhance comprehension of data breach beyond the analytical focal points identified by the research questions. A combination of AI with other modern technologies like machine learning and blockchain has further potential in strengthening data safeguard features. Nevertheless, the application of any of these technologies can only be successful after one has considered resource availability, technical competence, and integration opportunities. The review also discusses the importance of organizational culture and human aspects in the success of security measures which the author argues requires frequent and targeted security awareness programs to meet the needs of the different

generations within the workforce. However, the study also identifies certain devious of compliance model that warrants the need for development of more rich and elastic regulatory architectures for constituting proactive and adaptive security measures.

Recommendations for Future Directions

- ***Implement Adaptive Security Frameworks:*** It is recommended that organizations incorporate concepts of dynamism in their cybersecurity frameworks, which focuses on constant susceptibility analysis and leveraging of threat intelligence data for improvement of security measures. This approach should involve periodic security audits, penetration testing, and threat hunting in an effort to discover threats and weaknesses.
- ***Invest in AI and Machine Learning Capabilities:*** Based on the evidence suggesting that AI and advanced technologies lower the chance of a breach, it is in the best interest of corporations to invest in AI and machine learning algorithms to identify threats, abnormalities and manage security incidents. However, these investments should be compounded by measures to counter deal risks such as false positives and requirement of personnel skills to handling these systems.
- ***Develop Comprehensive Security Awareness Programs:*** Organizations should adopt continuous security awareness programs that will suit the need and susceptibilities of employees in organizations leading to the protection of organizational assets. Such programs should be designed to extend the traditional training models embodying the aspects of game solutions, scenarios, and frequent updates on security measures. Moreover, the organizations should encourage security awareness since people will be rewarded when they are security conscious.
- ***Implement Robust Data Minimization and Access Control Strategies:*** To mitigate the consequences of breaches, it is necessary for organizations to practice data minimization as well as install an intricate system of access control mechanisms. This should involve conducting an assessment of the current type and quality of stored data to remove all unnecessary sensitive data and dispose them in a secure manner; the adoption of new and improved access control technologies such as attribute based encryption and secure multi-party computation.
- ***Leverage Blockchain for Enhanced Data Integrity:*** However, organizations need to look into the possibility of making use of blockchain technology when the need arises in creating a system that is resistant to tampering and altering of audit trials and data in general. This should be done as part of an overall approach to the protection of data along with a systematically approach to considering the scalability, the performance and the compatibility with other systems.
- ***Develop Integrated Threat Intelligence Capabilities:*** Companies should focus on establishing active TI capacity, where internal threat sources are blended with external feed and sector intelligence. This integrated approach should be employed to enhance adaptive security approach and facilitate early identification of threats.

Based on the synthesis of findings from the systematic literature review of the approaches and technologies on data breach prevention, this research attests to the necessity of comprehensive and iterative security management in the contemporary informational systems. The considerations stressed the role of emerging technologies in advancing the concept, the importance of human aspects in its application, and the importance of maintaining the data security, while not hampering the work of the organization. This is a more innovative and comprehensive approach that employs both technological updates and human resource engagement to fight the ongoing problem of data breaches.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Angst, C. M., Block, E. S., D'Arcy, J., and Kelley, K. (2017). When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. MIS quarterly, 41(3), 893-A8. https://www.jstor.org/stable/26635018

[2] Ayereby, M. P. M. (2018). Overcoming data breaches and human factors in minimizing threats to cyber-security ecosystems (Doctoral dissertation, Walden University).

https://search.proquest.com/openview/57584a8528a23cadff644854f28f6bcf/1?pq-origsite=gscholarandcbl=18750anddiss=y

[3] Ali, S., & Chong, I. (2019). Semantic mediation model to promote improved data sharing using representation learning in heterogeneous healthcare service environments. *Applied Sciences*, *9*(19), 4175.

[4] Ballaro, J. M., Tyson, B., and Buckles, B. (2020). Information Technology Security Leaders' Solutions for Mitigating Data Breaches in a Multigenerational Workforce. International Leadership Journal, 12(2). http://internationalleadershipjournal.com/wp-content/uploads/2020/05/ILJ_Summer2020.pdf#page=75

[5] Bandari, V. (2023). Enterprise data security measures: a comparative review of effectiveness and risks across different industries and organization types. International Journal of Business Intelligence and Big Data Analytics, 6(1), 1-11. https://research.tensorgate.org/index.php/IJBIBDA/article/view/3

[6] Barnham, C. (2015). Quantitative and qualitative research: Perceptual foundations. International Journal of Market Research, 57(6), 837-854.

[7] Bhadouria, A. S. (2022). Study of: Impact of Malicious Attacks and Data Breach on the Growth and Performance of the Company and Few of the World's Biggest Data Breaches. Int. J. Sci. Res. Publ.

[8] Bhatia, T., and Verma, A. K. (2017). Data security in mobile cloud computing paradigm: A survey, taxonomy, and open research issues. The Journal of Supercomputing, 73(6), 2558-2631.

[9] Cheng, L., Liu, F., and Yao, D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 7(5), e1211. https://wires.onlinelibrary.wiley.com/doi/abs/10.1002/widm.1211

[10] Deloitte (2021). "Cybersecurity: The Impact of AI on Threat Detection and Response", https://www2.deloitte.com/us/en/pages/public-sector/articles/the-impact-of-ai-on-threat-detection-aand-response.html

[11] Desai, M., and Jaiswal, S. (2020). Importance of information security and strategies to prevent data breaches in mobile devices. In Improving business performance through innovation in the digital economy (pp. 215-225). IGI Global. https://www.igi-global.com/chapter/importance-of-information-security-and-strategies-to-prevent-data-breaches-in-mobile-devices/236942

[12] Diwan, T. D. (2021). An investigation and analysis of cyber security information systems: latest trends and future suggestion. Information Technology in Industry, 9(2), 477-492. http://it-in-industry.org/index.php/itii/article/view/372

[13] Fan, J. (2023). Legal Policies Failing on Data Breaches?–An Empirical Study of US Information Security Law Implementations. Procedia Computer Science, 221, 971-978. https://www.sciencedirect.com/science/article/pii/S1877050923008347

[14] Gartner, Inc. (2019). The Importance of Security Culture in Cybersecurity.

[15] Gootman, S. (2016). OPM hack: The most dangerous threat to the federal government today. Journal of Applied Security Research, 11(4), 517-525.

[16] Griffin, T. (2017). Strategies to Prevent Security Breaches Caused by Mobile Devices (Doctoral dissertation, Walden University). https://search.proquest.com/openview/74d44763ed86069c86c85561fe2a4a69/1?pq-origsite=gscholarandcbl=18750

[17] Ibrahim, A., Thiruvady, D., Schneider, J. G., and Abdelrazek, M. (2020). The challenges of leveraging threat intelligence to stop data breaches. Frontiers in Computer Science, 2, 36. https://www.frontiersin.org/articles/10.3389/fcomp.2020.00036/full

[18] IDC (2021). "The Business Value of Zero Trust: Security for the Digital Transformation Era".

[19] Igbal, S., Kiah, M. L. M., Anuar, N. B., Daghighi, B., Wahab, A. W. A., and Khan, S. (2016). Service delivery models of cloud computing: Security issues and open challenges. Security and Communication Networks, 9(17), 4726-4750.

[20] Jones, S. (2017). Data Breaches, Bitcoin, and Blockchain Technology: A Modern Approach to the Data-Security Crisis. Tex. Tech L. Rev., 50, 783. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/text50andsection=43

[21] Kaaniche, N., and Laurent, M. (2017). Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms. Computer Communications, 111, 120-141.

[22] Kitchin, R. (2016). "Getting smarter about smart cities: Improving data privacy and data security." (

[23] Knight, S. (2020). Strategies to Reduce Small Business Data Security Breaches (Doctoral dissertation, Walden University). https://search.proquest.com/openview/1e3e9871ee38371122acdaa9f8c30f0f/1?pq-origsite=gscholarandcbl=51922anddiss=y

[24] Kongnso, F. J. (2015). Best practices to minimize data security breaches for increased business performance. https://scholarworks.waldenu.edu/dissertations/1825/

[25] Kostic, L. C. (2020). Information security awareness techniques that reduce data breaches caused by social engineering attacks (Doctoral dissertation, Capella University).

[26] Malavet, J. N. (2017). Cyber Security in Higher Education: Accuracy of Resources Utilized by Information Technology Departments to Prevent Data Breaches (Master's thesis, Utica College). https://search.proquest.com/openview/94c4953e6d3101d5a787187fef3b49a3/1?pq-origsite=gscholarandcbl=18750

[27] Marseille, E. (2020). The Rapid Growth of Data Breaches in Today's Society (Master's thesis, Utica College). https://search.proquest.com/openview/3a55a67d9c495528627ddb5dd389fdd7/1?pq-origsite=gscholarandcbl=51922anddiss=y

[28] Mawel, M. (2022). Exploring the Strategic Cybersecurity Defense Information Technology Managers Can Implement to Reduce Healthcare Data Breaches (Doctoral dissertation, Colorado Technical University). https://search.proquest.com/openview/229812a9c4e0c3188d331e2df9663c8c/1?pq-origsite=gscholarandcbl=18750anddiss=y

[29] Mills, J. L., and Harclerode, K. (2017). Privacy, mass intrusion, and the modern data breach. Fla. L. Rev., 69, 771. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/uflr69andsection=28

[30] MITRE Corporation (2021). "Using Machine Learning for Cybersecurity Threat Detection", https://mad-certified.mitre-engenuity.org/bd8f4bb5-0694-40f0-9a50-a79e241b6210#acc.Uw9jp6cS

[31] Mohammed, Z. (2022). Data breach recovery areas: an exploration of organization's recovery strategies for surviving data breaches. Organizational Cybersecurity Journal: Practice, Process and People, 2(1), 41-59. https://www.emerald.com/insight/content/doi/10.1108/OCJ-05-2021-0014/full/html

[32] Nwankwo, M. I. (2020). IT Security Managers' Strategies for Mitigating Data Breaches in Texas School Districts. Walden University. https://search.proquest.com/openview/d10cf02a47fcb3bb5ee9359c393f931a/1?pq-origsite=gscholarandcbl=18750anddiss=y

[33] Ofori-Duodu, M. S. (2019). Exploring data security management strategies for preventing data breaches. Walden University. https://search.proquest.com/openview/93f957e9574b3ad2e771512b04dd739d/1?pq-origsite=gscholarandcbl=18750anddiss=y

[34] Osei-Amanfi, M. (2018). A case study exploration of strategies to avoid cloud computing data breaches. Grand Canyon University. https://search.proquest.com/openview/5622654f7d9e03763fe0948b25bc915f/1?pq-origsite=gscholarandcbl=18750anddiss=y

[35] Parisha, P., Puneet, R., and Sheenu, R. (2017). Data sharing security and privacy preservation in cloud computing: A survey. International Journal of Computer Applications, 167(11), 28-33.

[36] Pratt-Sensie, A. (2020). Security strategies to prevent data breaches in infrastructure as a service cloud computing (Doctoral dissertation, Walden University). https://search.proquest.com/openview/efb43ba7bac93bd2497ec7d3f3eaa814/1?pq-origsite=gscholarandcbl=18750anddiss=y

[37] Rivers, L. (2020). Strategies for Reducing the Risk of Data Breach within the Internet Cloud. Walden University. https://search.proquest.com/openview/e05497993d7ac4a6ef839beb8128dd4a/1?pq-origsite=gscholarandcbl=18750anddiss=y

[38] Schwartz, P. M., and Janger, E. J. (2006). Notification of data security breaches. Mich. L. Rev., 105, 913. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/mlr105andsection=36

[39] Sharma, P., and Barua, S. (2023). From data breach to data shield: the crucial role of big data analytics in modern cybersecurity strategies. International Journal of Information and Cybersecurity, 7(9), 31-59. https://publications.dlpress.org/index.php/ijic/article/view/46

[40] Shukla, S., George, J. P., Tiwari, K., and Kureethara, J. V. (2022). Data security. In Data Ethics and Challenges (pp. 41-59). Singapore: Springer Singapore. https://link.springer.com/chapter/10.1007/978-981-19-0752-4_3

[41] Simkus, A. (2017). Preventing Data Breaches at Law Firms: Adapting Proactive, Management-Based Regulation to Law-Firm Technology. Ariz. L. Rev., 59, 1111. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/arz59andsection=36.

[42] Suganya, M., and Prabha, T. (2022). A Comprehensive Analysis of Data Breaches and Data Security Challenges in Cloud Environment. In Proceedings of the 7th International Conference on Innovations and Research in Technology and Engineering (ICIRTE-2022), organized by VPPCOE and VA, Mumbai-22, INDIA. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4111762

[43] Talesh, S. A. (2018). Data breach, privacy, and cyber insurance: How insurance companies act as "compliance managers" for businesses. Law and Social Inquiry, 43(2), 417-440. https://www.cambridge.org/core/journals/law-and-social-inquiry/article/data-breach-privacyand-cyber-insurance-how-insurance-companies-act-as-compliance-managers-forbusinesses/1A10E0F87EB1C205EEA43AB4E8270FB2

[44] Teymourlouei, H., and Jackson, L. (2016). Detecting and preventing information security breaches. In Proceedings of the International Conference on Security and Management (SAM) (p. 304). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

[45] Ullah, B., and Nabi, S. I. (2022). Developing cyber security strategies for business organization to prevent data breaches. KASBIT Business Journal, 15(4), 62-79. https://www.kasbitoric.com/index.php/kbj/article/view/303

[46] Wang, Q., Ngai, E. W., Pienta, D., and Thatcher, J. B. (2023). Information Technology Innovativeness and Data-Breach Risk: A Longitudinal Study. Journal of Management Information Systems, 40(4), 1139-1170. https://www.tandfonline.com/doi/abs/10.1080/07421222.2023.2267319

[47] Wittkop, J. (2022). The cybersecurity playbook for modern enterprises: an end-to-end guide to preventing data breaches and cyberattacks. Packt Publishing Ltd. https://books.google.com/books?hl=enandlr=andid=ClpcEAAAQBAJandoi=fndandpg=PP1anddq=Data+Security+Strategies+to+Avoid+Data+Breaches+in+Modern+Information+Systemsandots=Fkl7J3TGIWandsig=_UC4LJEFhFG_7WLsfYeze27TzJY

[48] Wu, J., and Zha, P. (2022). A data security model for altering data ecosystem and affirmatively prevent mass data breaches. https://osf.io/preprints/d479z/

[49] Yuvaj, M. (2015). Cloud computing software testing: Techniques, challenges, and issues. International Journal of Emerging Technology and Advanced Engineering, 5(3), 56-59.