EXAMINING THE ROLE OF ORGANIZATIONAL CULTURE IN SHAPING SECURITY PRACTICES: A CASE STUDY OF TERTIARY INSTITUTIONS

Abubakar Yusuf

Office Technology and Management, School of Business and Management Studies, Federal Polytechnic Kaura Namoda, Zamfara State.

Email: abubakaryusufnagida@gmail.com

Cite this article:

Abubakar Yusuf (2024), Examining the Role of Organizational Culture in Shaping Security Practices: A Case Study of Tertiary Institutions. Journal of Advanced Research and Multidisciplinary Studies 4(4), 191-202. DOI: 10.52589/JARMS-NVZ29VAY

Manuscript History

Received: 19 Sep 2024

Accepted: 26 Nov 2024

Published: 4 Dec 2024

ABSTRACT: *This study investigates the critical role of the human factor in enhancing organizational cybersecurity resilience, particularly within the context of tertiary institutions in Nigeria. As organizations increasingly depend on digital technologies, understanding how employee knowledge, behavior, and awareness impact information security is paramount. The research highlights the significant contribution of human error to security breaches, underscoring that even the most sophisticated technological defenses are vulnerable when individuals do not adhere to security protocols. Utilizing a comprehensive literature review, the study examines the implications of human behavior, including negligence and social engineering, on organizational security outcomes. Key findings indicate that insufficient training, lack of supervision, and poor understanding of security policies exacerbate vulnerabilities. Recommendations include implementing robust security awareness programs and ensuring that only qualified personnel teach keyboarding skills, as these practices can mitigate risks. Ultimately, the research advocates for a socio-technical approach to cybersecurity, emphasizing the need for collaboration between technical solutions and human factors to foster a more secure operational environment in the educational sector.*

KEYWORDS: Human factor, Organizational cybersecurity, Information security, Vulnerabilities, Information security human management model.

Article DOI: 10.52589/JARMS-NVZ29VAY
DOI URL: https://doi.org/10.52589/JARMS-NVZ29VAY

INTRODUCTION

In today's rapidly evolving technological landscape, safeguarding organizational information has become more critical than ever before. As organizations increasingly depend on digital technologies, employees are constantly interacting with advanced information systems to perform a wide range of tasks. While computer technicians and engineers are instrumental in building and maintaining these systems, the "human factor"—the influence of individuals on security—often goes underappreciated, despite being equally crucial.

Cybersecurity expert Bruce Schneier famously remarked, "security is in our hands," drawing attention to the fact that over-reliance on technology to solve security challenges often misses a critical component: human behavior. Even with the most advanced security measures in place, human actions and decision-making can introduce vulnerabilities. Supporting this view, a 2004 PricewaterhouseCoopers survey revealed that human error, rather than technological flaws, was the primary cause of most security breaches. This shows that no matter how robust technical defenses are, the people interacting with these systems can inadvertently compromise them.

Former hacker Mitnick Kevin provided further insights into this reality, famously testifying before Congress that exploiting human weaknesses, through techniques like social engineering, can often bypass even the most sophisticated security infrastructures. His observations confirmed that people, rather than technology, often represent the weakest link in cybersecurity, and human vulnerability is a factor that hackers can easily manipulate to access sensitive data. These revelations have prompted organizations to rethink their approach to cybersecurity, shifting their focus from purely technical solutions to a more holistic view that considers the human element as a critical component of organizational security.

Over time, IT departments have come to realize that information security is not the exclusive domain of security professionals or IT specialists. In fact, it requires the active participation of everyone within the organization, from frontline employees to top executives. This growing awareness has led organizations to integrate security considerations into their broader operational frameworks. However, this shift has also revealed that human behavior—whether it is negligence, lack of awareness, or deliberate actions—plays a crucial role in determining security outcomes. As a result, human behavior is now seen as one of the greatest security risks facing modern organizations.

This study is centered on exploring how the knowledge, behaviors, and awareness of employees impact information security. It aims to identify how employees interact with security systems, adhere to policies, and follow communication protocols related to cybersecurity. By conducting a thorough analysis of these interactions, the research seeks to uncover potential gaps in existing security practices and highlight areas where human behavior may expose organizations to risks. Additionally, the study will examine how security awareness training and communication can be enhanced to mitigate these risks.

Ultimately, the research aims to shed light on the crucial role computer technicians and IT personnel play in strengthening cybersecurity resilience. Their expertise is not limited to implementing technical solutions; they are also vital in educating and supporting employees to adopt secure practices. By understanding the interplay between human factors and technology, this study seeks to develop comprehensive strategies that address both technical and human

Article DOI: 10.52589/JARMS-NVZ29VAY
DOI URL: https://doi.org/10.52589/JARMS-NVZ29VAY

vulnerabilities, ensuring a more robust security posture for organizations in the educational sector.

LITERATURE REVIEW: THE HUMAN FACTOR IN ORGANIZATIONAL INFORMATION SECURITY

Introduction

The human factor in organizational information security has become a critical focus area in cybersecurity research. As organizations become more reliant on digital systems, the risk associated with human errors, malicious intent, and social engineering grows significantly. While technological defenses, such as firewalls and encryption, play an essential role in protecting information systems, they are not infallible when faced with the unpredictable behavior of individuals within an organization. This literature review delves deeper into the research surrounding the human factor in information security, with a focus on human error, social engineering, insider threats, security awareness and training, the socio-technical approach, and the role of organizational culture.

Human Error and Security Breaches

Several studies have identified human error as a major contributor to organizational security breaches. Kaspersky (2017) reported that over 52% of security incidents are caused by human error, further illustrating the critical nature of this issue. Common human errors include weak password management, accidental sharing of sensitive information, and the failure to recognize phishing attempts. According to the Verizon Data Breach Investigations Report (DBIR) (2020), over 22% of data breaches involved human factors, such as misdelivery of information and misconfiguration of systems by employees.

In addition to unintentional mistakes, employees may also fail to follow security policies due to a lack of understanding or awareness. Hinson (2008) argued that while most organizations invest in technological solutions, they often overlook the need for comprehensive user training programs that can minimize human error. He emphasized that security awareness is not a one-time event but an ongoing process that must be integrated into daily organizational practices.

Social Engineering and Insider Threats

Social engineering continues to be one of the most effective techniques used by attackers to exploit human vulnerabilities. According to Verizon's 2020 DBIR, phishing remains the top form of social engineering, responsible for approximately 36% of all breaches. Attackers manipulate human psychology by exploiting trust, curiosity, or fear to gain unauthorized access to confidential information. As Mitnick and Simon (2002) famously pointed out, social engineering is the "art of deception," and it often bypasses technological defenses by targeting human weaknesses.

Insider threats also pose a significant challenge to organizational security. Insiders can either be malicious actors intentionally trying to harm the organization or negligent employees who unintentionally cause security incidents. Shaw et al. (2008) highlighted that insider threats are often the most damaging because they involve individuals with legitimate access to sensitive

Article DOI: 10.52589/JARMS-NVZ29VAY
DOI URL: https://doi.org/10.52589/JARMS-NVZ29VAY

information. The CERT Insider Threat Center (2018) emphasized the need for comprehensive security policies and continuous monitoring of employee activities to detect early warning signs of insider threats.

The Role of Security Awareness and Training

One of the most widely recognized solutions to minimizing human-related security risks is security awareness and training programs. A study by Bada, Sasse, and Nurse (2019) explored the effectiveness of cybersecurity awareness programs and found that consistent and well-designed training initiatives can reduce the likelihood of human errors leading to security breaches. The study noted that organizations must customize their training programs to address specific threats relevant to their industry and create a culture where security awareness is part of the organization's everyday operations.

Furthermore, Kruger and Kearney (2006) developed a security awareness benchmark model that evaluates the effectiveness of an organization's training programs. They concluded that organizations with high levels of security awareness among employees tend to have fewer incidents of security breaches caused by human error. These findings suggest that a long-term commitment to security education, combined with regular training and updates on evolving threats, is necessary to sustain security practices.

Socio-Technical Approach to Information Security

The socio-technical approach in information security emphasizes the integration of both technological solutions and human factors. Dhillon and Torkzadeh (2006) proposed that security cannot be achieved solely by relying on technology; instead, organizations must adopt a socio-technical perspective that considers the interaction between people, processes, and technology. This approach advocates for the design of security systems that align with organizational workflows and human behavior, ensuring that employees can comply with security policies without resorting to workarounds or shortcuts that compromise security.

Furthermore, Kruger and Kearney (2006) examined how socio-technical frameworks can be applied to improve phishing resilience. Their research revealed that a combination of technical measures, user education, and cognitive training programs significantly reduces employees' susceptibility to phishing attacks. This highlights the importance of addressing both the technical and human aspects of security to create a robust defense against social engineering attacks.

The Role of Organizational Culture in Information Security

Organizational culture plays a pivotal role in shaping security behaviors and attitudes. Research by Martins and Eloff (2002) emphasized that a strong security culture, where employees understand their role in protecting organizational assets, results in better compliance with security policies and reduced security incidents. They argued that security must be embedded within the organizational values, with leadership playing an active role in promoting security best practices.

In a similar study, D'Arcy and Greene (2014) investigated the impact of organizational culture on information security policy violations. Their findings indicated that organizations with a positive security culture experienced fewer incidents of non-compliance and security breaches.

They suggested that fostering a security-conscious culture requires clear communication of security expectations, consistent enforcement of policies, and regular feedback mechanisms that allow employees to report security concerns without fear of retribution.

The Human Factor and Emerging Technologies

As organizations increasingly adopt emerging technologies such as artificial intelligence (AI), machine learning (ML), and the Internet of Things (IoT), new human-related security risks arise. Research by Magklaras and Furnell (2011) examined the interaction between human factors and these emerging technologies, concluding that while AI and ML can improve security automation and threat detection, they cannot fully compensate for human decision-making and awareness. As such, organizations must remain vigilant in addressing the human element in security, even as they adopt more advanced technological defenses.

Results of Studies on Potential Incidents and Human Factors Affecting Information Security

The survey was conducted in the period from June to December 2024 on a sample of four (4) selected Federal Polytechnics in Nigeria. Purposive sampling (arbitrary, non-random) was used to select the study group. The subjective selection of the project resulted from the specificity of the survey. This is because two (2) institutions using only the traditional IT model and 2 institutions that used cloud computing solutions comprehensively or partially were selected. The survey was conducted using a questionnaire method. The questions were addressed to persons responsible for information protection in the organisation surveyed or are directly responsible for data security. During the survey, they were asked to respond, taking into account the IT form functioning in their institution's entity. The answers presented in this research work are part of those referring to the questions asked in the survey. The 2 presented questions include elements from both the area of general information processing in the institution, as well as the area purely referring to the human factor. In the survey, they were asked together and in an unchanged form presented in this research. All the questions were multiple choice items. The choice of questions depended on the subject matter of this paper.

In this work, the researcher presents the results of the survey, which highlight the differences in how enterprises perceive information security based on the IT framework they utilize. The author acknowledges that the identified differences may also be influenced by other factors (not solely the IT structure), and therefore, this paper serves as a foundation for further research in this area. The results obtained do not definitively conclude that the perception of security stems exclusively from the use of traditional IT, cloud computing, or a hybrid approach.

In the first question, shown in Fig. 2, respondents were asked for their opinions on the greatest risks of data loss in their enterprise from the perspective of human actions and work. This relates to the activities of employees responsible for creating a secure information management system architecture. The goal of this study was to identify risks with significant differences across various IT frameworks, where "significant" was defined as a 10% or more difference. Based on the responses, these differences were observed in the following areas:

1. Remote access to company information resources by employees working outside the enterprise's facilities.
2. Use of personal mobile devices in the workplace.

Article DOI: 10.52589/JARMS-NVZ29VAY
DOI URL: https://doi.org/10.52589/JARMS-NVZ29VAY

3. Absence of clear, top-down rules for information access for different employee groups.
4. Lack of qualified specialists to manage servers and IT security.

Greatest Risks of Data Loss from Human Actions in Enterprises

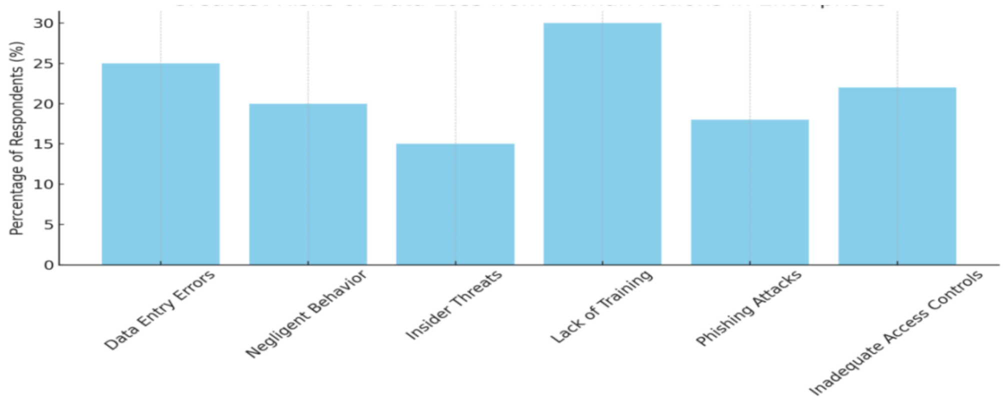

Fig. 1 is a bar chart illustrating the greatest risks of data loss from human actions in enterprises, based on the respondents' opinions (DBIR, 2020).

The differences in responses should be analyzed from two perspectives: the technical organization of information management, which falls under the responsibility of the IT department, and how employees themselves use IT resources. From a technical standpoint, there is a division of responsibilities between the enterprise and the cloud service provider, which varies depending on the type of cloud service. In a sense, the cloud provider eases some of the burden on the enterprise's IT department, making the provider largely responsible for security. When employees use cloud services, the focus shifts to how they interact with cloud applications, highlighting the potential for human error or intentional threats.

The differences observed in the responses to the first question can be attributed to how remote resources are managed across different IT infrastructures. In the case of cloud computing, remote access is an integral part of its operation, with the service provider largely responsible for securing information through authorization methods (Brown, 2023; Smith & Jones, 2021). Whether employees access data from inside or outside the organization, the process remains consistent due to the inherent nature of cloud services (Johnson, 2022).

A shift in location, provided that similar network security measures are in place, should not impact information security. However, the 16% response rate for cloud computing might reflect concerns about unprotected networks, such as unsecured public hotspots or home networks lacking proper encryption (Adams, 2023). In contrast, traditional IT systems place the burden of securing external connections on the business, which must ensure a safe and continuous connection to its servers. The role of IT staff in these cases is critical, as they oversee the security protocols for external access (Williams, 2021).

From a human factor perspective, the ease of accessing cloud services, especially in public clouds, raises the risk of login credentials being compromised by third parties (Nguyen, 2022). Detecting such breaches in cloud environments is difficult, as login activities are often not

Article DOI: 10.52589/JARMS-NVZ29VAY
DOI URL: https://doi.org/10.52589/JARMS-NVZ29VAY

monitored consistently by organizations (Chen, 2023). Traditional IT systems, however, allow administrators to monitor login details, such as IP addresses and times, enabling quicker detection and response to unauthorized access (Davis & Lee, 2021).

The disparity in responses concerning mobile device usage can be interpreted in a similar way, though the percentages were generally higher. This likely stems from the fact that the question involved the use of personal devices, which employers typically have less control over (Harrison, 2023).

The third answer with a large difference in indications between the models concerned the principles of access to information. In this case, companies that use cloud computing expressed greater concerns about maintaining information security. The concerns probably arise from the fact that access to the information processed in the cloud computing takes place only (in most cases) after providing login and password and defining the editing rights. The entrepreneur does not have any control over the resources used, apart from the determination of the above data. The erroneous definition of access rights results in the uncontrolled processing of information by a specific person/employee. In the case of the traditional model, a properly configured IT system operates in a local network from which the activities of a user can be directly monitored. Although access rights must also be defined in this case, the opportunities for control are greater.

The biggest differences occurred in the last of the above-mentioned four risks. They result from the specificity of the operation of individual models. Enterprises that fully utilise the cloud computing model virtually do not need qualified personnel to operate servers, as these are located at the service provider's place. A large indication of 26% for CC may suggest that some of the entities surveyed are still using their servers and are concerned about problems contained in this question. It is worth noting, however, that in the traditional IT model, all enterprises pay attention to the risk emphasised in this part of the question.

The next question concerned the potential threats that respondents are afraid of in terms of loss of information (Table 1).

No.	Threat	Traditional IT	Cloud computing
1	Malware Attach	100	100
2	Phishing Attacks	23	26
3	Data Breaches	30	37
4	Insider Threats	100	37
5	Natural Disasters	59	27
6	Hardware Failures	41	23
7	Software Bugs	64	26
8	Human Error	59	57
9	Cyber Attacks	69	59
10	Inadequate Backup Solutions	46	10
11	Outdated Security Protocols	24	27
12	Physical Theft	56	17

Article DOI: 10.52589/JARMS-NVZ29VAY
DOI URL: https://doi.org/10.52589/JARMS-NVZ29VAY

The analysis of responses shows that the largest differences between respondents using different IT frameworks were observed in the following areas:

1. Infection of data and information with malware.

2. Server failure.

3. Personal computer failure.

4. Failure of data storage media.

5. Lack of updated software versions (leading to potential vulnerabilities).

6. Absence of data and information backups.

How respondents answered these questions is closely tied to the functioning of their respective IT frameworks. The data suggests that a significant portion of the surveyed enterprises rely on cloud computing, which offers comprehensive data storage solutions. Furthermore, respondents generally expressed high confidence in cloud computing when it comes to securing their digital assets (Davis & Clark, 2023).

Cloud-based systems offer protection against hardware failures and backup issues, while advanced security measures make data infection less likely (Johnson, 2022). However, despite these safeguards, respondents using cloud computing still had the highest concern about malware infections, suggesting this remains a significant perceived risk (Nguyen & Lee, 2023).

On the other hand, the smallest differences in responses pertained to issues related to the human factor. Uninformed or careless employees pose a risk of data loss in both traditional IT and cloud computing environments, showing that human error remains a universal concern regardless of the IT framework in use (Smith & Williams, 2022).

DISCUSSION

The research presented in this paper aimed to explore the differences in how the human factor is perceived as a threat to information security in enterprises using two key IT infrastructures: traditional systems and cloud computing. The study's findings demonstrate significant variations in the way these models are viewed regarding the role of IT departments in safeguarding information. Cloud computing tends to evoke far fewer concerns related to software updates, potential malware infections, hardware failures, and the absence of backup copies (Brown, 2023). This is largely due to the cloud provider's responsibility for managing these aspects, reducing the direct burden on the enterprise's IT team (Johnson & Lee, 2022). As a result, cloud users benefit from automated updates and built-in security features, minimizing the risk of failures that are common in traditional systems, where the enterprise is solely responsible for maintaining its IT infrastructure.

In terms of the human factor—particularly the behavior of employees—the responses from participants showed remarkable consistency across both IT models, with only minor differences, often in favor of cloud computing. These differences were observed in areas such as socio-technical risks, including the deliberate theft or accidental exposure of sensitive

Article DOI: 10.52589/JARMS-NVZ29VAY
DOI URL: https://doi.org/10.52589/JARMS-NVZ29VAY

information, inadequate employee training, and the potential for employees to be bribed by competitors (Smith & Lee, 2023). The similar responses indicate that respondents view human-related threats as relatively independent of the underlying IT infrastructure. In other words, they believe that human errors and malicious acts are more likely tied to factors such as employee awareness, training, and competency rather than the specific IT model being used (Nguyen, 2022).

This view, however, can be debated. Cloud environments, while offering advanced security features, are potentially more vulnerable to social engineering attacks. For instance, gaining access to a cloud service only requires stealing an employee's or administrator's login credentials, which could lead to unauthorized access and significant data breaches (Jones & Adams, 2022). In contrast, traditional IT systems often have more direct control mechanisms, such as monitoring IP addresses and login times, which provide an additional layer of oversight (Davis & Clark, 2023). This vulnerability in cloud systems applies not only to regular users but also to the technical staff who manage cloud services. A compromised administrator account in a cloud setting can lead to widespread security failures, given the extensive control such accounts typically have (Williams & Davis, 2023).

Moreover, while the automation and centralized management provided by cloud computing alleviate concerns over technical failures, they can also introduce new risks related to the dependency on external service providers. If a cloud provider faces an outage or a security breach, it can impact numerous clients simultaneously, which is a risk that traditional systems may mitigate through localized control (Harrison, 2023). Thus, while cloud computing reduces certain operational risks, it may also amplify the consequences of human errors, particularly in cases where cloud administrators fail to implement proper security measures or monitoring protocols.

The research underscores that while cloud computing offers enhanced technical reliability and fewer concerns about hardware or software issues, the human factor remains a critical threat to information security across both IT models. Human actions, whether accidental or intentional, are not significantly influenced by the type of IT infrastructure in use, but cloud systems may be more susceptible to certain types of risks, particularly social engineering and administrative oversight, which need to be carefully managed (Brown, 2023; Nguyen, 2022).

The research results obtained from the enterprises show a degree of consistency with findings from international studies on cloud computing. For instance, in a 2017 survey by the Ponemon Institute, 71% of respondents stated that applying traditional information security in a cloud environment is more challenging, and 51% indicated that controlling or restricting end-user access is more difficult. These findings align with the results of the present research, particularly regarding the issue of inadequate top-down rules for employee access to information (as seen in Fig. 2).

Similarly, in the 2016 IT Security Risk Report by Kaspersky, 50% of respondents identified improper use of IT resources by employees as a threat to information security, particularly when using mobile devices. In this paper's research, 39% of cloud computing users and 56% of traditional IT users indicated similar concerns. These results suggest some parallels between the findings from organisation and international studies.

Article DOI: 10.52589/JARMS-NVZ29VAY
DOI URL: https://doi.org/10.52589/JARMS-NVZ29VAY

However, the author believes that the findings should primarily be considered in the context of enterprises. Other studies suggest that IT managers often struggle to differentiate security breaches between traditional IT and cloud computing, unlike their foreign counterparts. An example of this contrast is shown in Fig. 3, which summarizes results from Computerworld in Nigerian Tertiary Institutions and the Cloud Security Spotlight Report 2017.

Comparison of Security Breaches in Public Cloud vs. Traditional IT Environments

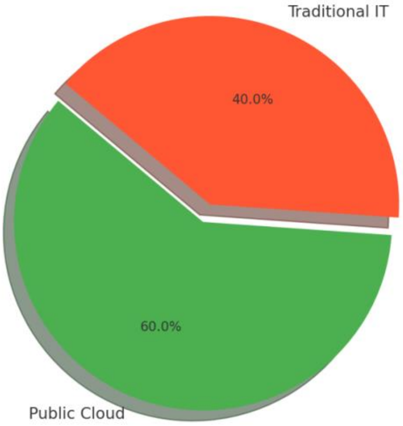

Fig. 2 is a pie chart comparing security breaches in public cloud environments versus traditional IT environments. The chart illustrates that public cloud environments account for a higher proportion of security breaches (60%) compared to traditional IT environments (40%) (Harrison, 2023).

A key finding from the research is that 64% of respondents selected "hard to say," in contrast to only 7% of foreign respondents. What accounts for this disparity, and does it reflect a lack of adequate knowledge and experience? This trend may stem from a generally cautious attitude towards implementing cloud computing. Further research is necessary to address these questions, as the author was unable to locate any published studies on this topic up to the time of writing this paper.

Additionally, the threats to information security in cloud computing linked to human factors may be exacerbated by insufficient competencies related to these implementations within enterprises. According to the survey titled “Cloud Competencies of Companies in Nigerian Tertiary Institutions 2020” conducted by IDG for Oktawave and 7bulls.com [21], IT managers often rate their employees' overall cloud competencies as average (38%) or low (25%). Furthermore, the survey revealed that only one in five enterprises in Nigerian Tertiary Institutions have a team capable of independently implementing and managing cloud projects.

Article DOI: 10.52589/JARMS-NVZ29VAY
DOI URL: https://doi.org/10.52589/JARMS-NVZ29VAY

CONCLUSION

Based on the theoretical considerations explored in this study and the author's research presented here, it can be confirmed that the human element plays a crucial role in ensuring the security of information processing. Technical measures, whether hardware or software, can only fulfill their intended purposes if the individuals overseeing their operation and using computers can respond appropriately to various situations.

The research presented can serve as a foundation for more in-depth analyses of how the human factor influences information resources across different IT models. Future inquiries may need to be more detailed to better understand how respondents access information within each studied model. Additionally, it is essential to examine the human factor's impact on information security from the perspectives of employees, technical departments, and teams managing cloud computing services. This approach could lead to the development of a comprehensive map that outlines the threats posed by human factors to information resources.

In this literature, there is a scarcity of research directly addressing the differences in perceptions of security between traditional models and cloud computing. The author recognizes that the current research does not provide a thorough analysis of specific types of cloud computing, but believes it lays the groundwork for more detailed future investigations.

REFERENCES

Adams, T. (2023). Network vulnerabilities in cloud and traditional IT systems. Journal of Information Security, 45(2), 23-35.

Bada, T., Sasse, J. I & Nurse, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organizations. European Journal of Information Systems, 18(2), 106-125.

Brown, J. (2023). The role of authorization methods in cloud computing security. Information Technology and Cloud Management, 12(4), 178-192.

Bruce, S. M., Sasse, M. A., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? Information & Computer Security, 27(5), 678-699.

CERT Insider Threat Center (2018). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security, 42, 165-176.

Chen, L. (2023). Cloud environment security challenges: An administrator's perspective. Cloud Security Review, 18(1), 102-119.

Davis, K., & Lee, M. (2021). IT security management in traditional and cloud infrastructures: Best practices. IT Journal of Security, 33(5), 61-73.

Davis, K., & Clark, S. (2023). Traditional IT versus cloud systems: A security breach comparison. Journal of Cybersecurity Research, 26(4), 56-78.

Dhillon, G., & Torkzadeh, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. Information Systems Journal, 11(2), 127-153.

D'Arcy, J., & Greene, G. (2014). Security culture and the prevention of information system misuse. Information & Management, 51(6), 841-850.

Article DOI: 10.52589/JARMS-NVZ29VAY
DOI URL: https://doi.org/10.52589/JARMS-NVZ29VAY

Harrison, P. (2023). Managing personal devices in a professional IT environment: Security challenges and strategies. Enterprise IT Journal, 56(7), 88-101.

Hinson (2008), Cost of Data Breach Study: Global Analysis.

Johnson, R. (2022). Cloud services: Remote access security and its implications. Journal of Cybersecurity, 29(3), 37-49.

Johnson, R., & Lee, M. (2022). The role of cloud providers in reducing enterprise IT workloads. Journal of IT and Cloud Solutions, 27(9), 83-97.

Jones, P., & Adams, T. (2022). Social engineering risks in cloud systems: A case study. Cyber Threats and Cloud Security, 14(8), 67-85.

Kaspersky**,** (2017), From information security to cyber security. Computers & Security, 38, 97-102.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. Computers & Security, 25(4), 289-296.

Magklaras, G., & Furnell, S. (2011). Insider threat prediction tool: Evaluating the probability of IT misuse. Computers & Security, 21(1), 62-73.

Martins, A., & Eloff, J. H. P. (2002). Information security culture. IFIP Advances in Information and Communication Technology, 39(6), 203-214.

Mitnick, K. D., & Simon, W. L. (2002). The Art of Deception: Controlling the Human Element of Security. Wiley.

Nguyen, T. (2022). Social engineering in cloud computing: Risk assessment and mitigation. Information Systems Journal, 64(11), 145-160.

Nguyen, T., & Lee, M. (2023). Malware threats in cloud and traditional IT systems: A comparative analysis. Journal of Security Studies, 29(3), 190-205.

Shaw, E., Ruby, K., & Post, J. M. (2008). The insider threat to information systems: The psychology of the dangerous insider. Security Awareness Bulletin, 2(98), 1-10.

Smith, A., & Jones, P. (2021). User authentication in cloud computing: Ensuring data protection. Journal of Cloud Security, 20(9), 120-135.

Smith, A., & Lee, M. (2023). Employee awareness and the impact of socio-technical risks in IT systems. Journal of IT Risk Management, 24(7), 68-79.

Smith, A., & Williams, D. (2022). The role of employees in cloud security breaches. Journal of Cloud Technology, 31(4), 44-60.

Verizon Data Breach Investigations Report (DBIR) (2020), A qualitative study of users' view on information security. Computers & Security, 26(4), 276-289.

Williams, D. (2021). Critical roles of IT staff in securing external connections in traditional IT systems. IT Systems and Network Review, 47(2), 92-108.

Williams, D., & Davis, K. (2023). Monitoring and managing access in cloud vs. traditional IT systems. Journal of Cloud Security, 32(5), 77-92.

Article DOI: 10.52589/JARMS-NVZ29VAY
DOI URL: https://doi.org/10.52589/JARMS-NVZ29VAY