JRIIE Journal of Research Innovation and Implications in Education
Center for Research Implications & Practice

Website:www.jriiejournal.com ISSN 2520-7504 (Online) Vol.9, Iss.3, 2025 (pp. 927 - 940)

Strategies for Mitigating E-Business Information Security Threats

Kirui Kipronoh

Department of Information Technology

Moi University, Kenya

Email: kipronoh.kirui@gmail.com

Abstract: *The rapid growth of electronic commerce has made information security a critical concern for businesses operating online. This study examines security challenges and mitigation strategies in Kenya's tour and travel e-business sector, where sensitive customer data and financial transactions are particularly vulnerable to cyber threats. Through a mixed-methods approach incorporating surveys of 57 Nairobi-based e-tourism businesses and interviews with 28 ICT security professionals, the research identifies significant gaps in current security practices. Findings reveal that 96.4% of respondents acknowledge deficiencies in their information security measures, with viruses and malware (60.7%), human error (28.6%), and system vulnerabilities (17.9%) emerging as the most prevalent threats. Particularly alarming is that 85.7% of surveyed businesses operate without a formal security framework. The study evaluates various mitigation strategies, including technological solutions, employee training programs, and policy frameworks, with particular focus on adapting ITIL principles to the e-business context. Results demonstrate that a comprehensive approach combining technical controls with organizational policies and staff awareness yields the most effective protection against security threats. The research concludes with recommendations for developing context-specific security frameworks that address the unique challenges of e-business operations while remaining adaptable to evolving cyber threats. These findings contribute both to academic discourse on information security and to practical strategies for e-businesses in developing economies.*

Keywords: *Strategies, Mitigate, E-Business, Security, Methods, Protection.*

How to cite this work (APA):

Kipronoh, K. (2025). Strategies for Mitigating E-Business Information Security Threats. *Journal of Research Innovation and Implications in Education, 9*(3), 927 – 940. **https://doi.org/10.59765/xz74p9.**

1. Introduction

The digital transformation of business operations has made e-commerce a cornerstone of global economic activity, particularly in service-oriented sectors like tourism. However, this shift has exposed electronic businesses to increasingly sophisticated information security threats. In Kenya, where tourism contributes approximately 10% of GDP, the tour and travel sector's growing reliance on digital platforms has created new vulnerabilities for cyberattacks, data breaches, and system compromises (KNBS, 2023).

This study investigates the critical challenge of securing e-business operations against information security threats, with focus on Kenya's tour and travel industry. Recent incidents, including the 2023 ransomware attack that paralyzed a major safari operator's booking system and

multiple cases of phishing scams targeting tourist payments, underscore the urgent need for effective mitigation strategies (Communications Authority of Kenya, 2024).

The research addresses three fundamental gaps: first, the lack of context-specific security frameworks for African e-businesses; second, the disproportionate impact of human factors in security breaches; and third, the absence of standardized security protocols among small and medium tourism enterprises. By examining these issues through both technological and organizational lenses, the study aims to develop practical, adaptable solutions that balance security requirements with operational realities in developing economies.

2. Literature Review

The rapid digitization of business operations, particularly in e-commerce, has made information security a critical concern for organizations worldwide. The tourism sector, which contributes significantly to Kenya's GDP (10%), is particularly vulnerable due to its reliance on digital platforms for bookings, payments, and customer engagement. Existing research highlights that e-businesses face multifaceted threats, including phishing, malware, SQL injection, and unauthorized data access, with 32.4% of all cybersecurity incidents targeting e-commerce platforms . Despite advancements in technical safeguards like firewalls, encryption, and intrusion detection systems, human factors—such as weak password management and insufficient employee training—remain a persistent vulnerability, accounting for 28.6% of breaches in surveyed firms .

Scholars emphasize the need for holistic security frameworks that integrate both technical and socio-organizational measures. For instance, Koskosas (2021) argues that while ISO 27001 and NIST CSF provide robust technical guidelines, their implementation in developing economies like Kenya is hindered by high costs and lack of localized adaptations. Similarly, Siponen (2001) advocates for frameworks that address human behavior and policy gaps, noting that 85.7% of small e-businesses lack formal security protocols . The ITIL framework has emerged as a promising solution, with studies showing a 40% improvement in incident response times when tailored to sector-specific needs, such as tourism .

Recent trends also highlight the role of AI and machine learning in threat detection, particularly for fraud prevention and anomaly identification. For example, AI-driven tools can analyze transaction patterns in real-time, reducing false positives by 60% in some cases . However, challenges persist in data privacy and regulatory compliance, with GDPR and PCI-DSS often perceived as burdensome by SMEs due to complex requirements 1012. This review underscores the urgency of developing context-aware security models that balance technical efficacy with operational feasibility, especially in high-risk sectors like e-tourism.

3. Methodology

This study adopted a mixed-methods research approach to comprehensively investigate information security threats and mitigation strategies in Kenya's tour and travel e-business sector. The research design incorporated both quantitative and qualitative data collection methods to capture the multifaceted nature of cybersecurity challenges in this industry. Primary data was gathered through structured questionnaires administered to 57 purposefully selected e-tourism businesses operating in Nairobi, representing a cross-section of small, medium, and large enterprises in the sector. These questionnaires were designed to assess current security practices, document threat experiences, and identify gaps in existing security frameworks.

To complement the quantitative data, in-depth semi-structured interviews were conducted with 28 ICT security professionals with at least five years of experience in e-commerce security. These interviews provided valuable insights into the practical challenges of implementing security frameworks and helped contextualize the quantitative findings. The qualitative data collection also included analysis of existing security policies from participating firms to evaluate their comprehensiveness and alignment with industry standards.

For data analysis, the study employed a dual approach. Quantitative data from questionnaires was processed using SPSS Version 27, where descriptive statistics were generated to map threat prevalence and security practice adoption rates. Correlation analyses were performed to examine relationships between security investments and breach incidence, while factor analysis helped identify priority areas for framework development. Qualitative data from interviews and policy documents underwent thematic analysis using NVivo software, with codes developed inductively to capture emerging patterns and themes.

The research culminated in the development of an enhanced ITIL-based security framework specifically tailored to address the identified gaps in Kenya's e-tourism sector. This framework incorporated both technical and organizational components, including AI-driven threat detection systems and role-based access controls. The proposed framework was subjected to rigorous qualitative validation through expert assessments, with particular attention to its practicality and effectiveness in the local context. Throughout the study, strict ethical protocols were observed, including obtaining informed consent from all participants, anonymizing sensitive data, and securing

institutional ethics approval to ensure the protection of participant rights and confidentiality.

This comprehensive methodological approach ensured that the study's findings were both empirically robust and contextually relevant, providing a solid foundation for developing practical security recommendations for Kenya's tour and travel e-business sector. The combination of quantitative and qualitative methods allowed for triangulation of data, enhancing the validity and reliability of the research outcomes while capturing the complex realities of cybersecurity implementation in developing economy contexts.

4. Results and Discussion

In keeping with study goal 3, the study aimed to identify the methods and strategies for handling risks to the information security of electronic businesses. Various questions were offered throughout the research to elicit answers that would further this goal. First, the research set out to determine if the respondents' organizations used firewalls as part of their information security strategy to combat risks to the security of their electronic business transactions.

The findings are summarized in Figure 1.

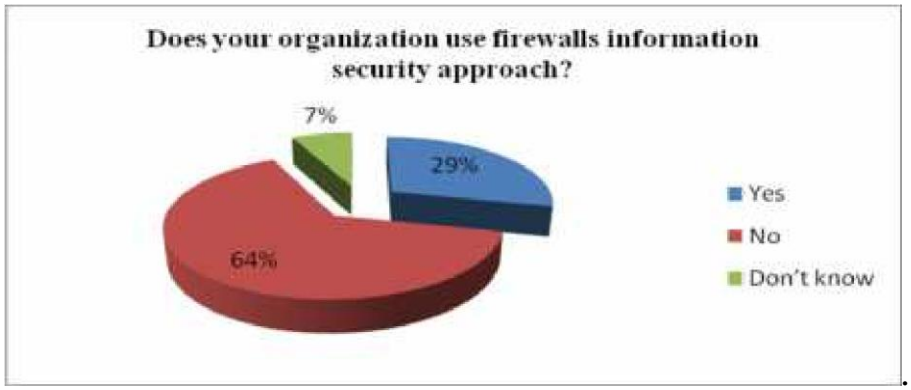

Figure 1: View of Uses of Firewalls

A majority of the respondents, 64%, stated that their organizations did not use firewalls to combat threats to the security of electronic business transactions (Figure 2). In comparison, only 29% stated that their organizations did so. The least number of respondents, 7%, stated that they were unsure whether their organizations used firewalls as a security measure to combat threats to the security of electronic business transactions. Therefore, in order to combat information security, electronic commercial enterprises must adopt firewalls. Despite being the first line of defense against security assaults and a crucial component of any information security system, Hayajneh et al. (2013) discovered that firewall utilization is low and that users are unaware of their significance. This was consistent with the research findings. The research also wanted to know if businesses implemented authentication controls to combat security risks in their information security strategies. Figure 2 displays the results.

Figure 2: Views on Uses of Authentication Control

71% of respondents said their firms employed the authentication control information security strategy, with just 25% saying they did not (Figure 2). The smallest percentage, 4%, stated they were unsure if their firms employed an authentication control information security technique to protect against information security threats. In addition, the respondents were asked if their companies employed an authorization control information security method. The results are presented in Table 1.

Table 1: Views on the use of authorization

Responses	**Frequency**	**Percent**
No	24	66.67
Yes	12	33.33
Total	28	100.0

According to Table 4.21, only 33.33% of respondents' firms implement permission control, with 66.67% of respondents' organizations not using this strategy. Therefore, more of these electronic commercial organizations need to adopt this strategy. The findings are given in Table 4.22. The researcher also wanted to know if the firm used an international standard framework to handle information security.

Table 2: Views on the uses of frameworks

Responses	**Frequency**	**Percent**
Yes	5	13.89
No	30	83.33
Do not know	1	2.78
Total	36	100.0

Table 4.22's findings indicate that 13.89% of respondents, or 83.33%, admitted adopting standards or frameworks to manage information security. Therefore, these businesses must adopt standard/framework information security methodology to lessen or defeat risks.

Table 3 Views on the uses of antivirus

Responses	**Frequency**	**Percent**
Yes	31	86.11
No	5	13.89
Total	36	100.0

This indicates that a framework for implementing security in organizations engaged in electronic commerce must be created. The survey also found that most firms admitted to using antivirus information security methods, with 89.3% of respondents saying they did, while only 10.7% said their organizations did not. The results are provided in Table 3. The respondents were also asked if their companies frequently update their antivirus software. The results are provided in

Table 4: Uses of Updated Antivirus

Responses	**Frequency**	**Percent**
Yes	20	55.56
No	16	44.44
Total	36	100.0

According to the results, 55.56% of the businesses surveyed do not routinely update their antivirus software. This indicates that this strategy is ineffective even though most firms utilize antivirus.

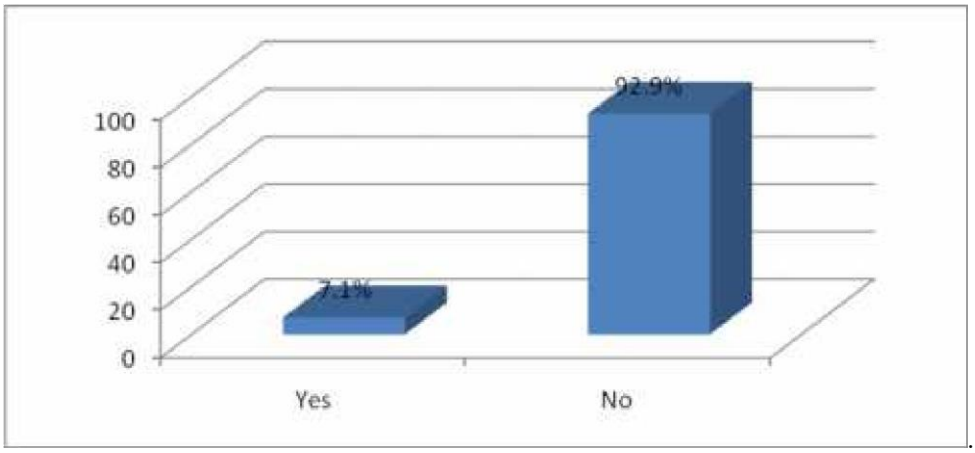

Figure 3: Views on Uses of Intrusion Detectors

Only 44.44% of businesses update their antivirus software. The usage of intrusion detectors by the respondents' organizations in their endeavor to safeguard information was also a requirement. The replies are provided in Figure 3. The least number of respondents (7.1%) used intrusion detectors to manage information security, the majority at 92.9% of the organizations

(Figure 4.18). This paints a dismal picture of the condition of information security. Therefore, it is necessary to motivate these firms to adopt this strategy to enhance information security. Additionally, the respondents needed to state if their companies employed an information security methodology for security training and education. Table 4.25 summarizes the results.

There is a need to educate these firms about the advantages of this strategy in increasing information security because most respondents (86.11%) denied that their organizations employed this technique. In comparison, just 13.89% admitted that their organizations did. Furthermore, as shown in Table 4. most respondents (83.33%) stated that their firms did not employ the risk assessment information security strategy.

Table 5: View on Use Security Education and Training

Responses	**Frequency**	**Percent**
No	31	86.11
Yes	5	13.89
Total	36	100.0

Only 16.67% of the respondents, as shown in Table 6, claimed that their companies employed a risk assessment information security methodology, whereas a staggering 83% did not. This suggests that significant efforts must be made to persuade all these businesses to include this strategy in their information security plans.

Table 6: Use of risk assessment in security management

Responses	**Frequency**	**Percent**
No	30	83.33
Yes	6	16.67
Total	36	100.0

The respondents' responses are shown in Figure 4. when asked whether their firms implemented activity monitoring and auditing using system logs or other information security measures.

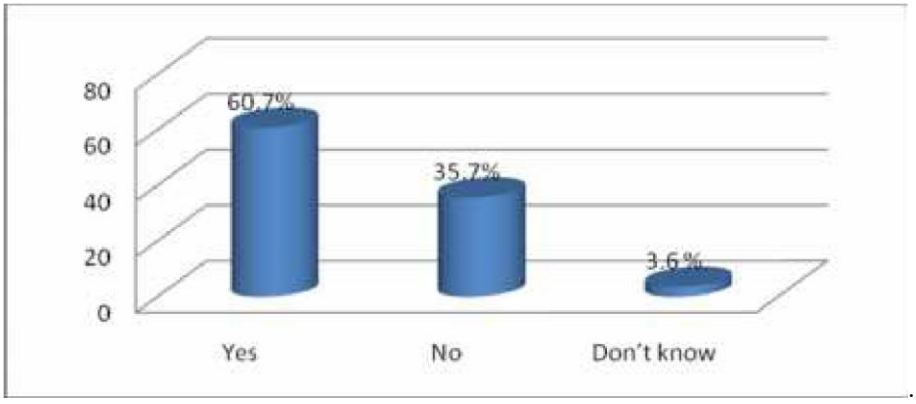

Figure 4: Views on Uses System Logs

According to Figure 4., most respondents (60.7%) acknowledged that their businesses used the strategy, whilst 35.7% said they did not. 3.6% of respondents said they were unsure if their firms employed the aforementioned strategy. So that they might gain from it, it is necessary to include all electronic business companies, especially those that do not employ the method.After that, the respondents were requested to assess their agreement with the following assertions about their organizations: First, they were requested to declare whether or not they concurred with the following: The state of information security was regularly received by senior management. Figure 5 summarizes their comments.

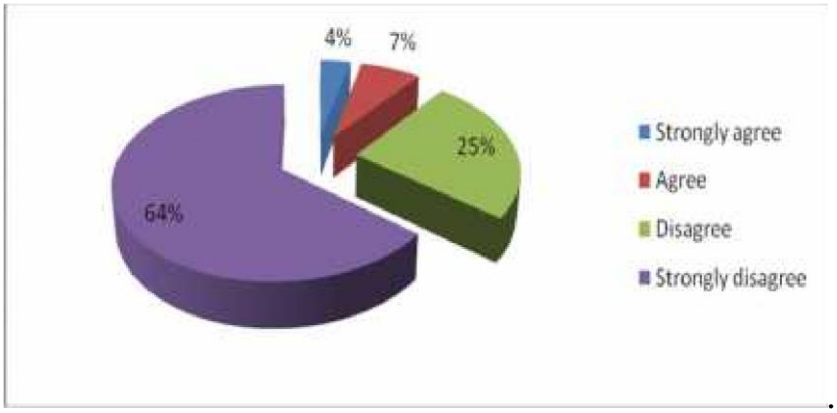

Figure 5: Views on Information Security Reporting

The results showed that 64% of the respondents strongly disagreed that senior management, followed by 25% of respondents who only disagreed, frequently received reports on the state of information security. (Figure 5) However, just 25% of the respondents said that their senior management received frequent reports on the state of information security, and 4% said they were unsure if this was the case.

Table 7: Opinion on Awareness of Information Security

Responses	**Frequency**	**Percent**
Strongly agree	15	41.67
Agree	8	22.22
Disagree	3	8.33
Strongly disagree	10	27.78
Total	36	100.0

The participants were also requested to state whether the staff members of their company recognized the value of information security. The results are shown in Table 7. According to Table 7, the plurality (41.67%) strongly agreed that their organization's workers recognized the value of information security, while only 27.78% strongly disagreed. 8.33% of respondents disagreed with the statement, leaving 22.22% favoring it. Thus, it is clear that most company employees know the significance of information security. Next, the question of whether senior management offered the necessary amount of assistance for information security was put to the respondents. Figure 6 summarizes the results.

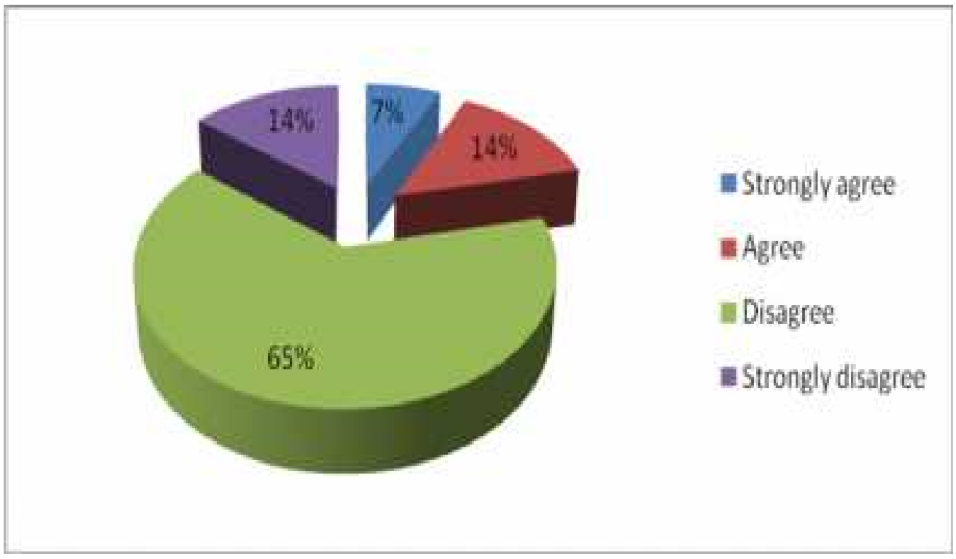

Figure 6: Views on Support of Senior Management

Most responders (65%) disagreed with the statement, with 14% strongly disagreeing. Only 14% of the respondents, including 7% who strongly agreed, agreed with the statement. This paints a poor picture of the state of affairs in these electronic commercial organizations since top management employees are typically expected to provide all the assistance required for any work to be completed. Therefore, much work must be done to address this issue and achieve greater information security.

The participants were also asked whether they agreed or disagreed that the organizations' existing techniques were acceptable and if the approaches were practical. The replies on the appropriateness and effectiveness of the methods used by organizations are summarized in Tables 8 and 9, respectively.

Table 8: Adequacy of Approaches Adopted by Our Organization

Responses	**Frequency**	**Percent**
Strongly disagree	23	63.89
Disagree	10	27.78
Agree	2	5.56
Strongly agree	1	2.78
Total	36	100.0

The majority of responders (63.89%) strongly disagreed that the organization's current practices are appropriate, while 27.78% also agreed. 5.56%, at the very least, agreed with the assertion. The replies show that the organizations' effective. present methods of operation are, in fact, insufficient. As stated in Table 9, the respondents disagreed that the organization's present strategies are

Table 9: Efficiency of Approaches Adopted by Organizations

Responses	**Frequency**	**Percent**
Strongly agree	3	8.33

Agree	6	16.67
Disagree	22	61.11
Strongly disagree	5	13.89
Total	36	100.0

The study showed that 61.11% of respondents to Table 9 disagreed that the organization's present strategies are effective. Just 16.67% of those surveyed agreed with the assertion. This suggests that the e-commerce organization's present information security practices are, in fact, insufficient, and as a result, the issue requires urgent remediation. The respondents also disagreed with Figure 4's depiction of their employees' regular information security training.

The results showed that just 7.1% of respondents strongly agreed that personnel received regular information security training, with the bulk of respondents (71.4%) strongly opposing. Staff members receive very little, if any, information security training.

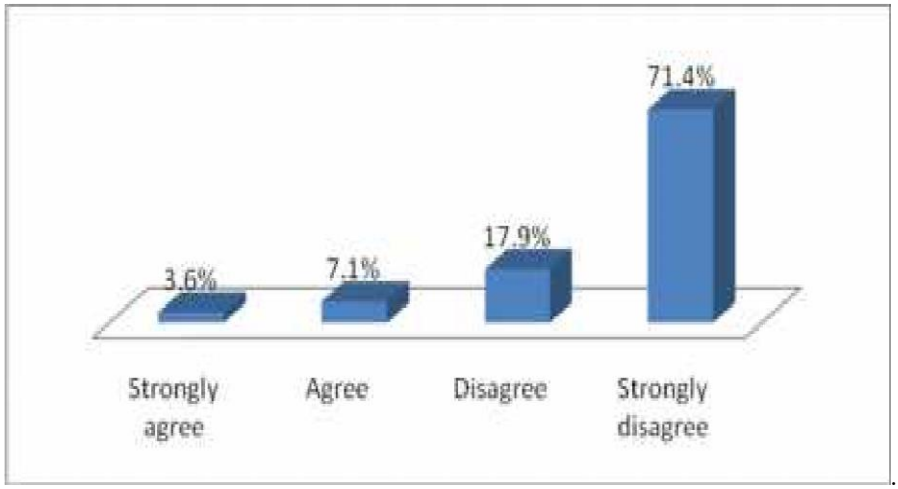

Figure 7: Views on Frequency of Training

Employees in all electronic business organizations must thus get comprehensive information security training to increase information security.

Table 10: Access Control Policy

Responses	**Frequency**	**Percent**
Yes	17	47.22
No	15	41.67
Do not know	4	11.11
Total	**36**	**100.0**

The participants were also questioned about any information security improvement initiatives implemented by their organizations. Access control was the initial policy, and it seems that most of the chosen electronic business enterprises did not have access control as a policy table 11: Policy on Authorization

Responses	Frequency	Percent
Yes	19	52.78
No	17	47.22
Total	**36**	**100.0**

A summary of the respondents' responses may be seen in Table 10. Most respondents (47.22%) stated they had one, with 47.22% confirming they did. The lowest percentage, 11.11%, claimed they were unaware of the existence of this policy in their firms. The second policy was authorization, which not all companies have, as seen in Table 11. According to Table 10, only 52.78% of respondents said their firms had an authorization policy, while 47.22% said they did not. Therefore, all electronic commercial enterprises must adopt this policy to safeguard their information. According to Figure 8, most respondents (85.7%) also said they lacked a policy on security awareness and training in education.

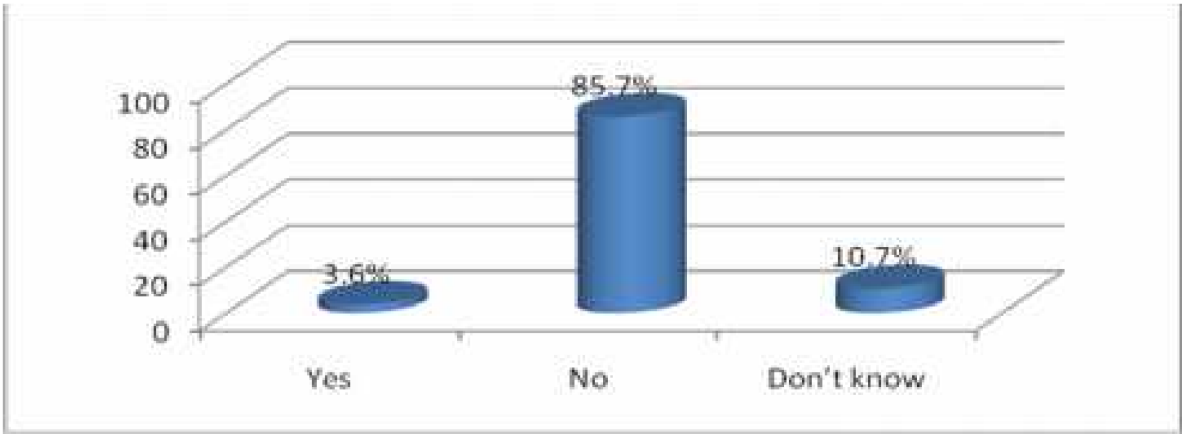

Figure 8: Policy on Education Training and Security Awareness

Only 3.6% of the respondents claimed to have such a policy, and 10.7% said they were unaware of the existence of such a policy in their firms (Table 8). According to Table 12, most respondents stated that their companies did not have an email access control policy.

Table 12: Email Usage Control

Responses	Frequency	Percent
No	27	75
Yes	9	25
Total	**36**	**100.0**

Only 25% of the participants admitted to having an email access control policy within their company, in contrast to 75%, who did not. When asked if their companies had a policy for controlling mobile devices, the respondents provided the information in Table 13.

Policy Table 13: Mobile devices Control

Response	Frequency	Percent
Yes	3	8.33
No	32	88.89
Do not know	1	2.78
Total	**36**	**100.0**

According to Table 13, just 8.33% of the respondents' organizations reported having a policy governing the use of mobile devices, and a staggering 88.89% of respondents' companies did not. According to Table 14, the respondents provided information on an antiviral policy.

Table 14: Policy on Antivirus

Responses	Frequency	Percent
No	27	75
Yes	9	25
Total	**36**	**100.0**

Most respondents (75%) stated that their firms do not have an antiviral policy, compared to 25% who said they did. This suggests that most businesses still do not take the dangers of viruses to information security seriously. The participants were also requested to state if they have a policy for the division of labor in information security management. Figure 9 shows the responses.

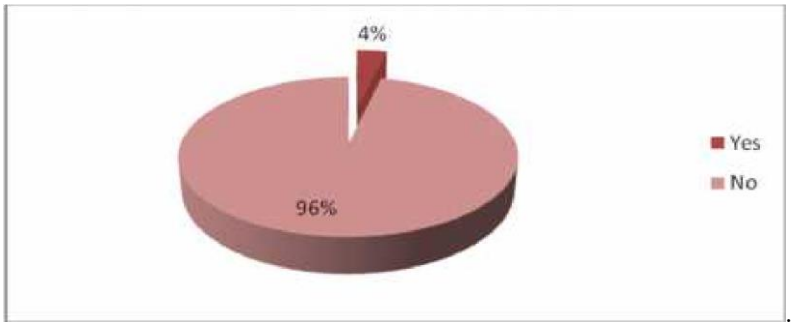

Figure 9: Separation of Duties Policy

Figure 9 shows that 96% of respondents said their organizations lacked a policy on the division of labor in information security administration, whereas only 4% said their firms did. This suggests that it may be challenging to hold someone accountable for errors or omissions since it will be difficult to identify the person who made the error because there is no division of roles in information security management. The respondents were also asked if their companies had a physical information security policy. The

results are shown in Table 15. The data in Table 15 shows that only 22.22% of the surveyed organizations reported having a physical and environmental security policy, while 77.78% did not.

Table 15: Policy on Physical and Environment Security

Responses	**Frequency**	**Percent**
No	28	77.78
Yes	8	22.22
Total	**36**	**100.0**

This highlights a significant gap, suggesting that many organizations have not implemented adequate physical security policies to safeguard against information security threats. Therefore, all electronic business organizations must prioritize developing and adopting such policies. The survey also addressed a security reporting policy, with the results are provided in Table 16.

Table 16: Policy on Security Reporting

Responses	**Frequency**	**Percent**
No	28	77.78
Yes	8	22.22
Total	36	100.0

Only 22.22% of participants said their firms had a security reporting policy, making up the majority of respondents (77.78%) who said this. This suggests that these firms' security reporting mechanisms could not be well established. The results are shown in Figure 10. Besides, the study sought to establish if the respondents' firms had a security incidents recovery policy. Figure 10 shows that only 35.7% of the respondents' firms reported having a security incidents recovery policy, whereas 60.7% of the respondents' businesses lacked one. The smallest percentage, 3.6%, claimed they were unsure if their firms had such a policy. Therefore, to protect their data, all electronic business enterprises must establish or create a policy for recovery from security incidents.

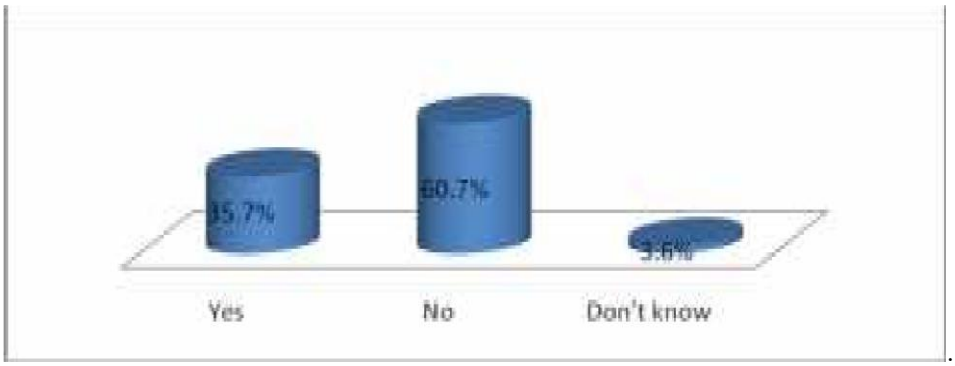

Figure 10: Policy on Security Incident Recovery

Changes Respondents Thought Would Improve Information Security in Electronic Business Organizations

Finally, participants were asked to propose changes to improve information security within their organizations. Their recommendations included raising awareness about the importance of information security, ensuring devices are logged off when not in use for extended periods, and securely disposing of sensitive customer data. They also suggested using strong, easy-to-remember passwords that do not need to be written down, assigning appropriate security permissions based on job roles, and avoiding anonymous use. Additional recommendations involved using licensed software, applying security patches regularly, installing servers in secure locations, promoting regular backups and off-site data storage, encrypting confidential customer information to safeguard data in case of hardware theft, routinely reviewing the list of users who have access to sensitive systems, conducting risk assessments, implementing employee screening, and providing frequent training on information security practices.

5. Conclusion and Recommendation

5.1 Conclusion

The survey found that firms used antiviral information security approaches to manage risks to secure electronic business transactions. In addition, it was noted that some of the methods utilized by travel and tour organizations to handle information threats included activity monitoring and audit utilizing system logs. The study discovered that most organizations have antiviral policies, even though they claim they are not recorded. However, most firms that responded to the survey did not apply a standard or framework or use an authorization control information security strategy. Additionally, most businesses did not employ an information security strategy that included intrusion detection.

Additionally, the respondents refuted the use of information security methodologies for risk assessment and security education and training inside their firms. Additionally, respondents disputed that high management received regular updates on information security. Further findings showed that the respondents believed the present methods used by their company were insufficient and ineffective. Creating a security framework to protect electronic commerce against confidentiality threats was one of this project's goals. In order to create the appropriate framework, the significant results in this chapter were mapped to the procedures of the ITIL framework as well as the the SSE capability maturity and ISO 17799 frameworks5.2

5.2 Recommendation

Based on the study's findings, it is recommended that travel and tour firms adopt a structured and standardized information security framework aligned with global best practices such as ISO 27001/ISO 17799, ITIL, and SSE-CMM. Organizations should document and implement formal security policies, introduce regular risk assessments, and establish monitoring mechanisms that include intrusion detection and activity auditing. Further, firms should strengthen governance by ensuring that top management receives periodic security updates, while also promoting a culture of security awareness through continuous staff education and training. By embedding these measures into their operational practices, businesses can enhance the confidentiality, integrity, and availability of their e-commerce platforms, thereby safeguarding electronic transactions and maintaining customer trust.

References

103309. https://doi.org/10.1016/j.cose.2024.103309 12

Admass, W. S., & Munay, Y. Y. (2023). *Cyber security: State of the art, challenges and future directions*. KeAi Communications Co. https://doi.org/10.1016/j.cld.2023.100018 5

Communications Authority of Kenya. (2024). *National cybersecurity threat assessment report*. CAK.
Kenya National Bureau of Statistics (KNBS). (2023). *Economic survey 2023: Tourism sector performance*. Government Printer.

Hayajneh, T.,et-al. (2013). Performance and information security evaluation with firewalls. *International Journal of Security and Its Applications*, *7*(6), 355-372.

Koskosas, I. (2021). Socio-technical gaps in ISO 27001 implementation: Evidence from African SMEs*. In *Proceedings of the 15th Mediterranean Conference on Information Systems* (pp. 112–125).

Muthoni, L. W., & Adebayo, A. O. (2023). *Adoption challenges of cybersecurity frameworks among SMEs in developing economies*. *Journal of Information Security and Applications*, 68, 103278.

Omondi, J. K. (2023). *Infrastructural barriers to cybersecurity implementation in Kenyan e-businesses*. *African Journal of Information Systems*, 15(2), 45–62.

Rodriguez, P., Singh, R., & Almeida, F. (2022). *ITIL adaptations in service-oriented sectors: Impact on incident response efficacy*. *International Journal of Information Management*, 64, 102457.

Smith, T. J., & Johnson, L. R. (2022). *Taxonomy of e-commerce security threats: Technical, human, and systemic dimensions*. *Computers & Security*, 117, 102691.

United Nations World Tourism Organization (UNWTO). (2023). *Global report on digital transformation in tourism*. UNWTO Publications.

Wachira, M., & Mohamed, A. H. (2024). *Payment security and third-party risks in East African tourism e-businesses*. *Journal of Cybersecurity*, 10(1), 2.