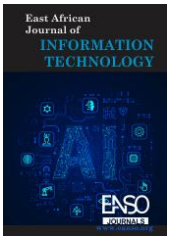


East African Journal of Information Technology
eajit.eanso.org
Volume 7, Issue 1, 2024
Print ISSN: 2707-5346 | Online ISSN: 2707-5354
Title DOI: https://doi.org/10.37284/2707-5354

EAST AFRICAN NATURE & SCIENCE ORGANIZATION

Original Article

Towards Digital Forensic Readiness: A Framework for Financial Service Providers

Georgina Odhiambo[1], Richard Omollo[1] & Paul Abuonji[1]*

[1] Jaramogi Oginga Odinga University of Science and Technology, P. O. Box 210 - 40601 Bondo – Kenya.
* Correspondence ORCID ID: https://orcid.org/0009-0004-1155-1462; email: ginakumu@gmail.com.

Article DOI: https://doi.org/10.37284/eajit.7.1.1897

Date Published:

30 April 2024

Keywords:

Cybercrime, Cybersecurity, Digital Forensic Readiness, Financial Service Providers, Information Security

ABSTRACT

Digital Forensic Readiness has widely been referred to as an organization's ability to proactively capture digital evidence and as a result, incur minimum costs of investigation in the event of incidents. However, several organizations still underestimate the usefulness of setting up their environments to be forensically ready until an incident occurs, and this often results in huge losses and costly investigations. Global trends show that financial institutions are amongst the worst-hit companies by cybercriminals, and this is attributed to one of the key motivations for cybercrime, which is financial gain. Kenya's cybercrime statistics over the past five years also show that financial services remain amongst the top hit sectors by cybercriminals. The aim of this study was to develop a Digital Forensic Readiness framework for Financial Services Providers. To achieve this, the study assessed the relevant existing frameworks to explore their strengths and gaps. Additionally, the study explored the current state of forensic readiness in Kenyan financial institutions by reviewing secondary data and analysing primary data collected from respondents in the financial services sector. The study adopted a descriptive research design with the main data collection tool being questionnaires, which were administered to respondents through an online survey. The collected data was analysed using the SPSS software 28.0.1 and a multiple regression analysis was performed to determine the influence of organizational factors, legal factors, technology, and policies on Digital Forensic Readiness. The outcome of the analysis indicated that these factors indeed had a significant effect on forensic readiness, with organizational factors and policies having more impact on the framework. The study recommended that organizations not only focus on complying with laws and implementing technological controls, but also prioritize improving forensic readiness awareness and culture, supporting forensic readiness activities, setting up training, and enforcing policies to ensure personnel compliance.

APA CITATION

Odhiambo, G., Omollo, R. & Abuonji, P. (2024). Towards Digital Forensic Readiness: A Framework for Financial Service Providers. *East African Journal of Information Technology*, *7*(1), 92-107. https://doi.org/10.37284/eajit.7.1.1897

CHICAGO CITATION

Odhiambo, Georgina, Richard Omollo and Paul Abuonji. 2024. "Towards Digital Forensic Readiness: A Framework for Financial Service Providers". *East African Journal of Information Technology* 7 (1), 92-107. https://doi.org/10.37284/eajit.7.1.1897.

Article DOI: https://doi.org/10.37284/eajit.7.1.1897

HARVARD CITATION
Odhiambo, G., Omollo, R. & Abuonji, P. (2024) "Towards Digital Forensic Readiness: A Framework for Financial Service Providers", *East African Journal of Information Technology*, 7(1), pp. 92-107. doi: 10.37284/eajit.7.1.1897.

IEEE CITATION
G. Odhiambo, R. Omollo & P. Abuonji "Towards Digital Forensic Readiness: A Framework for Financial Service Providers", *EAJIT*, vol. 7, no. 1, pp. 92-107, Apr. 2024.

MLA CITATION
Odhiambo, Georgina, Richard Omollo & Paul Abuonji "Towards Digital Forensic Readiness: A Framework for Financial Service Providers". *East African Journal of Education Studies*, Vol. 7, no. 1, Apr. 2024, pp. 92-107, doi:10.37284/eajit.7.1.1897.

INTRODUCTION

Technology has become an enabler to organizations and its benefits have attracted adoption by both large and small organizations. As technology evolves, software changes, users become more digitally savvy, and crimes committed become more sophisticated (Kazadi and Jazri 2015). Several authors have the opinion that it is impossible to completely secure systems (Alenezi et al. 2017; Emami 2016). Therefore, organizations need to prepare their environments to be able to identify attempts and capture data that may be useful in resolving incidents, strengthening systems, and making decisions. Several researchers in the past decade have emphasized the need for organizations to proactively prepare for incidents, and these efforts comprise digital forensic readiness (DFR). According to Mouhtaropoulos et al. (2011), DFR has become an indispensable part of the digital forensics discipline. A DFR posture yields admissible evidence and reduces the costs of corrective and legal actions, which are the two major objectives of DFR initially outlined by Tan (2001). Additionally, organizations can manage internal situations or incidents without the help of external security forces and thus reduce any associated costs of hiring investigators (López 2017).

Despite the benefits of DFR, several organizations have yet to implement it. Several data breaches and incidents in the past decade have been attributed to either poor implementation or the complete absence of security measures, controls, and procedures. Recent reports on cybercrime in Kenya (KPMG, 2022; Serianu, 2020, 2023) have revealed that financial service providers (FSPs) are among the worst-hit sectors by cybercriminals due to the monetary gains associated with crime in the sector. This study assessed the relevant existing frameworks to explore their strengths and gaps then proposed a framework highlighting factors that financial service providers need to consider and implement to be forensically ready. Additionally, the study explored the current state of forensic readiness in Kenyan financial institutions by conducting literature reviews and analysing data collected from respondents in the financial services sector to understand the actual practice of DFR in FSPs and make an analysis against recent statistics on cybercrime and litigations in the country.

RELATED WORK

The below frameworks and models were covered as part of the study to identify various relevant constructs, and these were used as a baseline in developing the proposed framework.

Article DOI: https://doi.org/10.37284/eajit.7.1.1897

Table 1. Digital Forensic Readiness Framework and Models

Framework/Model	Constructs			
	Technology and Infrastructure	**Organizational Factors**	**Legal Factors**	**Policies**
Rowlingson's Ten Step Approach (Rowlingson, 2004)		☒Training	☒Legal review	☒Evidence handling and storage policy ☒Escalation policy
Network Forensic Readiness framework (Endicott-Popovsky, Frincke, & Taylor, 2007)	☒Intrusion Prevention and Detection systems ☒Fault tolerant systems ☒Backup and Replication	☒Security Awareness and Training		☒Security policies ☒Incident response
Digital Forensics Management Framework (Grobler & Louwrens, 2010)	☒Infrastructure	☒Establishing management capability		☒DFR Training and Awareness strategy ☒Evidence Management plan ☒Investigation protocols ☒Risk mitigation plans
Factors Influencing DFR (Mankantshu, 2014)	☒Technology and Infrastructure	☒Corporate Governance	☒Legal and ethics	☒Policy
DFR Framework (Elyas, Ahmad, Maynard, & Lonie, 2015)	☒Technology ☒Architecture	☒Governance ☒Top Management Support ☒Culture		☒Forensic Policy
Cloud Forensic Readiness Framework (Alenezi, Hussein, Walters, & Wills, 2017)	☒Cloud infrastructure ☒Cloud architecture ☒Forensic technologies ☒Cloud security	☒Management support ☒Readiness strategy ☒Governance ☒Culture ☒Training procedures	☒Service Level Agreements ☒Jurisdiction	

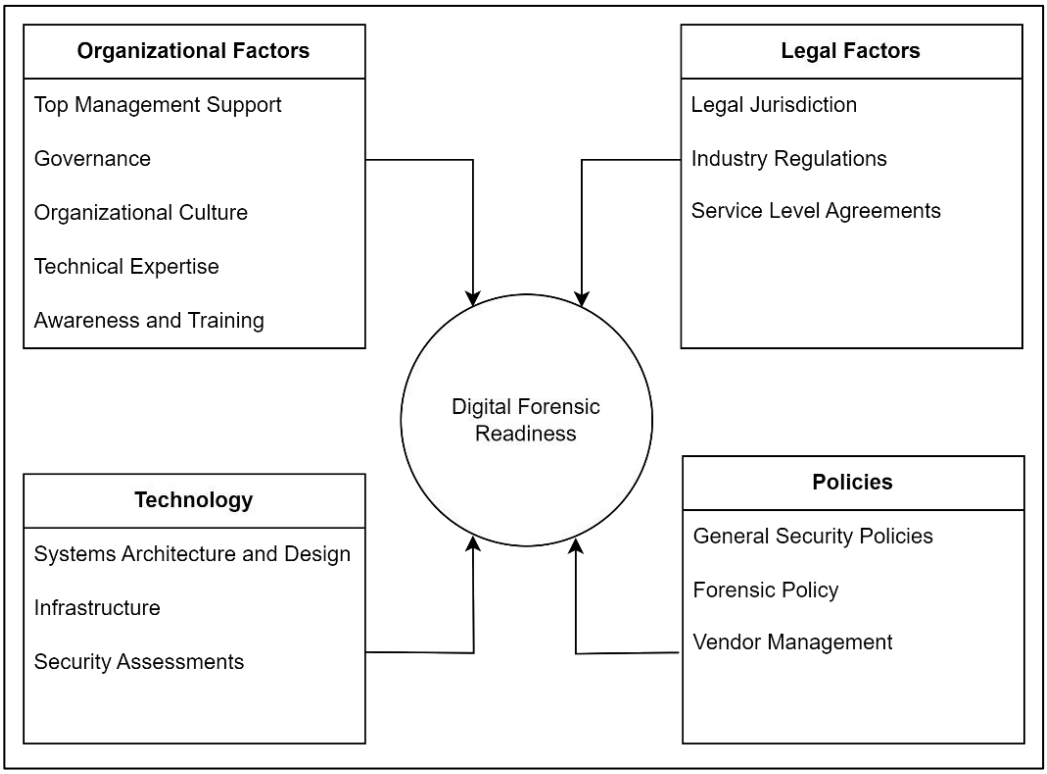
The constructs marked as ☒ appear in several frameworks and models hence considered as a good baseline for the proposed framework.
The constructs marked as ☒ are considered as important but are ideal when merged into other key constructs as they form part of a bigger picture.
Constructs marked as ☒ are very specific, and their applicability is limited if included as they are on the proposed framework.

PROPOSED FRAMEWORK

The constructs from DFR frameworks and models covered in the literature review were analysed and consolidated to form the proposed framework, with four key categories. These included Organizational Factors, Policies, Legal factors, and Technology and Infrastructure. These factors also formed the baseline for the survey questions that were used to assess the state of DFR in the financial services sector.

Article DOI: https://doi.org/10.37284/eajit.7.1.1897

Figure 1: Proposed Framework



Digital Forensic Readiness is the dependent variable in the proposed conceptual framework, with the following as the independent variables:

Organizational Factors

Top Management Support-Support from senior management is essential for the success of the DFR initiative. The top management's role, in this case, includes funding, staff allocation, resource allocation, and political backing if necessary.

Governance- This includes oversight and management of procedures and responsibilities to ensure that the forensic readiness program is effective and aligned with the business strategy.

Organizational Culture- The organization's culture includes assumptions, values, and practices that have a direct impact on forensic readiness. A good forensic culture should be instilled in an organization as part of the DFR strategy and should ideally be driven by the top management.

Technical Expertise- Experts with good knowledge of cybersecurity and forensic tools should be key to the organization's DFR program.

Awareness and Training- Various researchers have posited that humans are the weakest link in the information security chain. This is the reason why it is important for organizations to organize awareness and training programs for staff and those affiliated with the organization.

Legal Factors

Legal Jurisdiction- Organizations need to be aware of the judicial environments they are operating in and information security laws and regulations that apply to these jurisdictions. This information can be used when formulating or revising DFR and information security policies.

Industry Regulations- These are regulations and standards which are specific to industries. An example is the CBK guidelines on cybersecurity for PSPs. Industry regulations may be location-specific or cross-boundary.

Service Level Agreements- These are contracts between service providers and their customers. The contracts outline the nature of services provided by the SP and roles and responsibilities of each party.

Article DOI: https://doi.org/10.37284/eajit.7.1.1897

Technology

Various technological measures and tools can be implemented by organizations to ensure that evidence is proactively and securely captured and stored for possible use. These include:

System Architecture and Design- The organization's technical environment should include detection, prevention, and associated systems that monitor, log, prevent, report, and remediate malicious activity. Additionally, applications and systems used by the organization should be designed in a way that increases the ability of these platforms to securely capture digital evidence.

Infrastructure: Organizations should ensure that their environment provides optimal support for the implementation of systems, and that these systems are able to capture and securely store evidence.

Security Assessments- All components of an organization's technical environment should be assessed and analysed to identify potential sources of evidence. Additionally, a risk analysis should be done for each component to determine the level of impact on business processes that an incident on the organization's infrastructure may cause. Other processes to consider as part of security assessment on the technological environment include vulnerability assessments, audits, and penetration testing.

Policies

Forensic Policy- A forensic policy outlines the rules that guide processes and roles in line with forensic readiness and investigations. The policy should include a clear definition of roles in the DFR program, what evidence should be captured and how the evidence will be collected and stored, when and who to release the evidence to, and when to open a formal investigation. The policy may include other general components related to DFR.

General Security Policies- These should be aligned with the business strategy and ideally should include the forensics policy as well as other security policies including incident response, disaster recovery, and business continuity. Integration of these policies under general security policies allows for a more cohesive and coordinated response to security issues and incidents.

Vendor Management Policies- As several organizations rely on vendors for the provision of products and services, policies on onboarding procedures and vendor access to an organization's environment should be defined to manage third-party risks.

MATERIALS AND METHODS

This study adopted a descriptive research design, with the target population being IT professionals, Managers, Human Resources, Finance, and Operations personnel working in FSPs operating within Nairobi County. Institutions covered included banks (CBK 2023), Saccos (SASRA 2023), microfinance banks (Amfi, 2021), credit-only microfinance institutions (Amfi, 2021), insurance firms (IRA 2021), and payment service providers (CBK 2023).

According to Mugenda and Mugenda (2003), at least 10% of the target population is an adequate sample size for descriptive quantitative studies with a population of 1000 and below. The target number of FSPs in Nairobi was 227; this included Banks, Insurance, Microfinance Institutions, Saccos, and payment service providers. 15% of this population was studied, equaling 34 institutions. According to Balloun, Barrett, & Weinstein, (2011), researchers should target multiple respondents when studying several organizations in order to get comprehensive views. For this reason, the study additionally employed stratification, targeting 4 respondents per organization from the key departments: Human Resources, Management, Information Technology and Finance or Operations. This amounted to a total of 136 target respondents.

Data for the study was collected using a questionnaire that contained both open-ended and close-ended questions. The questionnaire was

Article DOI: https://doi.org/10.37284/eajit.7.1.1897

administered through an anonymous online survey and included sections that captured socio-demographic characteristics, organizational characteristics, Technical, Policy, and Legal Controls.

To ensure the content validity of the questionnaires administered in this study, the researcher consulted with the study supervisors, who were able to review the questionnaire's content, relevance, and objectivity. Additionally, the questions were designed based on the constructs outlined in the proposed DFR framework, ensuring that the study variables were well captured and operationalized in line with the research objectives. Data was analysed using SPSS version 26 (SPSS Inc. Chicago, IL). Descriptive statistics was used to analyse the demographic and organizational characteristics. Further analysis was conducted by subjecting the data to regression analysis.

RESULTS

Overview

The survey link to the questionnaire was shared with 136 respondents with 124 being completed and selected as fit for analysis indicating a response rate of 91.2%. In the socio-demographic characteristics, the study had a diverse range of respondents. The age of participants spans from 18 to over 55, with the majority (51.6%) falling within the 26-35 age group. In terms of education, 59.7% of respondents held a Bachelor's Degree, while 21% had a Master's Degree. On the characteristics of financial institutions, most respondents worked in Savings and Credit Cooperative Societies (Sacco's) at 21.0%, closely followed by Banks at 20.2%, Credit-only Microfinance institutions at 19.4%, Microfinance Banks and Insurance both at 15.3% and Payment Service Providers at 8.9%.

The distribution of respondents' current roles in their organizations is fairly even, with Information Technology (IT) leading at 20.97%, followed closely by Finance, Operations, and Human Resources (HR) tied at 20.16%. Management roles are the least represented at 18.55%. Notably, only 14 out of 124 respondents reported having at least one cybersecurity certification, with the majority of those (9 out of 14) working in IT, and three in management.

Looking at organization characteristics, in terms of respondents' knowledge about policies, regulations, and standards, data revealed that the highest awareness, at 27.1%, is related to The Data Protection Act, 2019. The Central Bank of Kenya Guidelines on Cybersecurity for Payment Service Providers, 2019 follows at 15%, while 14.4% of participants indicated a lack of knowledge about any of the listed policies, regulations, and standards. A more detailed breakdown by current role in *Table 2* indicates that participants in Information Technology (IT) roles exhibited the highest knowledge regarding policies, regulations, and standards, whereas participants in Operations roles had the least knowledge in this regard.

The study revealed diverse levels of organizational readiness for digital forensic programs in *Figure 2*. About 18.5% reported having fully defined programs, 28.2% had partially defined ones, 21.8% had none, and 31.5% were uncertain.

Management contributions to DFR efforts varied, with 59.7% of respondents indicating that their managers were involved in the approval and oversight of training activities, 46.8% indicating that managers engaged in information security planning and budgeting activities, and 30.6% indicating that managers supported cybersecurity and forensic readiness activities. 16.9% reported no management contributions. These findings align with the observations by Karie & Karume (2017), who also noted that management in several organizations did not consider forensic readiness as a priority, but instead focused more on what was deemed to bring more direct profits to organizations. While Mankantshu (2014) notes the criticality of top management in successfully implementing DFR, this study acknowledges management as a key component in a multi-component framework. Management plays a crucial role in DFR but is not a sole determinant.

Article DOI: https://doi.org/10.37284/eajit.7.1.1897

Instead, it is one of the several components that contribute to the effectiveness of DFR.

Table 2: Cross-tabulation of Knowledge on policies regulations and standards by current role

	What is your current role in your organization? If "Other", please specify					
	Finance	**HR**	**IT**	**Management**	**Operations**	**Total**
Central Bank of Kenya Guidelines on Cybersecurity for Payment Service Providers, 2019	8	10	14	10	6	48
ISO/IEC 27001	7	8	13	10	1	39
None of the above	5	16	9	3	13	46
The Computer Misuse and Cybercrimes Act, 2018	7	7	17	5	1	37
The Data Protection Act, 2019	18	16	24	18	11	87
The Kenya Information and Communications Act, 1998	2	9	9	8	3	31
The National ICT Policy, 2016	7	4	8	14	0	33
Total	25	25	26	23	25	124

Figure 2: Presence of DFR Programs and Strategies

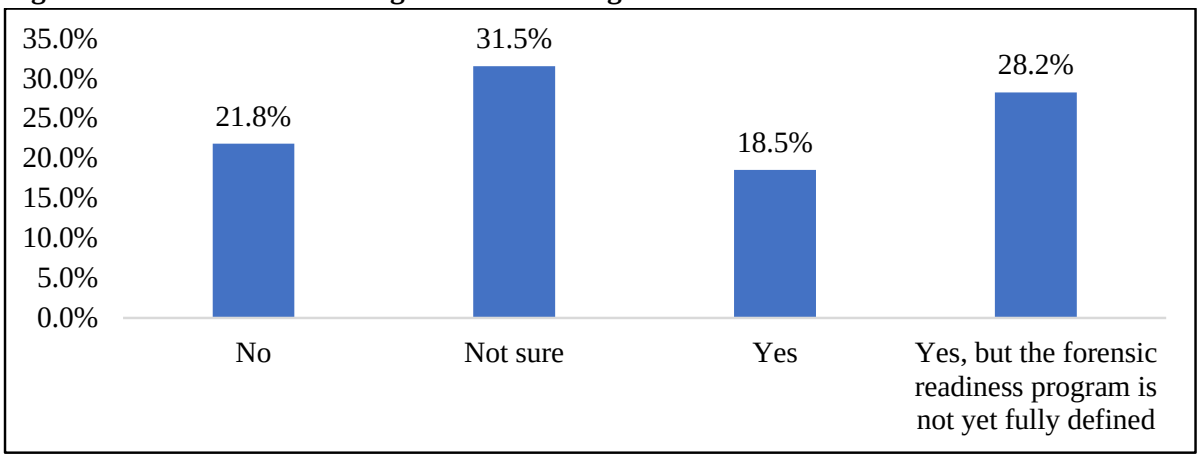


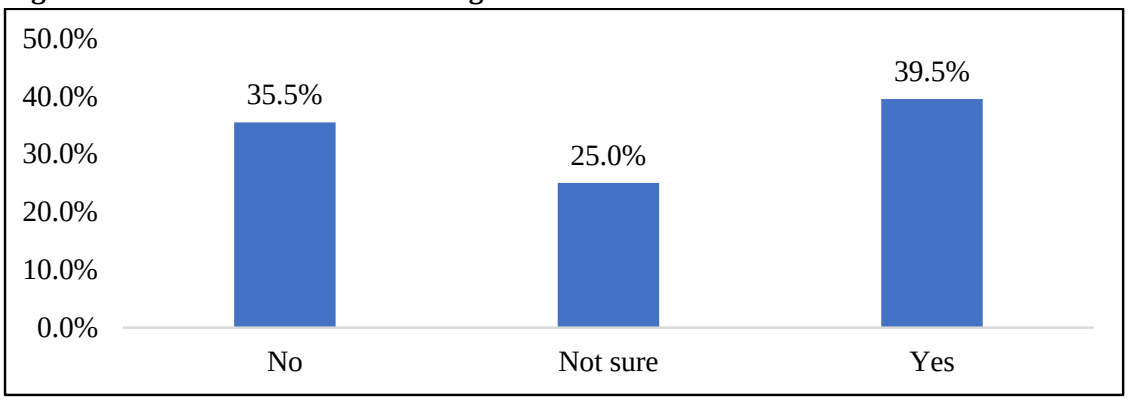
Table 3. Management contribution to DFR

	Responses		
	N	**% of respondents**	**% of total responses**
Approve and oversee training and awareness programs to all users on best practices	74	59.7%	38.3%
Engage in information security planning and budgeting activities	58	46.8%	30.1%
Support cybersecurity and forensic readiness activities	38	30.6%	19.7%
None of the above	21	16.9%	10.9%
Take part in drafting and revision of cybersecurity and forensic readiness policies	2	1.6%	1.0%
Total	193		100.0%

Forensic readiness training existed for 39.5%, 35.5% had none and 25% were not sure if it existed.

Article DOI: https://doi.org/10.37284/eajit.7.1.1897

Figure 3. Forensic Readiness Training



In terms of technical measures, 79.8% reported having anti-malware on all computers, 91.1% used firewalls, and 78.2% had email spam filters.

Table 4. Technical Measures

	N	Responses	
		% of respondents	%of total responses
Firewalls	113	91.1%	16.2%
Anti-malware on all computers	99	79.8%	14.2%
Email spam filters	97	78.2%	13.9%
User access control for all work devices	87	70.2%	12.5%
CCTVs	85	68.5%	12.2%
VPNs	70	56.5%	10.0%
Web filtering	54	43.5%	7.7%
None	38	30.6%	5.4%
Network Segmentation	37	29.8%	5.3%
Access logs	18	14.5%	2.6%
Total	698		100%

Regular planned audits on IT assets were conducted by 68.5%, with 50.7% done both internally and externally.

Table 5. Security Assessments

Variable	Category	f	%
Does the Company conduct regular, planned audits on IT assets?	No	16	12.9
	Not sure	23	18.6
	Yes	85	68.5
	Total	124	100.0
How does the Company conduct IT audits?	Both internally and externally	35	50.7
	Hire an external auditor	16	23.3
	Internally	18	26.0
	Total	69	100.0
How frequently do you conduct vulnerability Assessments?	Ad hoc	11	12.9
	Annually	23	27.1
	Biannually	7	8.2
	Monthly	7	8.2
	Not sure	26	30.6
	Quarterly	11	12.9
	Total	85	100.0

Article DOI: https://doi.org/10.37284/eajit.7.1.1897

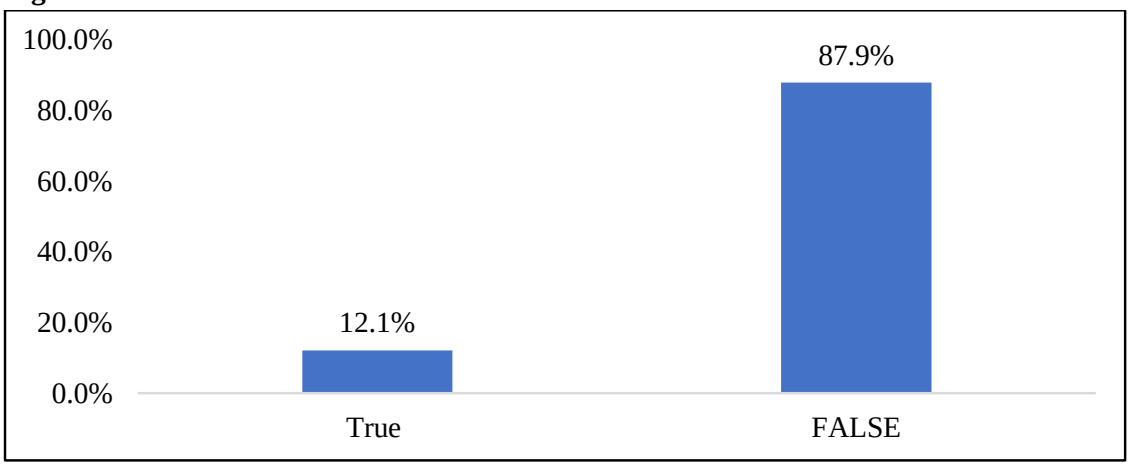
Despite best practices on IT controls and data handling, incidents were still experienced, hinting at potential compliance issues. These results support the findings from previous studies by Muraguri & Mwalili (2019) and Karie & Karume (2017), who also indicated lack of personnel compliance as a potential issue in forensic readiness.

Table 6: Data Handling

		Has your company experienced any information security incidents within the past 5 years?			
		No	**Not sure**	**Yes**	**Total**
Handling user data	All accounts for employees leaving the company are disabled or deleted	24	21	37	82
	All clients must sign an NDA with the company	8	7	33	48
	All employees are required to sign a Non-Disclosure Agreement (NDA) when joining the company	13	12	44	69
	All vendors must sign an NDA with the company	15	8	40	63
	The company handles customer/supplier data	25	29	44	98
	The company processes or stores sensitive personal data	31	23	38	92
Total		**34**	**35**	**55**	**124**

The study reveals significant insights into information security incidents within organizations. A substantial 87.9% of respondents acknowledged that their organizational operations involve financial transactions, heightening the risk of potential breaches. As indicated in several studies (Serianu, 2023; ISACA, 2020; Muraguri & Mwalili, 2019), these results also confirm that financial organizations remain among the most targeted sectors by cybercriminals due to the nature of transactions involved.

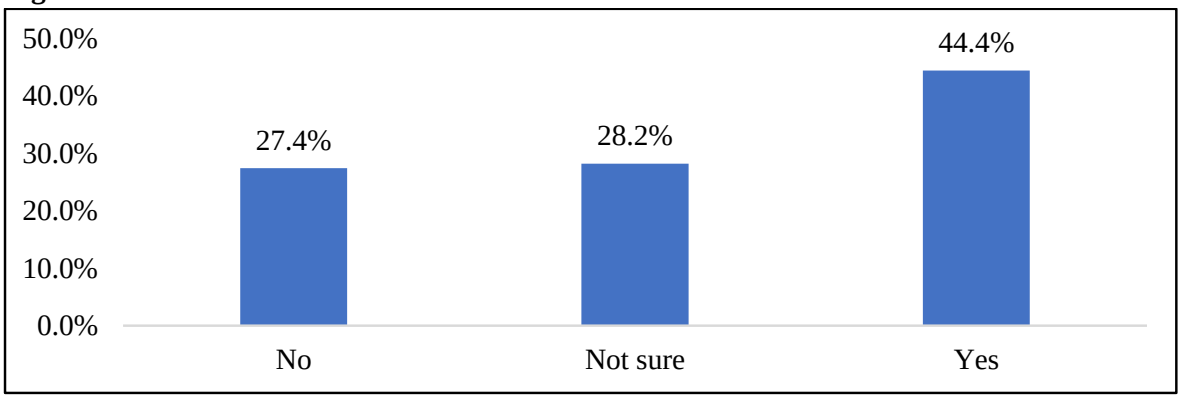
Figure 4. Risk of breaches



In *Figure 5*, 44.4% reported experiencing information security incidents within the past five years.

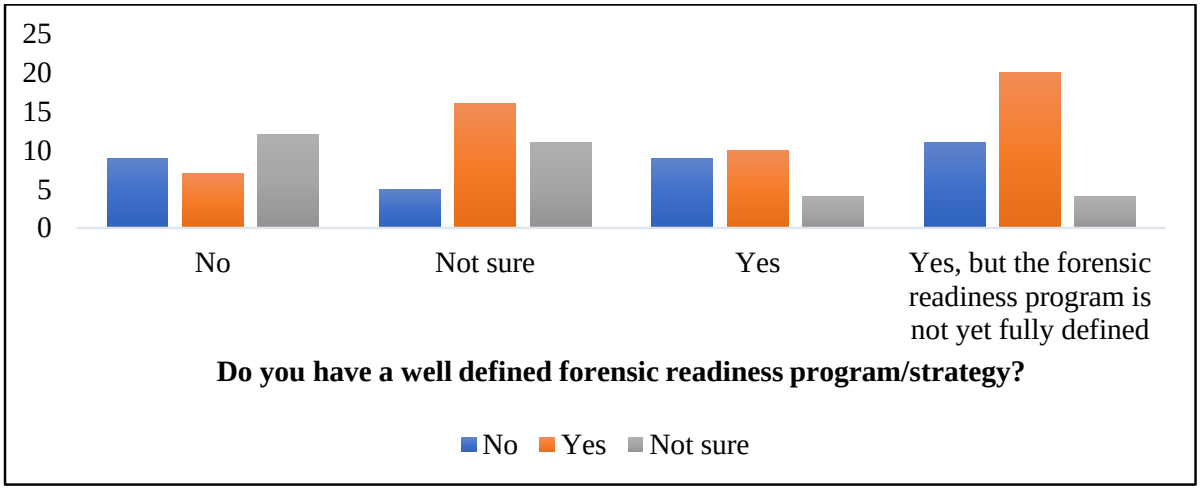
Article DOI: https://doi.org/10.37284/eajit.7.1.1897

Figure 5. Incidence occurrence



Most of the respondents in *Figure 6* below who indicated to have experienced an incident in the past five years also stated to have a forensic readiness program that was not yet fully defined. This finding aligns with the observations by López (2017), who noted that several organizations still lacked a standard mechanism to assess forensic readiness, and as such were at greater risk of experiencing incidences and incurring more losses.

Figure 6. Availability of DFR program by the occurrence of the information security incident



The study provides valuable insights into the reporting and management of information security incidents within organizations. Astonishingly, only 45.5% of the 55 incidents were reported, with 32% of the reported cases successfully prosecuted, while 64% were dismissed due to insufficient evidence. Phishing and malware incidents were most frequently reported. The primary reasons for not reporting incidents include a fear of bad publicity (53.3%), high costs yet the incidents were minor (43.3%), and internal resolution with disciplinary actions (43.3%). This outcome supports the findings by (Johnson, 2016), and the reports by Serianu (2020) and ISACA (2019), which also revealed a high rate of underreporting of incidents.

Figure 7 indicates that respondents are largely neutral (29%) about their organizations' preparedness for incidents, while over 20% agree that their organizations are prepared, and more than 30% disagree.

Article DOI: https://doi.org/10.37284/eajit.7.1.1897

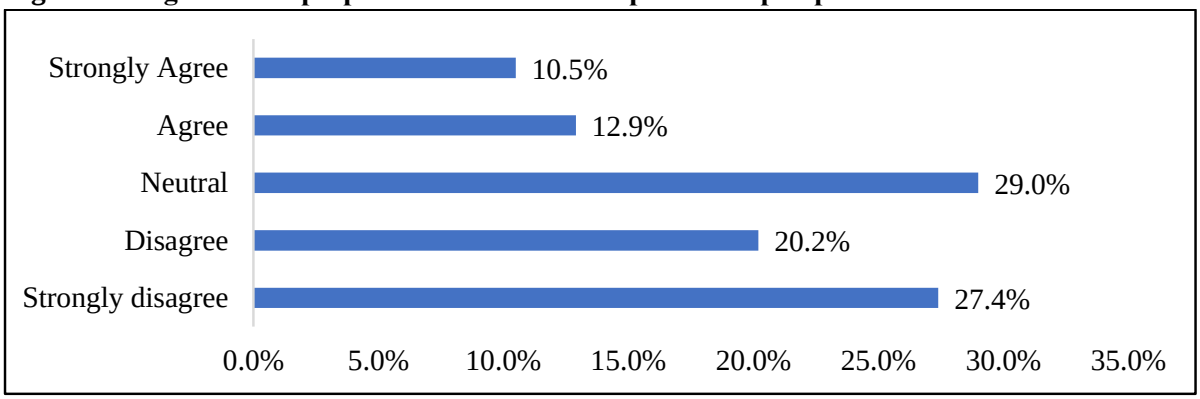
Table 7: Incident Reporting

Reported	Successfully prosecuted	Dismissed
45.5% of 55 cases	32% of 25 reported	64% of 25 reported

Table 8: Reasons for not Reporting Incidents

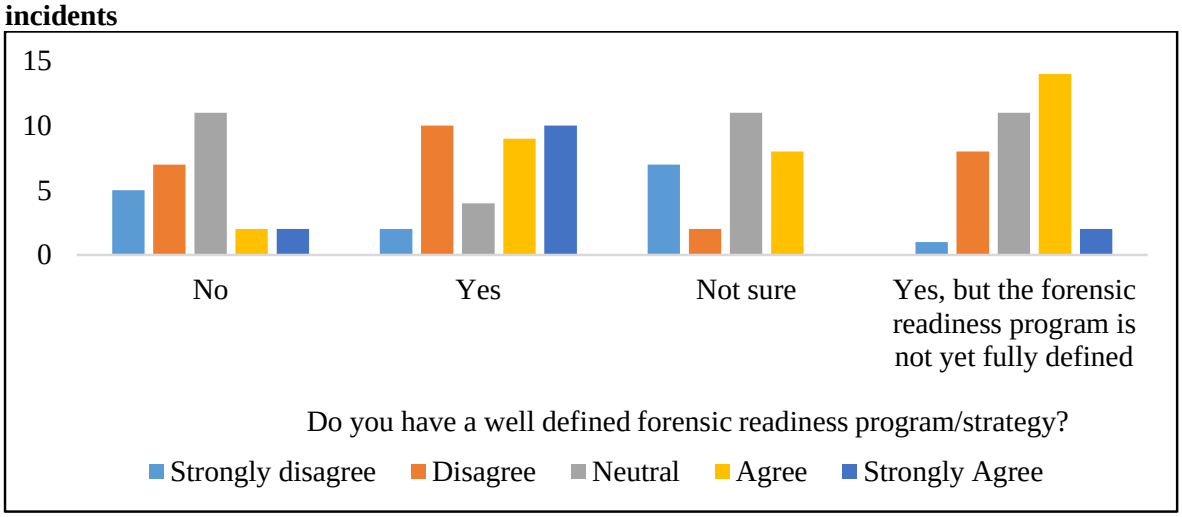
Reason	Responses		
	N	% of Respondents	% of total Reponses
Feared bad publicity	16	53.3%	35.5%
It would be costly, yet the incident was minor	13	43.3%	29.0%
Solved it internally with disciplinary actions	13	43.3%	29.0%
Didn't know who to report to	2	6.7%	4.4%
Not sure	1	3.3%	2.2%
Total	45		100.0%

Figure 7: Organization preparedness from the respondent's perspective



Further analysis in *Figure 8* reveals a correlation between strong agreement on preparedness and the presence of a well-defined forensic readiness program in organizations, highlighting the importance of comprehensive preparedness strategies.

Figure 8. Status of forensic readiness program by organization's preparedness for any potential incidents



Inferential statistics

A binomial logistic regression, also known as a logistic regression, was conducted after ensuring the data met the following assumptions:

Assumption #1: Your dependent variable should be measured on a dichotomous scale.

In this analysis the dependent variable was derived from the question; do you have a well-

Article DOI: https://doi.org/10.37284/eajit.7.1.1897

defined forensic readiness program/strategy? In the questionnaire, this variable had four categories YES, NO, Not sure, and yes, but the forensic readiness program is not yet fully defined.

Table 9*:* Dependent Variable

Original Variables	Variables used in the regression
No	No–coded to 0
Not sure	Coded as a missing value
Yes, but the forensic readiness program is not yet fully defined	Yes- coded to 1
Yes	Yes- coded to 1

Recoding the values into different variables enabled creating of a dichotomous scale of "Yes" and "No" for the dependent variable. It is also important to note that, for the purpose of the regression analysis, the two choices "yes" and "yes, but not yet fully defined" were combined. This was done with the assumption that a program/strategy can be considered well-defined with clear essential components, even though it might not yet be fully defined with all components comprehensively incorporated.

Assumption #2: You have one or more independent variables, which can be either continuous (i.e., an interval or ratio variable) or categorical (i.e., an ordinal or nominal variable).

For the independent variables the question, "Below is a list of some of the measures that constitute a good DFR program. Please select all that are currently implemented in your company". The question was designed to allow multiple responses which were then coded as follows.

Table 10: Grouping of independent variables.

Categories	Grouped into	
	Factor	
Access to data/evidence is restricted	Technology	1
All applications must pass security testing before use	Technology	1
Digital forensic readiness techniques and tools such as antimalware, intrusion detection and prevention systems have been implemented	Technology	1
None of the above measures is implemented in the organization		0
Not sure		Missing value
The company has a well-defined business continuity plan	Policy	2
The company has a well-defined DFR policy	Policy	2
The company offers staff training and guidance on their roles in forensic readiness	Organizational	3
The company's security policy complies with government and industry regulations	Legal	4
The Information security objectives are aligned with the overall company objectives	Policy	2
The root cause of all incidents, even those considered minor is always investigated	Policy	2
There is a well-defined and documented digital forensic investigations protocol to be followed in the event of an incident	Policy	2
Users are trained on information security best practices	Organizational	3

New variables were computed under the four factors: Organizational factors, Legal Factors, Technology and Infrastructure, and Policy. Points were computed for each factor given the number of times they were chosen by an individual respondent.

For the regression equation, there were four independent continuous variables;

Article DOI: https://doi.org/10.37284/eajit.7.1.1897

$Y= \beta0+\beta1X1+ \beta2X2+ \beta3X3+ \beta4X4+\varepsilon$

Where: Y= DFR (the bivariate dependent variable), β0=Constant, β1, β2, β3, β4= regression coefficients, X1, X2, X3, X4= Organizational factors, Legal factors, Technology, Policies (the independent variables in the study), ε=Error term

Assumption #3: You should have independence of observations and the dependent variable should have mutually exclusive and exhaustive categories.

Assumption #4: There has to be a linear relationship between any continuous independent variables and the logit transformation of the dependent variable, use the Box-Tidwell (1962) procedure to test for linearity.

Table 11: Variables in the equation

		Score	df	Sig.
Variables	Organization	.833	1	.361
	Legal	.833	1	.361
	Tech	.000	1	1.000
	Policy	2.596	1	.107
	LNORG by Organization	.833	1	.361
	LNLEGAL by Legal	.833	1	.361
	LNTECH by Tech	.026	1	.872
	LNP by Policy	2.395	1	.122

All the values in bold under the significance (Sig.) column are greater than 0.05 therefore this assumption was not violated.

Binary Logistic Regression

The provided classification table below summarizes the performance of a predictive model used to distinguish between organizations with a well-defined DFR (Digital Forensic Readiness) and those without. The table presents the observed and predicted outcomes, with "No" representing the absence of a well-defined DFR and "Yes" indicating its presence.

Table 12: Classification Table

Do you have a well-defined DFR?			Predicted		
	Observed		No	Yes	Percentage Correct
Step 1	Do you have a well-defined DFR	No	14	13	51.9
		Yes	13	46	78.0
	Overall Percentage				69.8

The cut value is .500

The results of the model's predictions are as follows:

- True Positives (TP): The model correctly predicted 46 cases where organizations had a well-defined DFR.
- True Negatives (TN): The model correctly predicted 14 cases where organizations lacked a well-defined DFR.
- False Positives (FP): The model incorrectly predicted 13 cases as having a well-defined DFR, but these organizations did not actually have one.
- False Negatives (FN): The model incorrectly predicted 13 cases as lacking a well-defined DFR, but these organizations did have one.

Article DOI: https://doi.org/10.37284/eajit.7.1.1897

The overall accuracy of the predictive model was found to be 69.8%, indicating its ability to correctly classify approximately 69.8% of the cases based on their DFR status.

The table below shows that this model is statistically significant for the variables in the equation with 0.001(p) <0.05.

Table 13: Variables in the Equation

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 0	Constant	.782	.232	11.319	1	.001	2.185

Looking at variables in the equation, note that the Predicted Probability is of Membership for Yes. According to *Table 14* below, The Wald test ("Wald" column) is used to determine statistical significance for each of the independent variables. The statistical significance of the test is found in the "Sig." column. From these results, organizational factors (p = .031) and Policy (p = .001), added significantly to the model/prediction but Legal (p = .789) and Technology (p = .871) did not add significantly to the model.

Table 14: Variables in the Equation

		B	S.E.	Wald	df	Sig.	Exp(B)	95% C.I.for EXP(B)	
								Lower	Upper
Step 1[a]	Organization	.967	.447	4.677	1	.031	2.631	1.095	6.321
	Legal	.165	.596	.077	1	.782	1.179	.367	3.794
	Tech	-.035	.215	.026	1	.871	.966	.634	1.472
	Policy	.778	.233	11.171	1	.001	2.177	1.380	3.437
	Constant	-1.134	.581	3.812	1	.051	.322		

a. Variable(s) entered on step 1: Organization, Legal, Tech, and Policy.

Table 15 below is the result of the Hosmer and Lemeshow Test performed to assess the goodness of fit of the logistic regression model. The p-value of the test is 0.314, which is greater than 0.05. This shows that the logistic regression model provides a good fit to the observed data.

Table 15: Hosmer and Lemeshow Test (Sweet and Martin 1999)

Step	Chi-square	Df	Sig.
1	8.221	7	.314

5.0 CONCLUSION

Based on the results of this study, it is evident that the organizational, legal, policy, and technological factors in the proposed framework indeed have an influence on DFR. The degree of significance, however, as shown in the results differs, with organizational factors and policies having a higher influence on forensic readiness and technological and legal factors having a slightly lower effect on DFR. This implies that even if legal compliance and technical measures are in place, people still play a huge role in ensuring the success of DFR programs. Therefore, it is imperative that organizations not only bolster their technical defenses but also prioritize the development of a proactive and resilient DFR culture.

REFERENCES

Alenezi, A., Hussein, R. K., Walters, R. J., & Wills, G. B. (2017). A framework for cloud forensic readiness in organizations. *2017 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering* (pp. 199--204). IEEE.

Amfi. (2021). *The Association for Microfinance Institutions (Amfi) Kenya*. Retrieved December 6, 2021, from https://amfikenya.c

Article DOI: https://doi.org/10.37284/eajit.7.1.1897

om/membership- categories/#159587011441 4-c9c0a307-77d0

Balloun, J. L., Barrett, H., & Weinstein, A. (2011). One is not enough: The need for multiple respondents in survey research of organizations. *Journal of Modern Applied Statistical Methods*, 26.

CBK. (2023). *Directory of Authorized Payment Service Providers (PSPs).* Retrieved February 15, 2023, from Central Bank of Kenya: https://www.centralbank.go.ke/wp-content/uploads/2023/02/Directory-of-Authorized-Payment-Service-Providers-February-2023.pdf

Elyas, M., Ahmad, A., Maynard, S. B., & Lonie, A. (2015). Digital forensic readiness: Expert perspectives on a theoretical framework. *Computers \& Security*, 70-89.

Emami, M. S. (2016). Importance of Hardware Systems and Circuits in Secure Software Development Life Cycle. *International Journal of Computer and Systems Engineering*, 1608-1611.

Endicott-Popovsky, B., Frincke, D. A., & Taylor, C. A. (2007). A Theoretical Framework for Organizational Network Forensic Readiness. *JCP*, 1--11.

Grobler, C., & Louwrens, C. (2010). A multi-component view of digital forensics. In *International Conference on Availability, Reliability, and Security* (pp. 647--652).

IRA. (2021). *Licensed Insurance Companies.* Retrieved December 6, 2021, from Insurance Regulatory Authority: https://www.ira.go.ke/ images/LICENCED-INSURANCE-COMPANIES-2021.pdf

ISACA. (2019). *State of Cybersecurity Part 2: Current Trends in Attacks, Awareness and Governance*. Retrieved October 2021, from https://www.isaca.org/- /media/files/isacadp/ project/isaca/why-isaca/surveys-and-reports/state-of-cybersecurity-2019-part-2_res_eng_0619#:~:text=Is%20your%20enterprise%20experiencing%20an,compared%20to%20a%20year%20ago%3F&text=enterprises%20are%20very%20li

ISACA. (2020). *State of Cybersecurity 2020 Part 2: Threat Landscape and Security Practices.* Retrieved November 4, 2021, from ISACA: https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpsc202

Kazadi, J. M., & Jazri, H. (2015). Using digital forensic readiness model to increase the forensic readiness of a computer system. In *2015 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)* (pp. 131-137). IEEE.

Karie, N. M., & Karume, S. M. (2017). Digital Forensic Readiness in Organizations: Issues and Challenges. *Journal of Digital Forensics, Security \& Law, 12*(4), 43-53.

KPMG. (2022). *Africa Cyber Security Outlook.* Retrieved 09 03, 2022, from https://assets.kpmg.com/content/dam/kpmg/ke/pdf/thought- leaderships/2022/KPMG%20Africa%20Cyber%20Security%20Outlook%202022.pdf

López, A. F. (2017). Are You Ready?: A Proposed Framework for the Assessment of Digital Forensic Readiness.

Mankantshu, M. A. (2014). Investigating the factors that influence digital forensic readiness in a South African organisation.

Mouhtaropoulos, A. a.-T. (2011). Digital forensic readiness: an insight into governmental and academic initiatives. In *2011 European Intelligence and Security Informatics Conference* (pp. 191-196). IEEE.

Mugenda, O. M., & Mugenda, A. G. (2003). Quantitative and qualitative approaches. *Nairobi: Acts Press*.

Muraguri, N., & Mwalili, T. a. (2019). Factors influencing cybersecurity readiness in deposit taking savings and credit cooperatives: A case study of Nairobi County. *International*

Article DOI: https://doi.org/10.37284/eajit.7.1.1897

Academic Journal of Information Systems and Technology, 157--182.

Rowlingson, R. (2004). A ten step process for forensic readiness. *International Journal of Digital Evidence*, 1--28.

SASRA. (2023). *List of Licensed and Authorized Sacco Societies In Kenya For the Financial Year Ending 31st December 2023.* Retrieved February 15, 2023, from Sacco Societies Regulatory Authority: https://www.sasra.go.ke/download/list-of-licensed-and-authorized-sacco-societies-in-kenya-for-the-financial-year-ending-31st-december-2023/

Serianu. (2020). *Africa Cybersecurity Report - Kenya.* Retrieved from https://www.serianu.com/downloads/KenyaCyberSecurityReport2020.pdf.

Serianu. (2023). *Africa Cybersecurity Report-Kenya.* Retrieved January 2024, from https://www.serianu.com/downloads/KenyaCyberSecurityReport2023.pdf

Sweet, S. A., & Grace-Martin, K. (1999). *Data analysis with SPSS.* Allyn \& Bacon Boston, MA, USA.

Tan, J. (2001). Forensic readiness. *Cambridge, MA: @ Stake*, 1-23.

The Republic of Kenya. (2018). Computer Misuse and Cybercrimes Act.

The Republic of Kenya. (2019). Data Protection Act.

The Republic of Kenya. (2019). National ICT Policy.

