Role of Cyber Security and Digital Forensic in Managerial Practices

Dr. Pooja P. Talreja[1], Shrushti Shetty[2], Rohin Agarwal[3], Tulsipriya Naidu[4]

[1]Fravashi Academy, Nashik
Email: *poojagopwani[at]gmail.com*

[2]Fravashi Academy, Nashik
Email: *shrushtishetty2007[at]gmail.com*

[3]Fravashi Academy, Nashik
Email: *rohinaggarwal1502[at]gmail.com*

[4]Lady Shriram College for Women, University of Delhi
Email: *tulsipriya2006[at]gmail.com*

Abstract: ***This paper examines how cybersecurity and digital forensics are integrated into managerial practices to protect organizational assets, preserve business continuity, and support decision-making after incidents. Combining recent empirical and review literature, the paper outlines adoption of cyber governance and forensics readiness by managers, frameworks and tools that support proactive and reactive measures, challenges (technical, legal, organizational), and concrete managerial policies and practice recommendations. The analysis shows that effective cybersecurity governance increases corporate value and reputation, while a forensic-ready posture shortens incident response, improves legal outcomes, and informs strategic risk decisions. An overview of forensic computing is provided, along with a discussion of important factors to take into account when conducting forensic investigations and analyzing digital evidence. The article also discusses important aspects of the administrative implications of forensic computing and identifies recommended practices for the digital forensics investigation process.***

Keywords: Cybersecurity Governance, Digital Forensics, Incident Response, Managerial Practices, Forensic Readiness, Corporate Risk Management

1. Introduction

In response to the rise in unwanted activity in computer and information systems, a new field of computer science called "digital forensics" was created. Computer attacks and cybercrimes are constantly expanding because to the growing reliance of society and industry on information technology, as well as the fact that e-commerce and online business have become crucial components of today's global business. The legal system, law enforcement, computer forensics, and investigations appear to be lagging behind in their attempts to locate offenders and successfully punish them for a variety of reasons.

Businesses, governments, and individuals alike are increasingly concerned about cyber security breaches in the current digital era. Digital forensics plays an equally important role in recognizing, analyzing, and mitigating cyberattacks as preventive measures. The principles of digital forensics, its function in cyber security, and its contribution to a safe digital environment are all covered in this article. https://www.webasha.com/blog/the-role-of-digital-forensics-in-cybersecurity

Value chains have changed as a result of digital transformation, resulting in new attack surfaces as well as increased efficiency. Managers today have to deal with operational (business continuity), legal (regulatory fines), strategic (brand and market value), and reputational cyber issues. As a result, managerial decision-making now heavily relies on two complimentary domains: cybersecurity (prevent, detect, respond) and digital forensics (examine, preserve evidence, support litigation). Strong cybersecurity governance is linked to increased corporate market value, according to recent empirical research, highlighting the significance of cyber programs at the board and management levels (Tan, W., 2025).

2. Theoretical framework and managerial lenses

In order to maximize predicted company value under cyber risk, managers make decisions about resource allocation and policy. This study adopts a risk-governance perspective. There are three essential managerial skills:

1) Governance and oversight, including compliance, cyber risk metrics, and board policies.
2) Operational cybersecurity: reaction (CSIRT/IR playbooks), detection (monitoring), and prevention (controls).
3) Forensic Readiness & Learning: post-incident analysis flowing back into controls and strategic planning, chain-of-custody protocols, and evidence preservation.

These competencies work together: operational teams put controls in place, forensic procedures convert incidents into management intelligence, and governance sets priorities and budgets.

2.1. Meaning of Digital Forensics

Identification, preservation, analysis, and presentation of electronic data are all part of the specialist field of forensic

Paper ID: SC26211103850 DOI: https://dx.doi.org/10.21275/SC26211103850

science known as "digital forensics." Finding proof of cybercrimes including fraud, hacking, data breaches, and even insider threats is crucial (https://www.webasha.com/blog/the-role-of-digital-forensics-in- cybersecurity).

The process of gathering and examining digital evidence while preserving its integrity and admissibility in court is known as “digital forensics”. One area of forensic science is digital forensics. It can assist with criminal and civil investigations in addition to being used to look into cybercrimes. While law enforcement organizations may employ digital forensics to examine data from a murder suspect's devices, cyber security teams can use it to identify the cybercriminals responsible for a malware assault. Because it handles digital evidence just like any other type of evidence, digital forensics offers a wide range of uses. When gathering tangible evidence from a crime scene, officials adhere to certain protocols. To guarantee correct handling and defense against tampering, digital forensics investigators follow a stringent forensics procedure called a chain of custody. Digital forensics and computer forensics are often referred to interchangeably. However, digital forensics technically involves gathering evidence from any digital device, whereas computer forensics involves gathering evidence specifically from computing devices, such as computers, tablets, mobile phones and devices with a CPU.

A new field in cyber security called "digital forensics and incident response" (DFIR) integrates incident response and computer forensics to improve cyber security operations. It ensures that any associated digital evidence is not compromised while speeding up the remediation of cyber threats.

2.1.1. Types of Digital Forensic Investigations

A variety of specialist fields that focus on various facets of digital forensics are included in digital forensic investigations. To tackle certain problems, each kind uses distinct investigation methods and resources. These various forensic disciplines, which range from examining data traffic in networks to closely examining home PCs, studying mobile devices, and probing cloud storage, all work together to bolster cybersecurity defenses. Examples of digital forensic investigations include the following:

a) Network Forensics
b) Mobile Device Forensics
c) Cloud Forensics

2.1.2. The Role of Digital Forensics in Cybersecurity

Learn how important digital forensics is to cybersecurity. Discover how digital forensic methods aid in data recovery, threat identification, cybercrime investigation, and legal compliance. Examine the procedures, resources, and practical uses of digital forensics in protecting the digital world (Cyber Security & Ethical Hacking , 2024)

2.1.3. Importance of Digital Forensics in Cybersecurity

By providing solutions that go beyond simply locating and addressing cyber incidents, digital forensics is essential to bolstering cybersecurity. It assists companies in creating a more robust digital framework by identifying evidence, assessing weaknesses, and offering practical insights. Some of these include:

Reducing Potential Hazards
a) Implementing Responsibility
b) Encouraging Adherence
c) Improving Reaction to Incidents

3. Managerial roles for cybersecurity

3.1 Strategic planning & investment decisions

Managers must approach cybersecurity as a capital investment, matching security initiatives to risk tolerances, calculating anticipated losses, and assessing return on investment using metrics (e.g., mean time to detect/contain, vulnerability remediation timelines). Research indicates that companies with proactive cybersecurity governance can get a market premium. (Tan, W., 2025).

3.2 Policy, compliance, and reporting

Policies for data classification, access control, incident reporting, and regulatory compliance (such as data protection regulations) are created by managers. Clear escalation procedures and transparent reporting minimize legal risk while preserving stakeholder confidence. The focus of national studies and CERT is on practical suggestions for industries that are rapidly digitizing. (Digital Threat Report, 2024.)

3.3 Culture and human factors

Phishing simulations, role-based training, senior sponsorship, and a security- conscious staff all contribute to cybersecurity effectiveness. Managers are required to include security into procurement choices and performance metrics.

4. Managerial roles for digital forensics

4.1 Forensic readiness planning

Forensic readiness procedures that guarantee logs, system pictures, and pertinent metadata are collected and stored with the least amount of disturbance to business operations should be mandated by managers. Corporate adoption templates are offered by frameworks like D4I and the literature on forensic readiness (Dimitriadis, et. al., 2020).

4.2 Coordination with legal and HR functions

Legal, regulatory, and disciplinary areas are frequently touched by forensic investigations. In order to control external reporting and guarantee the admissibility of evidence, managers coordinate communications, HR, and legal counsel.

4.3 Post-incident learning & governance

Timelines, root-cause, and TTPs are examples of forensic outputs that are used as inputs in management choices on future investments, contractual clauses, vendor modifications, product fixes, and insurance claims.

5. Literature Review

5.1 Cyber security as a managerial concern

Corporate-level cyber governance—policies, board oversight, risk metrics, and alignment with business strategy—correlates with stakeholder trust and market valuation. The literature from business, accounting, and management journals increasingly frames cyber security as a governance and strategic issue rather than just a technical IT problem (Tan, W., 2025).

5.2 Digital forensics: beyond law enforcement

Digital forensics, which was first focused on law enforcement, is now used for internal investigations, regulatory compliance, breach attribution, and risk reduction lessons learned. The necessity for process models that are both managerially practical and scientifically defendable is highlighted by scholarly evaluations and frameworks (such as D4I and cloud forensics) (Dimitriadis, et. al., 2020).

5.3 Convergence: incident response and forensic readiness

Modern frameworks heavily emphasize integrating prevention, detection, response, and forensic preparation in order to preserve evidence with the least amount of disruption to business activities. Reviews show that companies with proven forensic readiness minimize time-to-contain and improve legal defensibility (Tariq, et. al., 2023).

6. Research Methodology

In this field, managerial research combines quantitative measures stock reactions, financial impact, and event frequency with qualitative method. Mixed-methods studies, event studies on breach announcements, and bibliometric reviews mapping changing management concerns are examples of best-practice academic techniques. Total 91 responses have received out of the 100 respondents. Through 2024–2025, there will be a significant increase in business-focused cybersecurity research, according to recent systematic evaluations (Chotia, V., 2025).

7. Objective of the Study

To find the impact of cyber security and digital forensic in managerial Practices.

8. Hypothesis of the Study

There is no impact of cyber security and digital forensic in managerial Practices.

9. Analysis and Interpretation of Data

9.1. Detail description of demographic profile of the respondents

Table 1: Demographic Profile of the Respondents

S. No	Group	No. of Respondents	Percentage
1.	**Gender**		
	Male	56	61%
	Female	36	39%
2.	**Age**		
	Below 25	30	33%
	26- 35	25	27%
	36 -45	15	16%
	46 – 55	16	17%
	Above 56	6	7%
3.	**Education**		
	Undergraduate	10	11%
	Graduate	15	16%
	Post Graduate	35	38%
	Professionals	32	35%
4.	**Current Job Position**		
	Entry-level	11	12%
	Mid-level Manager	24	26%
	Senior Manager	18	20%
	Executive	20	22%
	IT Specialist	19	21%
5.	**Work Experience**		
	Less than 2 years	12	13%
	2–5 years	25	27%
	6–10 years	31	34%
	More than 10 years	24	26%

(Source: Primary data)

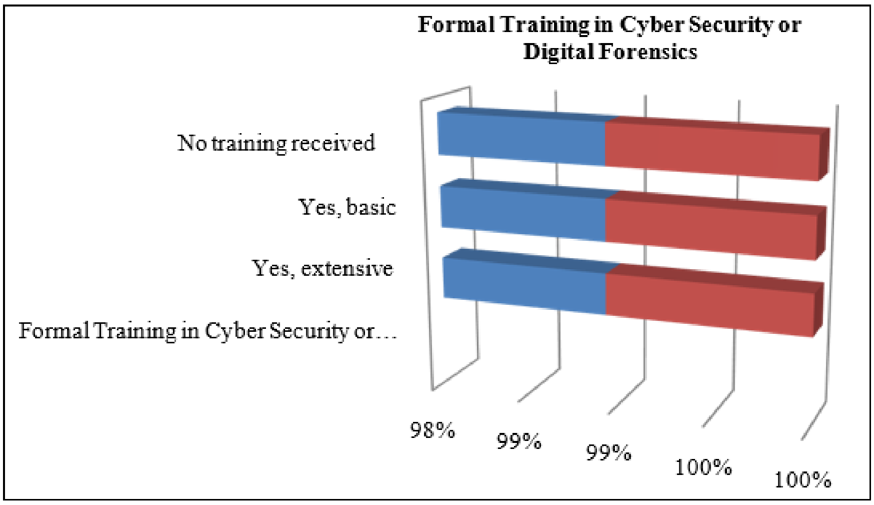
The above data has presents the basic information related to age, gender, education, job position and work experience of the respondents.

Table 2: Formal Training in Cyber Security or Digital Forensics

Group	No. of Respondents	Percentage
Yes, extensive	56	61%
Yes, basic	29	32%
No training received	7	8%
Total	92	100%

(Source: Primary data)

The above table depicted that 61% of the respondents faces extensive formal training in cyber security or digital forensics, whereas very low 7% respondents have not faces any formal training in cyber security or digital forensics.

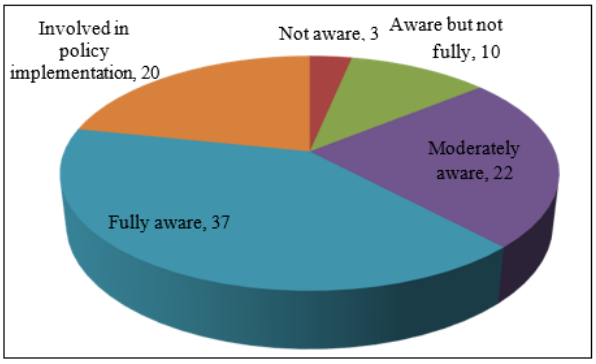


(Source: Primary data)

Table 3: Awareness of Your Organization's Cyber Security Policies

Group	No. of Respondents	Percentage
Not aware	3	3%
Aware but not fully	10	11%
Moderately aware	22	24%
Fully aware	37	40%
Involved in policy implementation	20	22%
Total	92	100%

(Source: Primary data)



(Source: Primary data)

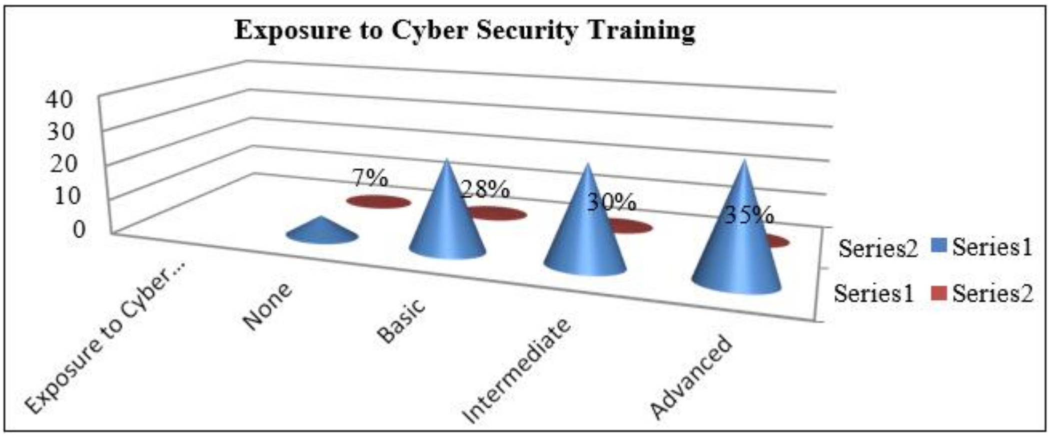
The above table depicted that 40% of the respondents aware about organisation's cyber security policies, whereas very low 3% respondents have not aware about organisation's cyber security policies.

Table 4: Exposure to Cyber Security Training

Group	No. of Respondents	Percentage
None	6	7%
Basic	26	28%
Intermediate	28	30%
Advanced	32	35%
Total	**92**	**100%**

(Source: Primary data)

The above table depicted that 35% of the respondents have faces and adopted exposure to cyber security training, whereas very low 7% of the respondents have faces and adopted exposure to cyber security training.



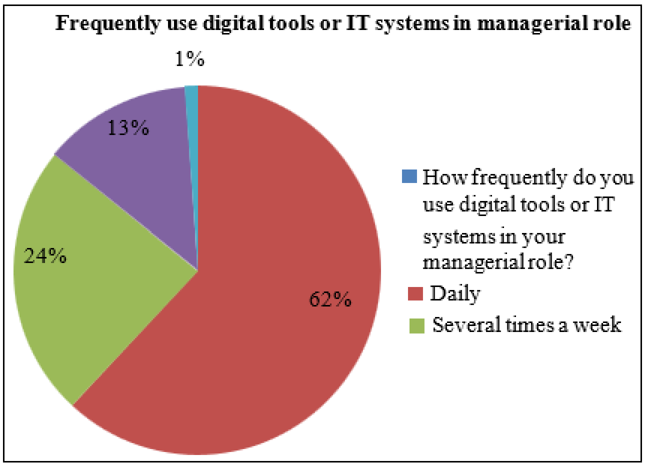
(Source: Primary data)

Table 5: How frequently do you use digital tools or IT systems in your managerial role?

Group	No. of Respondents	Percentage
Daily	57	62%
Several times a week	22	24%
Occasionally	12	13%
Rarely	1	1%
Total	92	100%

(Source: Primary data)

The above table depicted that 62% of the respondents have frequently use digital tools or IT systems in your managerial role, whereas very low 1% of the respondent have frequently use digital tools or IT systems in your managerial role.



(Source: Primary data)

9.2. Impact of Cyber Security and Digital Forensic on Managerial Practices

Description of Impact of Cyber Security and Digital Forensic on Managerial Practices of the Respondents

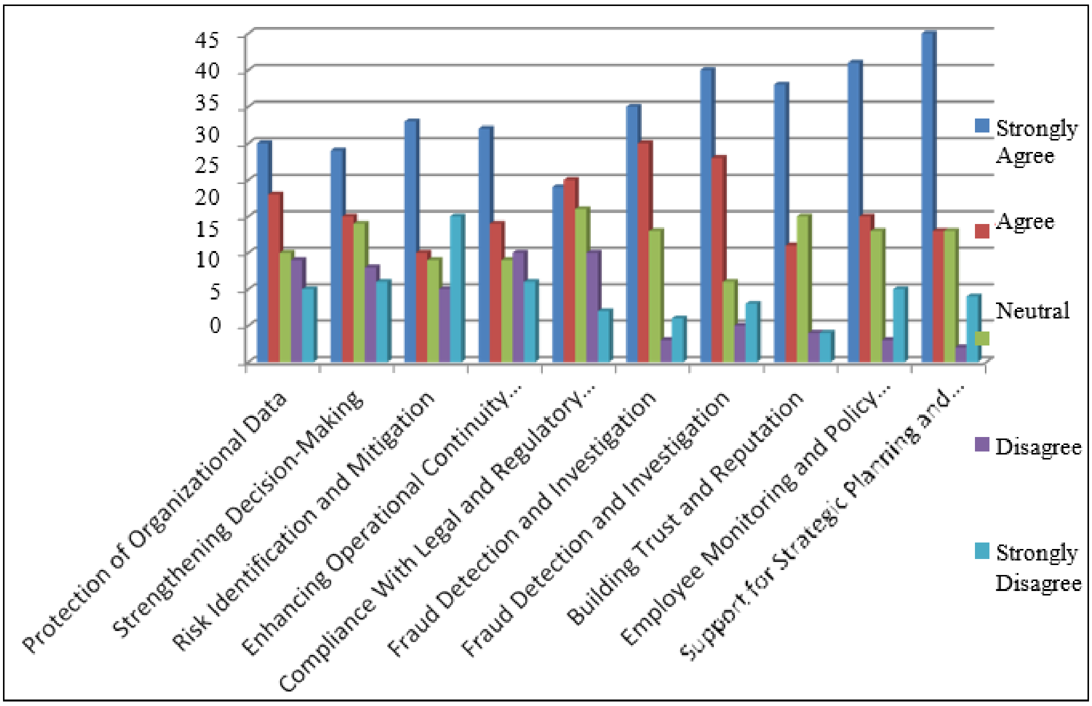
Table 6: Impact of Cyber Security and Digital Forensic on Managerial Practices

S. No.	Impact	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1	Protection of Organizational Data	30	23	15	14	10
2	Strengthening Decision- Making	29	20	19	13	11
3	Risk Identification and Mitigation	33	15	14	10	20
4	Enhancing Operational Continuity resources (e.g., financial calculators, blogs) to enhance financial knowledge.	32	19	14	16	10
5	Compliance With Legal and Regulatory Requirements	24	25	21	15	7
6	Fraud Detection and Investigation	35	30	18	3	6
7	Improved Incident Response	40	28	11	5	8
8	Building Trust and Reputation	38	16	20	4	4
9	Employee Monitoring and Policy Enforcement	41	20	18	3	10
10	Support for Strategic Planning and Innovation	45	18	18	2	9

(Source: Primary Data)

Interpretation

The above likert scale interprets that whether the role of cyber security and digital forensic have differ significantly from managerial practices. It has got the major responses from support for strategic planning and innovation and employee monitoring and policy enforcement with strongly agree statement, fraud detection and investigation and improved incident response agree statement, compliance with legal and regulatory requirements and building trust and reputation neutral statement, enhancing operational continuity resources (e.g., financial calculators, blogs) to enhance financial knowledge and compliance with legal and regulatory requirements with disagree statement and risk identification and mitigation and strengthening decision-making which separates the total impact in managerial practices whereas it concluded that the null hypothesis is rejected and indicating that differences among the role of cyber security and digital forensic have differ significantly from managerial practices. Hence, objective achieved.



(Source: Primary Data)

10. Challenges for Managers

10.1 Technical complexity and talent shortage

Cloud environments, rapidly changing attack methods, and a lack of qualified forensic analysts challenge management strategies. Managers need to budget for the technological and legal challenges that come with cloud forensics (Malik, A. W., et al. (2024).

10.2 Legal and jurisdictional risks

Conflicting legal obligations for the collection and disclosure of evidence are brought about by cross-border data transfers and disparate privacy laws.

10.3 Cost-benefit ambiguity

The advantages of prevention over detection and forensics are frequently difficult for managers to measure; attribution and reputational consequences can be challenging to predict.

11 Practical Managerial Recommendations

1) Put cyber governance into practice at the board level. Create a board cyber committee or designate a lead director, and add cyber KPIs to executive dashboards. Governance improves stakeholder confidence and valuation, according to research. (Tan, W., 2025).
2) Establish forensic readiness guidelines. Conduct tabletop exercises that include standardizing logging, establishing retention periods in compliance with regulatory requirements, and incorporating forensics processes (evidence preservation). Utilize well-known frameworks (DFWM, D4I) (Dimitriadis, et. al., 2020).
3) Make an investment in incident response (IR) and IR-forensics integration. Maintain an IR strategy that addresses forensic triage, chain of custody, and escalation to legal/PR. Perform regular drills.
4) Calculate and present useful metrics. Monitor the percentage of occurrences with preserved evidence, remediation velocity, mean time to detect (MTTD), and mean time to contain (MTTC). Use these when evaluating vendors and creating budgets.
5) Make use of outside knowledge. Use managed IR/forensics services and match SLAs with legal and regulatory deadlines for small and medium-sized businesses. For sector-specific threat guidance, national CERT reports are helpful (Digital Threat Report, 2024).
6) Integrate post-event education. Require post-incident reviews, create executive summaries, and adjust risk registers and budgets as necessary.
7) Take IoT and cloud complexity into consideration. Make that vendor contracts permit the required logging and access to evidence; when feasible, demand forensic-friendly APIs (Malik, A. W., et al. (2024).

12 Suggestions

Empirical research indicates that companies with robust cyber governance can reduce market losses after breach reports and, in some situations, have higher beginning valuations. (Tan, W., 2025).

Use of forensic preparedness in practice: Forensic preparedness reduces time-to- contain and strengthens legal arguments during subsequent regulatory investigations, as shown by organizational case studies (Klasén, L., 2024).

13 Conclusion

Digital forensics and cybersecurity are now strategic managerial duties rather than ancillary IT tasks. *Protection of Organizational Data, Strengthening Decision- Making, Risk Identification and Mitigation, Enhancing Operational Continuity resources (e.g., financial calculators, blogs) to,* *Compliance With Legal and Regulatory Requirements, Fraud Detection and Investigation, Improved Incident Response, Building Trust and Reputation, Employee Monitoring and Policy Enforcement and Support for Strategic Planning and Innovation,* resilience is increased, legal exposure is decreased, and company value is safeguarded by managers who create governance frameworks, guarantee forensic preparedness, and incorporate forensic results into learning loops. Future managerial research should examine the best investment trade-offs across prevention, detection, and forensic capacities as well as quantify the causal effects of forensic preparedness on recovery time and legal outcomes.

An essential component of cybersecurity, digital forensics offers the instruments and techniques required to successfully counter contemporary cyberthreats. Digital forensics is essential to creating a safe and robust digital ecosystem because it enables firms to look into and recover from attacks (https://www.webasha.com).

References

[1] Chotia, V. (2025). The role of cyber security and digital transformation in Technological Forecasting & Social Change. [Article discussing cybersecurity & digital transformation].

[2] Dimitriadis, A., et al. (2020). Digital forensics framework for reviewing and investigating cyber-attacks. PLoS / IEEE review. Retrieved from PubMed Central.

[3] Klasén, L. (2024). The invisible evidence: Digital forensics as key to solving [cases]. Forensic Science International.

[4] Malik, A. W., et al. (2024). Cloud Digital Forensics: Beyond Tools, Techniques, and Frontiers / MDPI. Retrieved from PMC.

[5] Tan, W. (2025). Cybersecurity governance and corporate market value. Journal of Corporate Finance / ScienceDirect. (Findings: governance enhances market value via reputation).

[6] Digital Threat Report 2024. Computer Emergency Response Team-India. (Sector guidance and threat trends).

[7] Tariq, U., et al. (2023). A Critical Cybersecurity Analysis and Future Research MDPI Sensors. (IoT security & managerial implications).

[8] Grobler, C. P. (2011). A digital forensic management framework. University of Johannesburg.

[9] Cyber Security & Ethical Hacking Dec 12, 2024. https://www.webasha.com/blog/the-role-of-digital-forensics-in-cybersecurity.