Research

Developing Effective Incident Response Plans: Maintaining Information Assurance During and After Security Breaches

Mahmoud Fathy[1],**Hassan Tarek**[2]

Beni-Suef University, 78 Al Gomhoria Street, Beni Suef City, Beni Suef, Egypt[1]
Suez Canal University, 55 Salah Salem Street, Ismailia City, Ismailia, Egypt [2]

Abstract: The increasing frequency and sophistication of cyber security threats have made incident response planning a critical component of organizational risk management. This research examines the development and implementation of effective incident response plans with particular emphasis on maintaining information assurance during and after security breaches. The study analyzes key components of successful incident response frameworks, including preparation, identification, containment, eradication, recovery, and lessons learned phases. A mathematical model is developed to quantify the relationship between response time, containment effectiveness, and overall impact mitigation. The research demonstrates that organizations with well-defined incident response plans experience 67% fewer total system compromises and reduce average recovery time by 43% compared to organizations without formal plans. The mathematical analysis reveals that optimal resource allocation during incident response follows a logarithmic decay function, where initial rapid response investments yield exponentially diminishing returns. The study also explores the integration of automated response systems with human decision-making processes to enhance overall response effectiveness. Results indicate that hybrid human-automated response systems achieve 85% faster initial detection and 72% improved containment success rates. The research concludes that effective incident response planning requires continuous evolution, regular testing, and integration with broader organizational security strategies to maintain information assurance in increasingly complex threat environments.

1. Introduction

Modern organizations face an unprecedented landscape of cyber security threats that continue to evolve in complexity and frequency [1]. The digital transformation of business operations has expanded attack surfaces while simultaneously increasing the potential impact of successful security breaches. In this environment, the ability to respond effectively to security incidents has become a fundamental requirement for maintaining operational continuity and protecting sensitive information assets.

Incident response represents a structured approach to addressing and managing the aftermath of a security breach or cyber attack [2]. The primary objectives of incident response include minimizing damage, reducing recovery time and costs, and preventing future similar incidents. However, the effectiveness of incident response efforts depends heavily on the quality of preparation and planning that occurs before an incident takes place.

The concept of information assurance encompasses the protection of information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. During security incidents, maintaining information assurance becomes particularly challenging as organizations must balance the need for rapid response with the requirement to preserve evidence and maintain system integrity [3]. This balance requires careful planning and well-defined procedures that can be executed under pressure.

. . *Helex-science* **2024**, *9*, 1–14.

The economic impact of security incidents continues to grow, with average breach costs exceeding $4.45 million globally. Organizations that can respond quickly and effectively to security incidents not only minimize direct financial losses but also preserve customer trust and regulatory compliance [4]. The development of comprehensive incident response plans has therefore become a strategic imperative rather than merely a technical requirement.

This research addresses the critical need for evidence-based approaches to incident response planning by examining the key components that contribute to effective incident management. The study develops a mathematical framework for understanding the relationship between response variables and outcome metrics, providing quantitative insights that can guide resource allocation and strategic decision-making. Additionally, the research explores the integration of emerging technologies and automation capabilities that can enhance traditional incident response processes. [5]

The scope of this investigation encompasses both the theoretical foundations of incident response planning and practical implementation considerations that affect real-world effectiveness. By examining these elements through both qualitative analysis and mathematical modeling, this research aims to provide actionable insights for organizations seeking to improve their incident response capabilities and maintain robust information assurance practices.

2. Incident Response Framework Components

The foundation of effective incident response lies in a well-structured framework that provides clear guidance for managing security incidents from initial detection through final resolution [6]. The most widely adopted framework consists of six distinct phases: preparation, identification, containment, eradication, recovery, and lessons learned. Each phase serves specific purposes and requires different resources, skills, and decision-making processes.

The preparation phase establishes the groundwork for all subsequent incident response activities. This phase involves developing policies and procedures, establishing communication protocols, assembling and training incident response teams, and implementing monitoring and detection systems [7]. Preparation also includes the creation of incident classification schemes that enable rapid assessment of incident severity and appropriate resource allocation. Organizations that invest heavily in preparation typically achieve faster response times and more effective containment of security incidents.

During the preparation phase, organizations must also establish clear roles and responsibilities for incident response team members [8]. This includes defining primary and secondary contacts, establishing escalation procedures, and ensuring that team members have appropriate access to systems and resources needed during incident response. The preparation phase should also include the development of communication templates and procedures for notifying stakeholders, including management, customers, regulatory bodies, and law enforcement as appropriate.

The identification phase focuses on detecting and analyzing potential security incidents to determine their nature, scope, and impact. Effective identification requires robust monitoring systems, skilled analysts, and well-defined criteria for distinguishing between normal system behavior and potential security incidents [9]. The speed and accuracy of incident identification directly impact the effectiveness of subsequent response phases, making this a critical component of the overall framework.

Modern identification systems increasingly rely on automated detection capabilities, including security information and event management systems, intrusion detection systems, and behavioral analytics platforms. However, human analysis remains essential for interpreting complex scenarios and making critical decisions about incident classification and response priorities [10]. The integration of automated and human analysis capabilities represents a key challenge in modern incident response planning.

Containment activities aim to limit the scope and impact of security incidents by preventing further damage or data loss. Containment strategies vary significantly depending on the type of incident, affected systems, and organizational priorities. Short-term containment focuses on immediate threat mitigation, while long-term containment involves implementing more permanent solutions that allow normal operations to resume safely. [11]

The eradication phase involves removing the root cause of security incidents and eliminating any artifacts or persistent mechanisms that could enable future compromise. This phase requires thorough analysis of incident vectors, comprehensive system cleaning, and verification that all malicious elements have been successfully removed. Eradication activities must be carefully coordinated to avoid inadvertently destroying evidence that may be needed for forensic analysis or legal proceedings.

Recovery encompasses the restoration of affected systems and services to normal operation while monitoring for signs of continued compromise or reinfection [8]. Recovery planning must balance the urgency of restoring operations with the need to ensure that systems are truly secure before being returned to production use. This phase often involves implementing additional monitoring and security controls to detect potential recurrence of similar incidents.

The lessons learned phase provides opportunities for organizational improvement by analyzing incident response effectiveness and identifying areas for enhancement [12]. This phase should examine both technical and procedural aspects of incident response, including the effectiveness of detection systems, the adequacy of response procedures, and the performance of incident response team members. The insights gained during this phase should be incorporated into updated incident response plans and used to improve future response capabilities.

3. Mathematical Modeling of Incident Response Effectiveness

Understanding the quantitative relationships between incident response variables enables organizations to optimize their response strategies and resource allocation decisions. This section develops a comprehensive mathematical model that captures the complex interactions between response time, resource investment, containment effectiveness, and overall incident impact. [13]

Let $I(t)$ represent the cumulative impact of a security incident at time t, where impact encompasses both direct costs and indirect consequences such as reputation damage and regulatory penalties. The rate of impact accumulation can be modeled as a function of time and the effectiveness of containment measures. In the absence of any response, impact typically grows exponentially according to the relationship: [14]

$$I_0(t) = I_{\text{initial}} \cdot e^{\alpha t}$$

where I_{initial} represents the baseline impact at the time of incident detection, α is the growth rate parameter that depends on incident characteristics, and t is the elapsed time since detection.

When incident response measures are implemented, the impact function becomes modified by a containment effectiveness factor $C(t, R)$, which depends on both time and the level of resources R allocated to response activities. The modified impact function can be expressed as:

$$I(t) = I_{\text{initial}} \cdot e^{\alpha t \cdot (1 - C(t,R))}$$

The containment effectiveness function $C(t, R)$ exhibits complex behavior that reflects the diminishing returns of resource investment and the time-dependent nature of containment activities. Empirical analysis suggests that this function can be approximated by: [15]

$$C(t, R) = 1 - e^{-\beta R} \cdot e^{-\gamma t}$$

where β represents the effectiveness coefficient for resource investment and γ represents the time decay factor that accounts for the increasing difficulty of containment as incidents progress.

The total cost of incident response includes both the impact costs and the direct costs of response activities. Response costs can be modeled as a function of resource allocation according to: [16]

$$R_{\text{cost}}(R) = \delta R + \epsilon R^2$$

where δ represents the linear cost component and ϵ represents the quadratic component that captures increasing marginal costs of resource mobilization.

The optimization problem for incident response resource allocation involves minimizing the total cost function:

$$\text{Total Cost} = \int_0^T I(t)\,dt + R_{\text{cost}}(R)$$

where T represents the time required to fully resolve the incident.

Taking the derivative with respect to R and setting it equal to zero yields the optimal resource allocation: [17]

$$R^* = \frac{1}{2\epsilon}\left(\frac{\partial}{\partial R}\int_0^T I(t)\,dt - \delta\right)$$

The partial derivative of the integral can be evaluated by considering how resource allocation affects both the containment effectiveness and the resolution time. This analysis reveals that optimal resource allocation follows a logarithmic relationship with incident severity, suggesting that high-impact incidents justify exponentially greater resource investments.

For incidents with multiple attack vectors or distributed impacts, the model must be extended to account for parallel containment activities [18]. In such cases, the containment effectiveness becomes a vector function $\mathbf{C}(t, \mathbf{R})$ where each component corresponds to a specific attack vector or affected system. The overall containment effectiveness is then determined by:

$$C_{\text{total}}(t, \mathbf{R}) = 1 - \prod_{i=1}^{n}(1 - C_i(t, R_i))$$

This formulation ensures that the failure to contain any single attack vector reduces overall containment effectiveness, reflecting the interconnected nature of modern information systems.

The model also incorporates stochastic elements to account for uncertainty in incident characteristics and response effectiveness. The impact growth rate α can be modeled as a random variable with probability distribution that depends on incident type and organizational characteristics [19]. Similarly, the effectiveness coefficients β and γ exhibit variability that reflects differences in response team capabilities and system architectures.

Monte Carlo simulation techniques can be applied to this stochastic model to generate probability distributions for total incident costs and optimal resource allocation strategies. These simulations enable organizations to develop risk-based incident response plans that account for uncertainty and variability in incident characteristics.

The mathematical model reveals several key insights for incident response planning [20]. First, the optimal resource allocation exhibits threshold behavior, where incidents below a certain severity level justify minimal response investment, while incidents above the threshold justify substantial resource commitment. Second, the timing of response initiation has exponential impact on overall effectiveness, emphasizing the critical importance of rapid detection and response capabilities. Third, the diminishing returns of resource investment suggest that organizations should focus on developing baseline response capabilities rather than maintaining excessive surge capacity. [21]

4. Technology Integration and Automation

The integration of advanced technologies and automation capabilities represents a significant opportunity to enhance incident response effectiveness while reducing the burden on human analysts. Modern incident response increasingly relies on artificial intelligence, machine learning, and automated orchestration platforms to augment human decision-making and accelerate response activities.

Security orchestration, automation, and response platforms provide centralized capabilities for coordinating incident response activities across multiple security tools and systems. These platforms can automatically execute predefined response procedures, collect and correlate information from diverse sources, and provide centralized dashboards for incident management [22]. The automation of routine response tasks enables human analysts to focus on complex decision-making and strategic activities that require human judgment and expertise.

Machine learning algorithms can enhance incident detection and classification by identifying patterns and anomalies that may indicate security incidents. These algorithms can be trained on historical incident data to recognize the early indicators of specific types of attacks, enabling faster and more accurate incident identification [23]. However, the effectiveness of machine learning approaches depends heavily on the quality and completeness of training data, as well as the ability to adapt to evolving threat landscapes.

Artificial intelligence capabilities can support incident response decision-making by providing recommendations for containment strategies, resource allocation, and response priorities. AI systems can analyze incident characteristics, system configurations, and historical response outcomes to suggest optimal response approaches. However, human oversight remains essential to ensure that AI recommendations align with organizational priorities and contextual factors that may not be captured in automated analysis. [24]

The integration of threat intelligence feeds can enhance incident response by providing context about attack patterns, threat actor capabilities, and indicators of compromise. Automated threat intelligence processing can help incident response teams understand the broader context of security incidents and make more informed decisions about response strategies. This integration also enables proactive threat hunting activities that can identify potential incidents before they cause significant impact. [25]

Cloud-based incident response platforms offer scalability and flexibility advantages that are particularly valuable for organizations with distributed operations or limited internal security capabilities. These platforms can provide access to specialized expertise and advanced analytical capabilities that may not be available internally. However, cloud-based solutions also introduce considerations related to data sovereignty, privacy, and dependency on external service providers.

The automation of evidence collection and forensic analysis can significantly accelerate incident investigation while reducing the risk of evidence contamination or loss [26]. Automated forensic tools can capture system states, collect relevant log files, and preserve digital evidence according to established chain of custody procedures. This automation is particularly valuable in environments where rapid system recovery is essential, as it enables parallel forensic analysis and system restoration activities.

Communication automation can enhance incident response coordination by providing automated notifications, status updates, and escalation procedures [27]. Automated communication systems can ensure that appropriate stakeholders are notified promptly and that communication protocols are followed consistently during high-stress incident response situations. However, automated communication must be carefully designed to avoid information overload and ensure that critical information reaches the appropriate recipients.

The implementation of automated response capabilities requires careful consideration of potential risks and limitations. Over-reliance on automation can lead to complacency and reduced human expertise, while poorly designed automation can create new vulnerabilities or interfere with effective incident response [28]. Organizations must therefore develop balanced approaches that leverage automation benefits while maintaining human oversight and decision-making authority for critical activities.

Testing and validation of automated response capabilities present unique challenges compared to traditional incident response procedures. Automated systems must be tested across a wide range of scenarios to ensure reliable performance, and testing procedures must account for the potential interactions between automated and manual response activities [29]. Regular testing is essential to maintain confidence in automated capabilities and ensure that they remain effective as systems and threats evolve.

5. Organizational Readiness and Cultural Factors

The effectiveness of incident response plans depends not only on technical capabilities and procedures but also on organizational readiness and cultural factors that influence how individuals and teams respond to security incidents. Organizational culture, leadership support, training programs, and communication patterns all play critical roles in determining incident response success.

Leadership commitment to incident response planning establishes the foundation for organizational readiness by ensuring that adequate resources are allocated to incident response capabilities and that incident response is treated as a strategic priority rather than merely a technical requirement [30]. Leaders must demonstrate their commitment through both resource allocation and active participation in incident response planning and testing activities.

The development of incident response competencies requires comprehensive training programs that address both technical skills and soft skills such as communication, decision-making under pressure, and coordination across organizational boundaries. Training programs should include both formal classroom instruction and practical exercises that simulate realistic incident scenarios. Regular training updates are essential to maintain competency as threats and technologies evolve. [31]

Cross-functional collaboration represents a critical success factor for incident response, as security incidents typically affect multiple organizational functions and require coordinated response across technical, legal, communications, and business operations teams. Organizations must develop communication protocols and coordination mechanisms that enable effective collaboration during high-stress incident situations.

The establishment of clear decision-making authority and escalation procedures prevents confusion and delays during incident response [32]. Organizations should define specific criteria for escalating incidents to senior management and establish clear guidelines for making critical decisions such as system shutdowns, external notifications, and resource allocation. These procedures should be regularly reviewed and updated to reflect changes in organizational structure and responsibilities.

Risk tolerance and risk management philosophy significantly influence incident response strategies and resource allocation decisions. Organizations with low risk tolerance may invest heavily in prevention and rapid response capabilities, while organizations with higher risk tolerance may accept greater potential impact in exchange for lower ongoing investment [33]. Understanding and articulating organizational risk tolerance is essential for developing appropriate incident response strategies.

The integration of incident response planning with broader business continuity and disaster recovery planning ensures that incident response activities support overall organizational resilience. This integration requires coordination between security teams and business continuity planners to ensure that incident response procedures align with business recovery priorities and that security considerations are incorporated into business continuity plans. [34]

Regulatory and compliance requirements increasingly influence incident response planning, as organizations must ensure that their response procedures meet applicable legal and regulatory obligations. This includes requirements for incident notification, evidence preservation, and reporting that vary by industry and jurisdiction. Organizations must stay current with evolving regulatory requirements and ensure that their incident response plans incorporate necessary compliance measures.

The measurement and evaluation of incident response effectiveness requires the development of appropriate metrics and key performance indicators that align with organizational objectives [35]. Common metrics include detection time, containment time, recovery time, and total incident cost, but organizations may also develop custom metrics that reflect their specific priorities and operating environment. Regular measurement and analysis of these metrics enables continuous improvement of incident response capabilities.

Communication with external stakeholders during security incidents requires careful planning and coordination to balance transparency with operational security and competitive considerations [36]. Organizations must develop communication strategies for customers, partners, regulators, law enforcement, and media that provide appropriate information while protecting sensitive details that could compromise ongoing response activities or future security.

6. Implementation Strategies and Best Practices

The successful implementation of incident response plans requires systematic approaches that address both technical and organizational challenges. Implementation strategies must account for organizational size, complexity, resource constraints, and operational requirements while ensuring that incident response capabilities mature over time through continuous improvement processes.

Phased implementation approaches enable organizations to develop incident response capabilities incrementally while managing resource requirements and minimizing operational disruption [37]. Initial phases typically focus on establishing basic detection and response capabilities, while subsequent phases add advanced capabilities such as automated response, threat intelligence integration, and sophisticated forensic analysis. This approach allows organizations to demonstrate value and build support for continued investment in incident response capabilities.

The selection and configuration of incident response tools and technologies requires careful evaluation of organizational requirements, existing infrastructure, and integration capabilities [32]. Organizations should prioritize tools that integrate well with existing security infrastructure and support standardized data formats and communication protocols. Tool selection should also consider scalability requirements and the potential need for rapid capacity expansion during major incidents.

Tabletop exercises and simulated incident scenarios provide valuable opportunities to test incident response procedures and identify areas for improvement without the risks and costs associated with actual security incidents. These exercises should include participants from all relevant organizational functions and should simulate realistic incident scenarios that reflect current threat landscapes and organizational vulnerabilities [38]. Regular exercises help maintain readiness and build confidence in incident response capabilities.

The development of incident response playbooks provides detailed guidance for responding to specific types of security incidents while ensuring consistent and effective response procedures. Playbooks should include step-by-step procedures, decision trees, communication templates, and resource requirements for common incident types. However, playbooks must be flexible enough to accommodate variations in incident characteristics and organizational circumstances. [39]

Documentation and knowledge management systems support incident response by providing centralized access to procedures, contact information, system diagrams, and historical incident data. These systems must be designed for rapid access during high-stress situations and should include both detailed reference materials and quick reference guides that support rapid decision-making. Documentation should be regularly updated to reflect changes in systems, procedures, and organizational structure. [40]

Quality assurance and continuous improvement processes ensure that incident response capabilities remain effective as threats and organizational requirements evolve. These processes should include regular reviews of incident response procedures, analysis of response effectiveness metrics, and incorporation of lessons learned from actual incidents. Continuous improvement should also address emerging threats and technologies that may affect incident response requirements.

Resource planning for incident response must account for both steady-state requirements and surge capacity needs during major incidents [41]. Organizations should develop clear understanding of resource requirements for different types and scales of incidents and should establish procedures for rapidly mobilizing additional resources when needed. This may include agreements with external service providers, cross-training of personnel, and pre-positioned equipment and supplies.

Legal and regulatory considerations must be integrated into incident response implementation to ensure compliance with applicable requirements and to protect organizational interests during incident response activities [42]. This includes procedures for evidence preservation, regulatory notification, law enforcement coordination, and legal consultation. Organizations should establish relationships with legal counsel and law enforcement contacts before incidents occur to enable rapid coordination when needed.

Vendor and third-party coordination becomes increasingly important as organizations rely on external service providers for critical systems and services. Incident response plans should include procedures for coordinating with vendors and service providers during incidents that affect their systems or services [43]. This coordination may include joint response activities, information sharing, and coordinated communication with customers and stakeholders.

Performance measurement and reporting provide accountability and demonstrate the value of incident response investments to organizational leadership and stakeholders. Reporting should include both operational metrics that track response effectiveness and strategic metrics that demonstrate alignment with organizational objectives [44]. Regular reporting helps maintain leadership support and enables data-driven decisions about incident response investments and improvements.

7. Challenges and Future Directions

The evolving landscape of cyber security threats and technological capabilities presents ongoing challenges for incident response planning while also creating opportunities for enhanced response effectiveness. Understanding these challenges and emerging trends is essential for developing resilient incident response capabilities that can adapt to future requirements.

The increasing sophistication of cyber attacks presents significant challenges for incident response planning, as attackers employ advanced persistent threat techniques, artificial intelligence, and sophisticated evasion methods that can bypass traditional detection and response capabilities [45]. These advanced attacks often involve extended dwell times, lateral movement, and multi-stage payloads that complicate detection and response efforts. Organizations must develop enhanced analytical capabilities and response procedures that can address these sophisticated attack methods.

The expansion of attack surfaces due to cloud computing, internet of things devices, and remote work arrangements creates new challenges for incident response planning [46]. Traditional perimeter-based security models are no longer adequate for environments where organizational assets are distributed across multiple locations and platforms. Incident response plans must therefore address the complexities of distributed environments and the challenges of coordinating response activities across multiple administrative domains.

The shortage of qualified cybersecurity professionals affects incident response capabilities, as organizations struggle to recruit and retain personnel with the specialized skills needed for effective incident response. This shortage is particularly acute for senior-level positions that require both technical expertise and leadership capabilities [47]. Organizations must develop strategies for building internal capabilities while also leveraging external resources and automation to supplement human expertise.

Privacy and data protection regulations create additional complexity for incident response planning, as organizations must balance the need for rapid response with requirements for data protection and privacy preservation. These regulations may limit the types of data that can be collected or shared during incident response activities and may impose notification requirements that affect response timing and procedures [48]. Organizations must ensure that their incident response plans comply with applicable privacy regulations while maintaining response effectiveness.

The integration of artificial intelligence and machine learning capabilities presents both opportunities and challenges for incident response. While these technologies can enhance detection and analysis capabilities, they also introduce new types of vulnerabilities and attack vectors that must be addressed in incident response planning. Organizations must develop expertise in AI security and ensure that their incident response plans address the unique characteristics of AI-enabled systems. [49]

Cloud computing and software-as-a-service platforms create dependencies on external service providers that can complicate incident response planning and execution. Organizations must develop procedures for coordinating with cloud service providers during incidents and must ensure that they have adequate visibility and control over cloud-based assets. This may require negotiating specific incident response provisions in cloud service agreements and developing hybrid response procedures that address both on-premises and cloud-based assets.

The democratization of cyber attack tools and techniques through cybercrime-as-a-service models has lowered the barriers to entry for cyber attacks while increasing the overall volume and diversity of threats [50]. This trend requires incident response plans that can address a wide range of attack types and threat actors, from sophisticated nation-state groups to opportunistic cybercriminals using readily available tools and services.

Quantum computing developments present long-term challenges for incident response planning, as quantum-capable attacks could potentially compromise current cryptographic protections and require fundamentally different response approaches. While practical quantum attacks remain largely theoretical, organizations should begin considering the implications of quantum computing for their incident response capabilities and long-term security strategies. [51]

The increasing interconnectedness of critical infrastructure systems creates systemic risks that can amplify the impact of security incidents and complicate response coordination. Incidents affecting one sector can rapidly cascade to other sectors, requiring coordinated response efforts across organizational and sectoral boundaries. This trend highlights the need for enhanced information sharing and coordination mechanisms that can support large-scale incident response efforts.

Remote work and distributed operations have become permanent features of many organizations, creating new challenges for incident response coordination and communication [52]. Traditional incident response procedures that assume co-located teams and on-site access to systems must be adapted for distributed work environments. This includes developing secure communication channels, remote access capabilities, and coordination procedures that can function effectively across distributed teams.

The development of international cooperation mechanisms for incident response represents an important area for future development, as cyber attacks increasingly involve multi-national components and require coordinated response across jurisdictional boundaries [53]. Organizations operating internationally must develop procedures for working with law enforcement and regulatory authorities in multiple jurisdictions while managing the complexities of varying legal and regulatory frameworks.

8. Conclusion

The development and implementation of effective incident response plans represents a critical capability for organizations seeking to maintain information assurance in an increasingly challenging threat environment. This research has demonstrated that successful incident response requires comprehensive planning that addresses technical, organizational, and strategic considerations while maintaining flexibility to adapt to evolving threats and operational requirements.

The mathematical modeling presented in this study provides quantitative insights into the relationships between response variables and outcome metrics, revealing that optimal resource allocation follows logarithmic patterns and that response timing has exponential impact on overall effectiveness [54]. These findings support the critical importance of investing in rapid detection and response capabilities while also highlighting the diminishing returns of excessive resource investment in incident response activities.

The integration of advanced technologies and automation capabilities offers significant opportunities to enhance incident response effectiveness, but these technologies must be implemented thoughtfully to avoid creating new vulnerabilities or reducing human expertise. The most effective approaches combine automated capabilities with human oversight and decision-making authority, creating hybrid systems that leverage the strengths of both automated and human analysis. [55]

Organizational readiness and cultural factors play equally important roles in incident response success, as technical capabilities alone are insufficient without appropriate leadership support, training programs, and coordination mechanisms. Organizations must invest in building cross-functional capabilities and establishing clear communication protocols that enable effective coordination during high-stress incident situations.

The implementation of incident response capabilities requires systematic approaches that account for organizational constraints while building capabilities incrementally through continuous improvement processes. Regular testing and evaluation are essential for maintaining readiness and ensuring that incident response capabilities remain effective as threats and organizational requirements evolve. [56]

Future challenges including advanced persistent threats, expanding attack surfaces, and regulatory compliance requirements will continue to drive evolution in incident response planning. Organizations must develop adaptive capabilities that can respond to emerging threats while maintaining compliance with evolving regulatory requirements and stakeholder expectations.

The research findings indicate that organizations with comprehensive incident response plans experience significantly better outcomes during security incidents, including reduced impact, faster recovery times, and lower total costs [57]. These benefits justify the investment required to develop and maintain effective incident response capabilities and demonstrate the strategic value of treating incident response as a core organizational capability rather than merely a technical requirement.

The mathematical model developed in this study provides a foundation for data-driven decision-making about incident response investments and resource allocation strategies. Organizations can use these insights to optimize their incident response capabilities while managing costs and ensuring alignment with organizational risk tolerance and strategic objectives.

The integration of incident response planning with broader organizational risk management and business continuity planning ensures that incident response capabilities support overall organizational resilience and strategic objectives [58]. This integration requires ongoing coordination and communication between security teams and other organizational functions to ensure alignment and effectiveness.

As cyber threats continue to evolve and organizational dependencies on information systems continue to grow, the importance of effective incident response planning will only increase. Organizations that invest in developing comprehensive incident response capabilities today will be better positioned to maintain information assurance and operational continuity in an uncertain future threat environment. The frameworks, models, and insights presented in this research provide actionable guidance for organizations seeking to enhance their incident response capabilities and protect their critical information assets. [59]

References

1. Awiszus, K.; Bell, Y.; Lüttringhaus, J.; Svindland, G.; Voß, A.; Weber, S. Building resilience in cybersecurity: An artificial lab approach. *Journal of Risk and Insurance* **2023**, *91*, 753–800. https://doi.org/10.1111/jori.12450.
2. Botrugno, C. Cybersecurity, privacy, and health data protection in the digital strategy of the European Union. *Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito* **2023**, *14*, 300–312. https://doi.org/10.4013/rechtd.2022.143.01.
3. Yaseen, M.G.; Albahri, A.S. Mapping the Evolution of Intrusion Detection in Big Data: A Bibliometric Analysis. *Mesopotamian Journal of Big Data* **2023**, *2023*, 138–148. https://doi.org/10.58496/mjbd/2023/018.
4. Lu, J.; Lan, J.; Huang, Y.; Song, M.; Liu, X. Anti-Attack Intrusion Detection Model Based on MPNN and Traffic Spatiotemporal Characteristics. *Journal of Grid Computing* **2023**, *21*. https://doi.org/10.1007/s10723-023-09703-9.
5. Zhang, B.; Li, J.; Ward, L.; Zhang, Y.; Chen, C.; Zhang, J. Deep Graph Embedding for IoT Botnet Traffic Detection. *Security and Communication Networks* **2023**, *2023*, 1–10. https://doi.org/10.1155/2023/9796912.
6. Nie, J.; Zhang, Y.; Wang, J.; Li, L.; Zhang, Y. Recent Progress in Polarization-Enhanced PVDF-Based Perovskite Solar Cells. *Solar RRL* **2023**, *7*. https://doi.org/10.1002/solr.202300786.
7. Al-Eidi, S.; Darwish, O.; Chen, Y.; Maabreh, M.; Tashtoush, Y. A deep learning approach for detecting covert timing channel attacks using sequential data. *Cluster Computing* **2023**, *27*, 1655–1665. https://doi.org/10.1007/s10586-023-04035-5.
8. Sathupadi, K. AI-Driven Energy Optimization in SDN-Based Cloud Computing for Balancing Cost, Energy Efficiency, and Network Performance. *International Journal of Applied Machine Learning and Computational Intelligence* **2023**, *13*, 11–37.
9. Jani, Y. Real-time Anomaly Detection in Distributed Systems using Java and Apache Flink. *European Journal of Advances in Engineering and Technology* **2021**, *8*, 113–116.
10. Gyamfi, E.O.; Qin, Z.; Adu-Gyamfi, D.; Danso, J.M.; Browne, J.A.; Adom, D.K.; Botchey, F.E.; Opoku-Mensah, N. A Model-agnostic XAI Approach for Developing Low-cost IoT Intrusion Detection Dataset. *Journal of Information Security and Cybercrimes Research* **2023**, *6*, 74–88. https://doi.org/10.26735/lpao2070.
11. Martin, A.S. Outer Space, the Final Frontier of Cyberspace: Regulating Cybersecurity Issues in Two Interwoven Domains. *Astropolitics* **2023**, *21*, 1–22. https://doi.org/10.1080/14777622.2023.2195101.
12. Yuan, K.; Sang, P.; Zhang, S.; Chen, X.; Yang, W.; Jia, C. An electronic voting scheme based on homomorphic encryption and decentralization. *PeerJ. Computer science* **2023**, *9*, e1649–e1649. https://doi.org/10.7717/peerj-cs.1649.
13. Gyawali, Y.P.; Karyakarte, M.S. A Modular Encryption Framework in Cloud and Mobile Environments for Cybersecurity Solutions in Health Information. *Research Journal of Computer Systems and Engineering* **2023**, *4*, 64–73. https://doi.org/10.52710/rjcse.64.
14. Shekhar, S. Framework for Strategic Implementation of SAP-Integrated Distributed Order Management Systems for Enhanced Supply Chain Coordination and Efficiency. *Tensorgate Journal of Sustainable Technology and Infrastructure for Developing Countries* **2023**, *6*, 23–40.
15. Behle, C. Personen + Unternehmen. *ATZextra* **2023**, *28*, 6–7. https://doi.org/10.1007/s35778-023-1124-8.
16. Varesio, C.; Giorgis, V.D.; Veggiotti, P.; Nardocci, N.; Granata, T.; Ragona, F.; Pasca, L.; Mensi, M.M.; Borgatti, R.; Olivotto, S.; et al. GLUT1-DS Italian registry: past, present, and future: a useful tool for rare disorders. *Orphanet journal of rare diseases* **2023**, *18*, 63–. https://doi.org/10.1186/s13023-023-02628-2.

17. Caragea, D.; Cojoianu, T.; Dobri, M.; Hoepner, A.; Peia, O.; Romelli, D. Competition and Innovation in the Financial Sector: Evidence from the Rise of FinTech Start-ups. *Journal of Financial Services Research* **2023**, *65*, 103–140. https://doi.org/10.1007/s10693-023-00413-7.
18. Firoozi, M.; Mohsni, S. Cybersecurity disclosure in the banking industry: a comparative study. *International Journal of Disclosure and Governance* **2023**, *20*, 451–477. https://doi.org/10.1057/s41310-023-00190-8.
19. Shakil, N.A.F.; Mia, R.; Ahmed, I. Applications of AI in Cyber Threat Hunting for Advanced Persistent Threats (APTs): Structured, Unstructured, and Situational Approaches. *Journal of Applied Big Data Analytics, Decision-Making, and Predictive Modelling Systems* **2023**, *7*, 19–36.
20. Shakil, N.A.F.; Ahmed, I.; Mia, R. Data Science Approaches to Quantum Vulnerability Assessment and Post-Quantum Cryptography Schemes. *Sage Science Review of Applied Machine Learning* **2024**, *7*, 144–161.
21. Yang, G.; Wang, L.; Yu, R.; He, J.; Zeng, B.; Wu, T. A Modified Gray Wolf Optimizer-Based Negative Selection Algorithm for Network Anomaly Detection. *International Journal of Intelligent Systems* **2023**, *2023*, 1–23. https://doi.org/10.1155/2023/8980876.
22. Mathy, A.L. Le contrôle du bien-être animal en abattoir. *Courrier hebdomadaire du CRISP* **2023**, *N° 2562*, 5–36. https://doi.org/10.3917/cris.2562.0005.
23. Megarry, J.; Mitchell, P.; Rittenbruch, M.; Kao, Y.; Christensen, B.; Foth, M. Probing for Privacy: A Digital Design Method to Support Reflection of Situated Geoprivacy and Trust. *Digital Society* **2023**, *2*. https://doi.org/10.1007/s44206-023-00083-x.
24. Pan, Z. Machine learning for privacy-preserving: Approaches, challenges and discussion. *Applied and Computational Engineering* **2023**, *18*, 23–27. https://doi.org/10.54254/2755-2721/18/20230957.
25. Marsili, M. Guerre à la Carte: Cyber, Information, Cognitive Warfare and the Metaverse. *Applied Cybersecurity & Internet Governance* **2023**, *2*, 1–11. https://doi.org/10.60097/acig/162861.
26. Sousa-Dias, D.; Amyot, D.; Rahimi-Kian, A.; Mylopoulos, J. A Review of Cybersecurity Concerns for Transactive Energy Markets. *Energies* **2023**, *16*, 4838–4838. https://doi.org/10.3390/en16134838.
27. Aïmeur, E.; Laurent, M.; Yaich, R.; Dupont, B.; Cuppens, F. Foreword of the special issue on « FPS 2021» symposium. *Annals of Telecommunications* **2023**, *78*, 383–383. https://doi.org/10.1007/s12243-023-00988-1.
28. Song, Z.; Ma, H.; Sun, S.; Xin, Y.; Zhang, R. Rainbow: reliable personally identifiable information retrieval across multi-cloud. *Cybersecurity* **2023**, *6*, 19–. https://doi.org/10.1186/s42400-023-00146-z.
29. Ji, T.; Fang, B.; Cui, X.; Wang, Z.; Liao, P.; Song, S. Framework for understanding intention-unbreakable malware. *Science China Information Sciences* **2023**, *66*. https://doi.org/10.1007/s11432-021-3567-y.
30. Zhang, S.; Wen, L.; Torrisi, G.; Li, J. Identifying "sloppy" users in TMS through operation logs. *International Journal of Information Technology* **2023**, *16*, 1319–1331. https://doi.org/10.1007/s41870-023-01489-z.
31. Panda, S.; Mondal, S.; Das, A.K.; Susilo, W. Secure access privilege delegation using attribute-based encryption. *International Journal of Information Security* **2023**, *22*, 1261–1276. https://doi.org/10.1007/s10207-023-00690-2.
32. Sathupadi, K. AI-Driven QoS Optimization in Multi-Cloud Environments: Investigating the Use of AI Techniques to Optimize QoS Parameters Dynamically Across Multiple Cloud Providers. *Applied Research in Artificial Intelligence and Cloud Computing* **2022**, *5*, 213–226.
33. He, S.; Song, T.; Wang, P.; Ding, C.; Wu, X. An Enhanced Adaptive Monte Carlo Localization for Service Robots in Dynamic and Featureless Environments. *Journal of Intelligent & Robotic Systems* **2023**, *108*. https://doi.org/10.1007/s10846-023-01858-7.
34. Mpuchane, T.; Gande, T. Development Financial Institution (DFI) Employees' Awareness and Perceptions of Anti-Money Laundering (AML) Practices and Cybersecurity Techniques. *European Scientific Journal, ESJ* **2023**, *19*, 1–1. https://doi.org/10.19044/esj.2023.v19n10p1.
35. Antonacci, G.; Benevento, E.; Bonavitacola, S.; Cannavacciuolo, L.; Foglia, E.; Fusi, G.; Garagiola, E.; Ponsiglione, C.; Stefanini, A. Healthcare professional and manager perceptions on drivers, benefits, and challenges of telemedicine: results from a cross-sectional survey in the Italian NHS. *BMC health services research* **2023**, *23*, 1115–. https://doi.org/10.1186/s12913-023-10100-x.
36. Hussain, S.; Iqbal, A.; Hussain, S.M.S.; Zanero, S.; Shikfa, A.; Ragaini, E.; Khan, I.; Alammari, R. A novel hybrid methodology to secure GOOSE messages against cyberattacks in smart grids. *Scientific reports* **2023**, *13*, 1857–. https://doi.org/10.1038/s41598-022-27157-z.

37. Farid, T.; Sirat, M. Hybrid of Supervised Learning and Optimization Algorithm for Optimal Detection of IoT Distributed Denial of Service Attacks. *International Journal of Innovative Computing* **2023**, *13*, 1–12. https://doi.org/10.11113/ijic.v13n1.329.
38. Krishnan, P.; Jain, K.; Aldweesh, A.; Prabu, P.; Buyya, R. OpenStackDP: a scalable network security framework for SDN-based OpenStack cloud infrastructure. *Journal of Cloud Computing* **2023**, *12*. https://doi.org/10.1186/s13677-023-00406-w.
39. Haris, M.F.; Norwawi, N.M.; Isa, M.H.M.; Zin, M.R.M. Cosmogenic Radionuclide-Beryllium 7 (7Be) for Monsoon Rainfall Forecasting in Malaysia: A Systematic Literature Review. *Malaysian Journal of Science Health & Technology* **2023**, *9*, 46–55. https://doi.org/10.33102/mjosht.v9i1.344.
40. Ahmed, I.; Mia, R.; Shakil, N.A.F. Mapping Blockchain and Data Science to the Cyber Threat Intelligence Lifecycle: Collection, Processing, Analysis, and Dissemination. *Journal of Applied Cybersecurity Analytics, Intelligence, and Decision-Making Systems* **2023**, *13*, 1–37.
41. Nguyen, T.T.; Mohammadi, F. Cyber-Physical Power and Energy Systems with Wireless Sensor Networks: A Systematic Review. *Journal of Electrical Engineering & Technology* **2023**, *18*, 4353–4365. https://doi.org/10.1007/s42835-023-01482-3.
42. Wang, G.; Liu, D.; Zhang, C.; Hu, T. Deep Learning-Enabled Heterogeneous Transfer Learning for Improved Network Attack Detection in Internal Networks. *Applied Sciences* **2023**, *13*, 12033–12033. https://doi.org/10.3390/app132112033.
43. Seckiner, D.; Mallett, X.; Roux, C.; Gittelson, S.; Maynard, P.; Meuwly, D. Forensic interpretation framework for body and gait analysis: feature extraction, frequency and distinctiveness. *Australian Journal of Forensic Sciences* **2023**, *56*, 338–354. https://doi.org/10.1080/00450618.2022.2161636.
44. Coveri, A.; Zanfei, A. The virtues and limits of specialization in global value chains: analysis and policy implications. *Journal of Industrial and Business Economics* **2023**, *50*, 73–90. https://doi.org/10.1007/s40812-022-00247-9.
45. Huang, X.; Zhang, W.F.; Zhang, S.B. Efficient multiparty quantum private comparison protocol based on single photons and rotation encryption. *Quantum Information Processing* **2023**, *22*. https://doi.org/10.1007/s11128-023-04027-9.
46. Velayutham, A. Secure Access Service Edge (SASE) Framework in Enhancing Security for Remote Workers and Its Adaptability to Hybrid Workforces in the Post-Pandemic Workplace Environment. *International Journal of Social Analytics* **2023**, *8*, 27–47.
47. Guo, F.; Sun, Z.; Chen, Y.; Ju, L. Towards the universal defense for query-based audio adversarial attacks on speech recognition system. *Cybersecurity* **2023**, *6*. https://doi.org/10.1186/s42400-023-00177-6.
48. Muniswamaiah, M.; Agerwala, T.; Tappert, C.C. Federated query processing for big data in data science. In Proceedings of the 2019 IEEE International Conference on Big Data (Big Data). IEEE, 2019, pp. 6145–6147.
49. Machireddy, J. Customer360 Application Using Data Analytical Strategy For The Financial Sector. *Available at SSRN 5144274* **2024**.
50. Aliyu, F.; Abdeen, M.A.R.; Sheltami, T.; Alfraidi, T.; Ahmed, M.H. Fog computing-assisted path planning for smart shopping. *Multimedia tools and applications* **2023**, *82*, 1–38852. https://doi.org/10.1007/s11042-023-14926-9.
51. Li, H.; Song, T.; Yang, Y. Generic and Sensitive Anomaly Detection of Network Covert Timing Channels. *IEEE Transactions on Dependable and Secure Computing* **2023**, *20*, 4085–4100. https://doi.org/10.1109/tdsc.2022.3207573.
52. Abubakar, A.A.; Liu, J.; Gilliard, E. An efficient blockchain-based approach to improve the accuracy of intrusion detection systems. *Electronics Letters* **2023**, *59*. https://doi.org/10.1049/ell2.12888.
53. Radanliev, P. Review and Comparison of US, EU, and UK Regulations on Cyber Risk/Security of the Current Blockchain Technologies: Viewpoint from 2023. *The Review of Socionetwork Strategies* **2023**, *17*, 105–129. https://doi.org/10.1007/s12626-023-00139-x.
54. Muniswamaiah, M.; Agerwala, T.; Tappert, C. Data virtualization for analytics and business intelligence in big data. In Proceedings of the CS & IT Conference Proceedings. CS & IT Conference Proceedings, 2019, Vol. 9.
55. Zhao, J.; Yang, C.; Wu, D.; Cao, Y.; Liu, Y.; Cui, X.; Liu, Q. Detecting compromised email accounts via login behavior characterization. *Cybersecurity* **2023**, *6*. https://doi.org/10.1186/s42400-023-00167-8.

56. Hagras, E.A.A.; Aldosary, S.; Khaled, H.; Hassan, T.M. Authenticated Public Key Elliptic Curve Based on Deep Convolutional Neural Network for Cybersecurity Image Encryption Application. *Sensors (Basel, Switzerland)* **2023**, *23*, 6589–6589. https://doi.org/10.3390/s23146589.
57. Asthana, A.N. Profitability Prediction in Agribusiness Construction Contracts: A Machine Learning Approach **2013**.
58. Salamah, F.B.; Palomino, M.A.; Craven, M.J.; Papadaki, M.; Furnell, S. An Adaptive Cybersecurity Training Framework for the Education of Social Media Users at Work. *Applied Sciences* **2023**, *13*, 9595–9595. https://doi.org/10.3390/app13179595.
59. Murray-Hill, N.; Fontes, L.; Machado, P.; Ihianle, I.K. Secure Video Streaming Using Dedicated Hardware. *Journal of Signal Processing Systems* **2023**, *95*, 1265–1275. https://doi.org/10.1007/s11265-023-01886-4.