International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 7.101

# Assessment of Organizational Incident Response Readiness

**Mohammed Ali Obayes Muthek**

Department of English-Faculty of Education - University of Hilla - Babylon – Iraq

**Abstract:** ***In the digital era, organizations face increasing challenges in protecting their information systems from evolving cyber threats, necessitating the development of effective strategies to enhance cybersecurity readiness. This study aims to analyse the level of organizational preparedness against cyber risks using a multi-theoretical framework based on Institutional Theory, Game Theory, and Deterrence Theory. A descriptive-analytical approach was employed, collecting data through surveys and interviews with cybersecurity experts across several organizations. The data were analysed using descriptive and inferential statistical methods to assess the factors influencing cybersecurity readiness. Results indicated a significant impact of institutional and organizational factors in strengthening cybersecurity practices. The study highlights the importance of deterrence strategies based on rapid response and game-theoretic planning to achieve effective protection. Additionally, findings show that investing in security culture and employee training reduces cyberattack risks and enhances response capabilities. In conclusion, the study emphasizes the necessity of adopting an integrated approach that combines theoretical frameworks with practical applications to improve organizational cybersecurity readiness, focusing on raising institutional awareness and implementing effective deterrence strategies. The study recommends further future research to develop dynamic evaluation models that adapt to the changing landscape of digital threats.***

**Keywords:** Cybersecurity readiness, Institutional Theory, Game Theory, Deterrence Theory, Security culture

## 1. Introduction

In recent years, cyber threats have escalated not only in frequency but also in complexity and impact, making cybersecurity a paramount concern for organizations worldwide. According to industry forecasts, the global cost of cybercrime is expected to exceed USD 10.5 trillion annually by 2025 (Morgan, 2021), underlining the scale of economic and operational risks organizations face. Nearly two-thirds of companies report experiencing cyber incidents each year (Barreuther et al., 2022), and even those with considerable investments in IT security infrastructure remain vulnerable to attacks (Hiscox, 2021). This landscape illustrates a critical insight: technical defenses alone are not sufficient to ensure resilience. Instead, organizations must possess comprehensive incident response management (IRM) capabilities to effectively detect, contain, mitigate, and learn from security incidents.

Despite the recognized importance of IRM, many organizations continue to struggle with the implementation of effective incident response processes. Numerous challenges hinder their progress, including limited resources, inadequate awareness of IRM's strategic value, lack of skilled personnel, and fragmented organizational structures (Kuypers et al., 2016; van der Kleij et al., 2022). Furthermore, incident response is often treated as a purely technical function, neglecting the crucial socio-organizational components such as communication, coordination, and leadership. This narrow view limits the effectiveness and maturity of IR programs, particularly in small and medium-sized enterprises (SMEs) where formal structures and dedicated teams may be lacking (ENISA, 2019; Andrade et al., 2021). Another critical issue lies in the tools and models available to support IRM readiness. While several frameworks and maturity models such as SIM3 (Stikvoort, 2019) and CREST's CSIRMA (2014) have been developed to guide organizations in assessing and improving their IRM capabilities, these are often limited in scope, overly technical, or lacking empirical validation. Moreover, many models are not designed to accommodate organizations at early maturity levels, and do not sufficiently consider the socio-technical nature of cybersecurity functions (Akinsanya et al., 2020; Zhao & White, 2017). Consequently, there exists a gap between academic research and industry practice, whereby theoretical models do not adequately translate into usable guidance for real-world implementation. This study is motivated by the need to address this gap. The increasing risk and complexity of cyber incidents call for a more nuanced, integrated approach to evaluating and enhancing incident response readiness. A deeper understanding is required not only of what technical capabilities are necessary, but also of how organizational culture, leadership, communication, and collaboration affect IRM effectiveness. This is particularly crucial for organizations that lack formal cybersecurity governance or are not bound by regulatory requirements, yet are still exposed to significant threats. Accordingly, the main objective of this research is to assess organizational incident response readiness by critically examining existing maturity models and identifying key enablers and barriers to effective IRM implementation. The study aims to provide a holistic framework for evaluating readiness that incorporates both technical and non-technical dimensions, and that is scalable and adaptable to varying organizational sizes and contexts. The assessment will consider preparedness, detection capabilities, response coordination, post-incident learning, and continuous improvement, while also integrating organizational aspects such as training, leadership engagement, and cross-functional collaboration.

Finally, this research seeks to make a dual contribution. Theoretically, it aims to advance the understanding of IRM as a socio-technical capability, moving beyond traditional, technology-centric views. Practically, it aims to deliver actionable insights and assessment tools that organizations can use to measure and improve their readiness, regardless of their current maturity level. By addressing the current limitations in IRM evaluation and proposing a more inclusive

and applicable model, this study supports the development of more resilient organizations capable of withstanding the evolving cyber threat landscape.

## 2. Materials and Methods

This study adopts a quantitative research methodology to assess the Cybersecurity Incident Response Readiness (CIRR) of organizations. The methodology is structured to empirically investigate the preparedness of organizations in countering cyber threats, and to explore the interrelationships among key dimensions of incident response capabilities. By employing a model-driven approach, we aim to test specific hypotheses related to organizational readiness, as detailed in Table 3. The ultimate goal is to provide actionable insights for improving cybersecurity readiness and enabling more resilient incident response strategies across diverse organizational contexts.

To collect primary data, we utilized a structured questionnaire as the main instrument. The questionnaire was specifically designed to serve as a robust quantitative tool that aligns with the study objectives. It allows for systematic data collection and statistical analysis to evaluate the maturity of incident response readiness and the influencing factors.

The questionnaire was administered in a closed-ended format to ensure consistency and reliability in the responses, and to facilitate ease of analysis.

Through this rigorous methodological approach, the study aspires to contribute empirical evidence to the field of cybersecurity management, supporting both academia and practice with measurable, data-driven.

## 3. Results

**Incident Response Readiness**

The analysis of the Incident Response Readiness (IRR) revealed that organizations generally exhibit a high level of preparedness in managing and responding to cybersecurity incidents, respondents demonstrated strong agreement with several key statements. The item "Our organization egularly monitors security alerts to detect security incidents" received the highest mean score of 4.34 (SD =0.878), reflecting an 86.8% agreement rate, indicating that most organizations prioritize continuous threat monitoring as a critical aspect of their cybersecurity strategy.

Similarly, high mean values were reported for other indicators of readiness, such as "Our organization is committed to implementing procedures to recover from security incidents" (M = 4.29, SD = 0.792; 85.8%) and "Our organization proactively prepares for emerging 147 security incidents" (M = 4.19, SD = 0.938; 83.8%). These scores suggest that not only are organizations reactive in handling incidents, but they also show strong intent to be proactive and recovery-focused in their approaches.

Furthermore, the statement "Our organization is well152 prepared to respond to security incidents" scored a mean of 4.17 (SD = 0.911; 83.5%), while "Our organization maintains uninterrupted incident handling capabilities 24/7" also received high agreement (M = 4.13, SD = 1.046;82.6%). These results emphasize that most organizations have confidence in their continuous incident response availability and general preparedness However, relatively lower, though still positive, scores were reported for resilience and response speed. The item "Our organization has the ability to stay resilient against potential incidents in the next 12 months" had a mean of 4.02 (SD = 0.993; 80.4%), and "Incident response speed (from detection to full recovery) is fast and effective" received the lowest mean score of 3.95 (SD = 0.941; 79.0%), indicating areas for potential improvement in response timeliness and long-term sustainability.

**Response Readiness Assessment**

In terms of organizational support for incident response, the most commonly reported supporting entity was the Business Continuity Team (17.39%), followed by the CISO (12.42%) and Crisis Management Team (10.56%). This reflects a distributed approach to incident response, relying on various departments. Notably, only 1.86% of respondents reported relying on Outsourced Services, suggesting that internal handling remains the dominant model.

Regarding staffing levels, a significant portion of organizations have more than 10 dedicated personnel (37.89%) or 4–10 members (32.30%) involved in incident response, highlighting a trend toward building specialized internal capabilities. However, 4.35% of organizations reported having no dedicated personnel, suggesting critical gaps in readiness for a small segment of the sample.

On the technological front, basic tools such as firewalls (21.12%) and antivirus (11.18%) were the most widely implemented. Advanced tools such as SIEM (6.21%), EDR (9.32%), and SOAR (3.11%) were less commonly adopted, indicating that while organizations have baseline protections, fewer are leveraging advanced automated response systems. Concerning incident response plan reviews, 32.92% of organizations review their plans annually, and 26.71% do so quarterly. However, 6.83% stated that their organization does not have an IR plan at all, and 16.15% were unsure about the frequency of updates, highlighting a concerning lack of formal planning or communication in some cases. Regular readiness assessments of technical teams were reported by 58.39% of respondents, while 26.09% conduct them irregularly, and 8.70% do not assess at all. Similarly, assessments of executive teams are performed regularly by only 44.10%, with 11.80% of organizations not conducting such assessments, pointing to a potential gap in leadership readiness.

In terms of methods used to evaluate IRR, the most common were monitoring metrics (25.47%), external audits (21.12%), and red team activities (13.66%), suggesting a mixture of internal and external validation strategies. However, 8.07% reported having no assessment process at all, and 8.70% were unsure.

When asked about confidence in their incident response measurement processes, 80.12% of organizations were either moderately (41.61%) or very confident (38.51%). In contrast, 16.15% were not confident, suggesting inconsistencies in methodology and assurance across organizations:

Regarding metrics used to measure readiness, Mean Time to Detection (MTTD) (19.25%) and Count of Detected Incidents (18.01%) were most common, while advanced metrics like Dwell Time (3.11%) and SLA adherence (4.97%) were rarely used. Alarmingly, 7.45% reported not using any metrics, and 16.15% were unsure—highlighting a maturity gap in performance measurement.

Finally, when asked about investment in specialized tools/software for readiness assessment, 40.37% of organizations indicated they had made no such investment, and 29.19% were unsure. Only 18.63% had invested in specific tools, suggesting a significant opportunity for improvement in measurement infrastructure.

## 4. Discussion

The results of this study provide valuable insights into the current state of Incident Response Readiness (IRR) across organizations. Overall, the data indicate a generally high level of preparedness, particularly in foundational practices such as real-time monitoring of security alerts, proactive recovery procedures, and continuous detection capabilities.
These findings align with prior literature and theoretical frameworks, particularly Institutional Theory, which posits that organizations often conform to established norms and practices to gain legitimacy and maintain competitive parity (DiMaggio & Powell, 1983). The widespread use of standard tools like firewalls and antivirus software, as well as formalized roles such as CISOs and Crisis Management Teams, reflects this normative behavior and institutional conformity

However, despite this high baseline, notable gaps emerged in more advanced areas of readiness. Specifically, the lower implementation rates of tools such as SIEM, SOAR, XDR, and Threat Intelligence Platforms suggest a lag in the adoption of modern, integrated response solutions. This may reflect financial, technical, or organizational constraints, but it also suggests that some organizations are failing to keep pace with the rapidly evolving threat landscape. From a Game Theory perspective, this may place such organizations at a strategic disadvantage in the cybersecurity "game," where adversaries adapt continuously, and response agility becomes a key competitive factor (Akinwumi et al., 2017).
Furthermore, while many organizations reported having 4–10 or more dedicated personnel for incident response, the irregular assessment of both technical and executive teams' readiness is concerning. The disconnect between operational capabilities and leadership preparedness could undermine coordinated response efforts during actual incidents. Executive teams play a critical role in strategic decision-making, resource allocation, and crisis communication. Failure to regularly assess and train these leaders reduces the overall resilience of the organization.

This observation is consistent with previous studies (Appari et al., 2009; Al-Soud et al., 2024), which stress the importance of leadership engagement in incident management.

Equally important is the limited use of performance metrics and specialized tools to evaluate incident response capabilities. While some organizations use quantitative metrics such as MTTD, MTTR, and incident resolution rates, a considerable number either lack formal assessment processes or are unsure about them. This highlights a deficiency in measurement maturity and internal communication, which directly impacts the organization's ability to identify weaknesses and improve continuously.

The Deterrence Theory provides a relevant lens here: without demonstrable and measurable readiness, organizations lose their ability to deter attackers through the perception of strength and preparedness (Powell, 2008).

Another noteworthy issue is the lack of investment in specific tools/software designed for incident response readiness assessment. The reliance on generic or no tools at all points to a reactive rather than proactive approach to cybersecurity management. This potentially undermines the accuracy of preparedness assessments and limits the ability to identify capability gaps. Moreover, uncertainty among respondents regarding their organization's investment in such tools reflects poor internal communication and awareness, which may hinder effective incident response coordination. Taken together, these findings suggest that while organizations generally recognize the importance of incident response readiness, there remains significant room for strategic, technological, and procedural improvement.

Integrating advanced technologies, conducting regular cross-functional assessments, adopting standardized metrics, and ensuring leadership readiness will be crucial steps toward building a robust cybersecurity posture.

## 5. Conclusion

This study aimed to evaluate the level of Incident Response Readiness in organizations through a comprehensive assessment of people, processes, and technologies involved in managing cybersecurity incidents. The results reveal that while many organizations have established solid foundational capabilities—such as dedicated incident response teams, frequent security monitoring, and formal recovery procedures—critical shortcomings persist in advanced readiness areas.

The findings underscore the need for organizations to move beyond basic compliance and adopt a more strategic, integrated, and proactive approach to incident response. Regular assessment of both technical and executive teams, investment in specialized tools for readiness evaluation, and implementation of a comprehensive metrics framework are all essential components of a mature incident response program.

From a theoretical perspective, the results support the applicability of Institutional Theory, Game Theory, and Deterrence Theory in understanding organizational behavior in cybersecurity contexts. Institutional pressures drive baseline compliance, competitive dynamics push for strategic investment, and perceived preparedness serves as a deterrent to adversaries. However, for these theoretical frameworks to be operationalized effectively, organizations must close

existing readiness gaps and foster a culture of continuous improvement.

Finally, enhancing Incident Response Readiness is not merely a technical challenge, but an organizational imperative that requires leadership commitment, cross functional collaboration, and a data-driven approach. Future research may build upon these findings by exploring longitudinal changes in IRR or by developing benchmarking models to assess maturity across different 341 industries and organizational sizes.

## References

[1] Ab Rahman, N. H., Glisson, W. B., Yang, Y., & Choo, K.344 K. R. (2016). Forensic-by-Design Framework for Cyber345 Physical Cloud Systems. IEEE Cloud Computing, 3(1),346 50-59. https://doi.org/10.1109/MCC.2016.5.

[2] Abdulhafedh H, Al-Saadoon A, Abu-Mejdad N (2023).348 Efficiency of Fungal β-carotene Against Some Causative349 Agents of Dermatomycoses. Iran J War Public Health; 15350 (2) :167-175. http://ijwph.ir/article-1-1339-en.html

[3] Agrafiotis, I., Nurse, J. C., Goldsmith, M., Creese, S., &Upton, D. (2018). A Taxonomy of Cyber-Harms:Defining the Impacts of Cyber-Attacks andUnderstanding How They Propagate. Journal ofCybersecurity, 4, tyy006. https://doi.org/10.1093/cybsec/tyy006

[4] Ahmad, A., Maynard, S. B., Desouza, K. C., Kotsias, J.,Whitty, M. T., & Baskerville, R. L. (2021). How canorganizations develop situation awareness for incidentresponse: a case study of management practice Computers and Security, 101, Article 102122.https://doi.org/10.1016/j.cose.2020.102122

[5] Ahmad, S, Ahmad, B, Saqib, SM & Khattak, RM 2012, 'Trust Model: Cloud's Provider and Cloud's User', International Journal of Advanced Science and Technology, vol. 44, pp. 69-80. https://www.earticle.net/Article/A206760

[6] Al-Mhiqani, Mohammed Nasser, Rabiah Ahmad, Z.Zainal Abidin, Warusia Yassin, Aslinda Hassan, Karrar Hameed Abdulkareem, Nabeel Salih Ali, and Zahri Yunos. 2020. "A Review of Insider Threat Detection: Classification, Machine Learning Techniques, Datasets, Open Challenges, and Recommendations" Applied Sciences 10, no. 15: 5208.https://doi.org/10.3390/app10155208

[7] Alsharafat W. (2013), "Applying Artificial Neural Network and eXtended Classifier System for Network Intrusion Detection", The International Arab Journal of Information Technology, Vol. 10, No.3,pp.230-238.380 https://doi.org/10.59743/aujas.v2i2.1158

[8] Arcuri, M.C., Gai, L., Ielasi, F. and Ventisette, E. (2020), "Cyber-attacks on hospitality sector: stock market reaction", Journal of Hospitality and Tourism Technology, Vol. 11 No. 2, pp. 277-290. https://doi.org/10.1108/JHTT-05-2019-0080

[9] Barnum S (2014) Standardizing cyber threat intelligence information with the structured threat information eXpression (STIX). Version 1.1, Revision1.MITRE. http://stixproject.github.io/getting-tarted/whitepaper/

[10] Becker B. E. (2009). Aquatic therapy: scientific foundations and clinical rehabilitation applications. PM & R : the journal of injury, function, and rehabilitation,1(9),859–872. https://doi.org/10.1016/j.pmrj.2009.05.017

[11] Bitzer. M, Häckel.B, Leuthe.D, Ott.J, Stahl.B, and Strobel.J. (2023). Managing the Inevitable – A Maturity Model to Establish Incident Response Management Capabilities. Comput. Secur. 125, C (Feb2023). https://doi.org/10.1016/j.cose.2022.103050

[12] Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. The Geneva papers on risk and insurance. Issues and practice, 47(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

[13] DeLuca, G. C., Kimball, S. M., Kolasinski, J., Ramagopalan, S. V., & Ebers, G. C. (2013). Review: the role of vitamin D in nervous system health and disease. Neuropathology and applied neurobiology, 39(5), 458–484. https://doi.org/10.1111/nan.12020

[14] DeVito, N. J., & Drysdale, H. (2022). Issues with reporting and interpretation of Khan et al. 2021. BMC infectious diseases, 22(1), 567. https://doi.org/10.1186/s12879-022-07551-8

[15] Jeebaratnam, N. ., Rao, B. N. ., Sesadri, U. ., Shirisha, N.., & Kumar, N. M. . (2024). Optimizing trust, Cloud Environments Fuzzy Neural Network, Intrusion Detection System. International Journal of Intelligent Systems and Applications in Engineering, 12(17s),260–275.Retrievedfrom https://ijisae.org/index.php/IJISAE/article/view/4871

[16] Kuypers, K. P., Riba, J., de la Fuente Revenga, M., Barker, S., Theunissen, E. L., & Ramaekers, J. G. (2016). Ayahuasca enhances creative divergent thinking while decreasing conventional convergent thinking. Psychopharmacology,233(18),3395–3403. https://doi.org/10.1007/s00213-016-4377-8

[17] Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers&security,105,102248. https://doi.org/10.1016/j.cose.2021.102248

[18] Mitropoulos, P., et al. (2006) A Biobjective Model for the Locational Planning of Hospitals and Health Centers. Health Care Management Science, 9, 171-179. https://doi.org/10.1007/s10729-006-7664-9

[19] Morgan, S. Humans on the internet will triple from 2015 to 2022 and hit 6 billion. Cybercrime Magazine. 2019;Availablefrom: https://cybersecurityventures.com/howmany-internet-users-will-the-world-have-in-2022-and-in2030 .

[20] Rådestad, E., Klynning, C., Stikvoort, A., Mogensen, O., Nava, S., Magalhaes, I., & Uhlin, M. (2018). Immune profiling and identification of prognostic immune-related risk factors in human ovarian cancer. Oncoimmunology, 8(2), e1535730. https://doi.org/10.1080/2162402X.2018.1535730

[21] Röglinger, M., Pöppelbuß, J. and Becker, J. (2012), "Maturity models in business process management",

Business Process Management Journal, Vol. 18 No. 2, pp. 328-346. https://doi.org/10.1108/14637151211225225

[22] Ruefle, R., Dorofee, A., Mundie, D., Householder, A.D., Murray, M. and Perl, S.J., (2014), Computer security incident response team development and evolution, IEEE Security & Privacy, 12(5), pp.16-26. https://ieeexplore.ieee.org/document/6924672

[23] Schlette, D.; Böhm, F.; Caselli, M.; Pernul, G. (2021). Measuring and visualizing cyber threat intelligence quality. Int. J. Inf. Secur. 20, 1 (Feb 2021), 21–38. https://doi.org/10.1007/s10207-020-00490-y

[24] Schmitz, A., Pinheiro Marques, J., Oertig, I., Maharjan, N., & Saxena, S. (2021). Emerging Perspectives on Dipeptide Repeat Proteins in C9ORF72 ALS/FTD. Frontiers in cellular neuroscience, 15, 637548. https://doi.org/10.3389/fncel.2021.637548

[25] . Senavongse, W., Farahmand, F., Jones, J., Andersen, H., Bull, A. M., & Amis, A. A. (2003). Quantitative measurement of patellofemoral joint stability: force displacement behavior of the human patella in vitro. Journal of orthopaedic research: official publication of the Orthopaedic Research Society, 21(5), 780–786. https://doi.org/10.1016/S0736-0266(03)00061-5

[26] Thangavelu, R., Edwin Raj, E., Pushpakanth, P., Loganathan, M., & Uma, S. (2021). Draft Genome of Fusarium oxysporum f. sp. cubense Strain Tropical Race 4 Infecting Cavendish (AAA) Group of Banana in India. Plant disease, 105(2), 481–483. 478 https://doi.org/10.1094/PDIS-06-20-1170-A

[27] Tøndel, C., Kanai, T., Larsen, K. K., Ito, S., Politei, J. M., Warnock, D. G., & Svarstad, E. (2015). Foot process effacement is an early marker of nephropathy in young classic Fabry patients without albuminuria. Nephron, 129(1), 16–21. https://doi.org/10.1159/000369309

[28] Van der Kleij, S. W., Burgess, A. P., Ricketts, J., & Shapiro, L. R. (2022). From Bibliophile to Sesquipedalian: Modeling the Role of Reading Experience in Vocabulary and Reading Comprehension. Scientific Studies of Reading, 26(6), 514–526. https://doi.org/10.1080/10888438.2022.2068418