Plan, Prepare and Respond: A Holistic Cyber Security Risk Management Platform

Dharani Goli, Hamad Al-Mohannadi and Mohammad Shah

Plan, Prepare and Respond: A Holistic Cyber Security Risk Management Platform

Dharani Goli
Computer Science and Engineering
University of Westminster
London, UK
w1868764@my.westminster.ac.uk

Hamad Al-Mohannadi
Cyber Response Department
Ministry of Defence
Doha, Qatar
almohannadi7@gmail.com

Mohammad Shah
Computer Science and Engineering
University of Westminster
London, UK
M.Shah1@westminster.ac.uk

***Abstract*—Cyber attacks pose an escalating threat to organisations, carrying the potential for substantial financial losses, reputational damage, and legal ramifications. To effectively safeguard against such attacks, organisations must adopt a proactive approach that includes comprehensive planning and preparation for potential incidents. Unfortunately, many organisations struggle in this process due to a lack of efficient mechanisms, tools, training, and processes for defending, responding to, and recovering from cyber attacks. Cyber readiness serves as a vital strategy for preparing organisations to combat these threats. However, the existing frameworks and tools available for assisting organisations in handling cyber attacks and managing cybersecurity risks are insufficient. This paper presents a holistic solution aimed at enhancing organisations' cyber readiness in responding to cyber attack events. The proposed approach involves conducting a thorough assessment of the organisation's current security posture, identifying vulnerabilities and weaknesses, and offering recommendations for improvement. By implementing this comprehensive strategy, organisations can enhance their ability to withstand and respond effectively to cyber attacks.**

***Index Terms*—Cyber Security, Cyber Risk, Cyber Risk Management, Plan, Prepare, Response**

I. INTRODUCTION

Cyber attacks have emerged as a significant threat in the modern digital landscape, posing serious risks to individuals, organisations, and even nations. These malicious activities involve unauthorized access, disruption, or manipulation of computer systems, networks, and information. Cyber attackers employ a range of sophisticated techniques, including malware, phishing, ransomware, and denial-of-service attacks, to exploit vulnerabilities in technology infrastructure and compromise sensitive data. The battle against cyber attacks requires constant vigilance cyber attack modelling system [7]. Cybersecurity security, protects computers, networks, and data from unauthorized access, use, disclosure, disruption, modification, or destruction. This includes protecting against cyber threats such as malware, hacking, and phishing attacks. In recent years, the field of cybersecurity has evolved rapidly as digital technologies have become more widespread and sophisticated. As a result, cybersecurity has become an increasingly important concern for individuals, businesses, and governments. Figure 1 shows that as the technology evolves the cyber threats evolves exponentially.

One major change in cybersecurity in recent years has been the increasing use of cloud computing, which has introduced new challenges and risks [1]. For example, using cloud-based services has made it more difficult to secure data, as it is often stored and accessed in multiple locations [2]. In addition, the rise of mobile devices and the Internet of Things (IoT) has increased the number of potential entry points for cyber threats [3]. Another key change in the field of cybersecurity has been the growing sophistication and complexity of cyber threats. Cyber criminals have become increasingly organized and well-funded and have developed a range of sophisticated tactics and technologies to evade detection and compromise networks and systems.

In response to these changes, the field of cybersecurity has also evolved to become more proactive and preventive. This has involved the development of new technologies and techniques to detect and defend against cyber threats and implement more effective risk management and incident response processes [22]. The importance of having cyber risk insurance [5] has also increased in recent years, as the potential costs of a cyber-attack can be significant and can derail the company's business. Cyber insurance [15] can help to protect an organisation against the risk of financial impact from a cyber-attack by covering the costs of responding to the attack and restoring systems and data. This can include expenses such as legal fees, forensic investigation costs, and the cost of providing credit monitoring services to affected customers.

The paper follows a structured organisation, beginning with a background studies of cyber readiness and cyber security risk management in section II. In section III, the architecture of the proposed framework is presented, outlining its key components and functionalities. The subsequent section, section IV, presents the findings and results obtained from implementing the framework, highlighting its effectiveness in enhancing cyber readiness. Finally, the paper concludes by summarising the key findings, discussing their implications, and offering future directions for further research and development in this domain.

II. BACKGROUND

A key aspect of cybersecurity is risk management [4], which involves identifying and assessing potential risks and

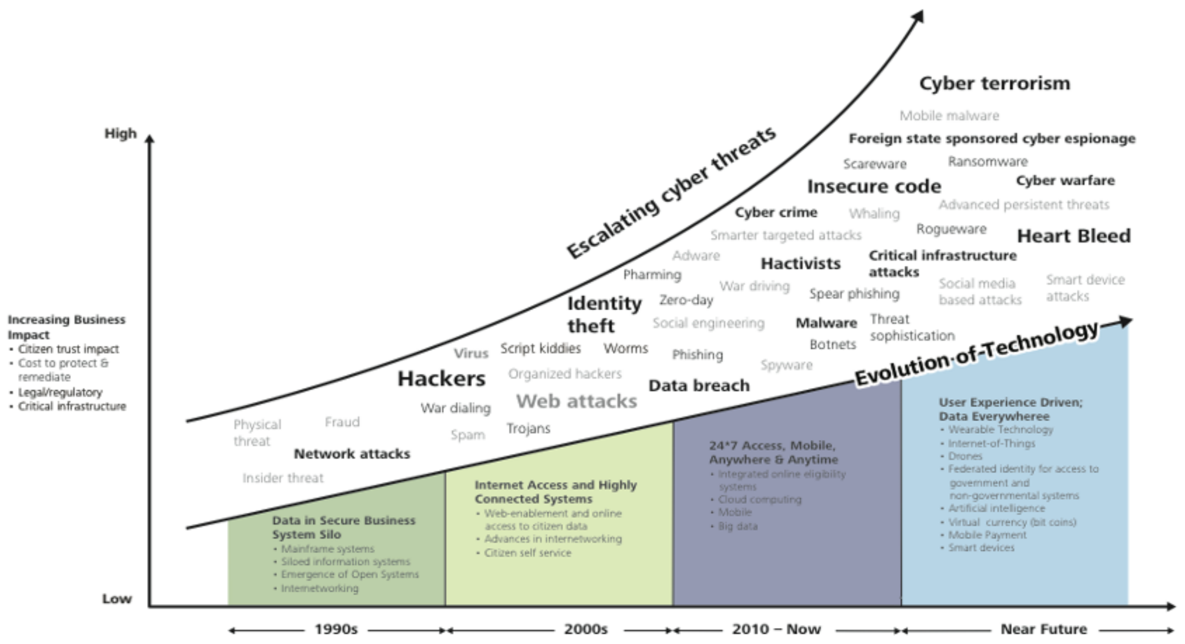

Fig. 1. Evolving technology and rapidly escalating cyber threats call for a deliberate approach to make commanding progress (Source: Reproduced from the 2014 Deloitte-NASCIO Cybersecurity Study “State governments at risk: Time to move forward”)

implementing strategies to mitigate or prevent them. This often involves conducting cybersecurity analysis, which evaluates an organisation’s security posture and identifies potential vulnerabilities. Once potential risks have been identified, cybersecurity management involves implementing and maintaining effective security measures to protect against them [6]. This may include implementing technical controls such as firewalls and intrusion detection systems and policies and procedures to educate and train leadership teams and employees on cybersecurity best practices [12].

Cyber incidents and resulting losses have been steadily increasing in recent years. According to a report by the Cybersecurity and Infrastructure Security Agency (CISA), the number of cyber incidents reported to the agency increased by over 50% from 2018 to 2019 [9]. Similarly, a study by the Ponemon Institute found that a company's average cost of a data breach increased by 6.4% in the past year, reaching an average of $3.86 million [8]. Cyber incidents’ increasing frequency and severity have also garnered attention from policymakers and industry experts. In 2019, the World Economic Forum identified cyber-attacks as one of the global economy’s top five risks [10]. This highlights the importance of addressing the rising cyber incidents and losses trend.

Cybersecurity risk is a significant concern for businesses and organisations of all sizes. According to a report by the National Institute of Standards and Technology (NIST), the cost of cyber-attacks on the global economy is estimated to be $3 trillion annually [11]. This trend is concerning as the impact of a cyber-attack can be significant, leading to financial losses, legal liabilities, and damage to an organisation’s reputation. One key factor contributing to cybersecurity risk is the sensitivity of the information being protected. The more sensitive the information, the higher the risk of a cyber-attack, as hackers may be more motivated to target it. For example, a healthcare organisation handling sensitive patient data may be at a higher risk of cyber-attacks than a retail business with less sensitive information [18].

Organizations face cybersecurity risks that can be heightened by various factors, including vulnerabilities introduced by employees [12]. Technical vulnerabilities, such as outdated software, can serve as entry points for adversaries seeking unauthorized access to systems. Moreover, weak passwords and a lack of security training among employees can further amplify the risk of cyber attacks [13]. Additionally, the likelihood of a cyber attack plays a crucial role in determining cybersecurity risk. Certain industries or organizations with a substantial online presence may face a higher likelihood of being targeted. The level of security measures implemented within an organization also significantly influences its cybersecurity risk [14].

Finally, the cost of implementing and maintaining effective cybersecurity measures is a factor that can contribute to cybersecurity risk [19]. While implementing such measures can be expensive, the potential losses from a cyber-attack can be even greater. Therefore, it is important for businesses to carefully consider the cost-benefit of implementing cybersecurity measures. Cybersecurity risk is a complex and dynamic concept that depends on various factors. It is important for organisations to regularly assess and manage their cybersecurity risk to protect against potential threats. Cyber readiness [21] is refers as the preparedness or the ability to act against the cyber atack [17] [20].

This paper presents a comprehensive approach to enhance cyber readiness within organisations, focusing on effectively combating cyber attacks through systematic planning, preparation, and response strategies. The proposed approach encompasses a holistic framework that addresses various aspects of cyber threats. In addition, the methods outlined in this research are thoroughly tested to validate their effectiveness. Based on the results, actionable recommendations are provided to guide organizations in improving their cyber readiness measures.

III. Proposed Model

In this project we proposed a cyber risk management system called ’molecules’ that allows organisations to take a holistic approach to cyber risk readiness. The platform is divided into three phases, allowing organisations to **plan**, **prepare**, and **respond** to threats systematically and comprehensively. With hands-on metrics and an easy-to-use interface, Molecules is designed to be accessible to organisations of all sizes and levels of expertise as shows in figure 2.

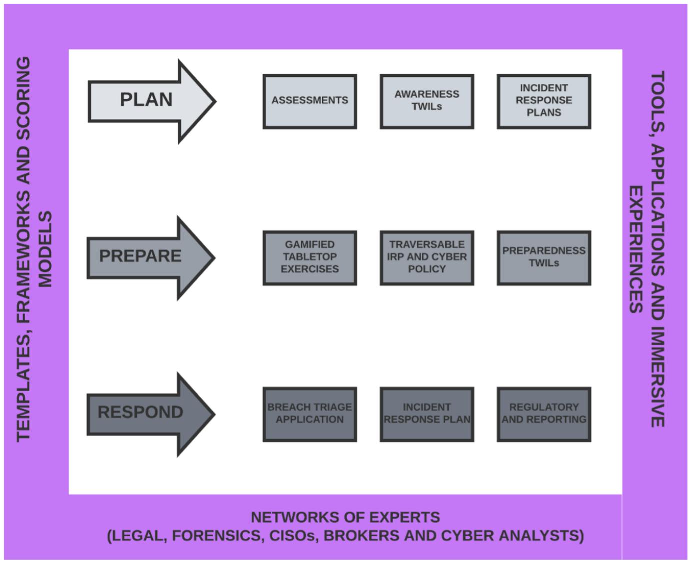
TEMPLATES, FRAMEWORKS AND SCORING MODELS
PLAN
ASSESSMENTS
AWARENESS TWILs
INCIDENT RESPONSE PLANS
PREPARE
GAMIFIED TABLETOP EXERCISES
TRAVERSABLE IRP AND CYBER POLICY
PREPAREDNESS TWILs
RESPOND
BREACH TRIAGE APPLICATION
INCIDENT RESPONSE PLAN
REGULATORY AND REPORTING
TOOLS, APPLICATIONS AND IMMERSIVE EXPERIENCES
NETWORKS OF EXPERTS
(LEGAL, FORENSICS, CISOs, BROKERS AND CYBER ANALYSTS)

Fig. 2. Overall architecture of MOLECULES

A. Plan

The planning phase of cyber risk management includes a concept called the cyber readiness score, which is an overall evaluation of an organisation’s level of preparedness for cyber threats. This score is calculated based on four key areas: awareness, preparedness, responsiveness, and recoverability figure 3.

Awareness measures an organisation’s understanding of its current level of cyber risk and its efforts to educate employees and stakeholders about potential threats. This may include things like cyber risk assessments, training programs, and communication campaigns. It is calculated based on various parameters, including awareness levels, questionnaire responses, and tests or evaluations scores. This score may also include input from third parties, such as partners or vendors, on their readiness to support the organisation in the event of a cyber incident.

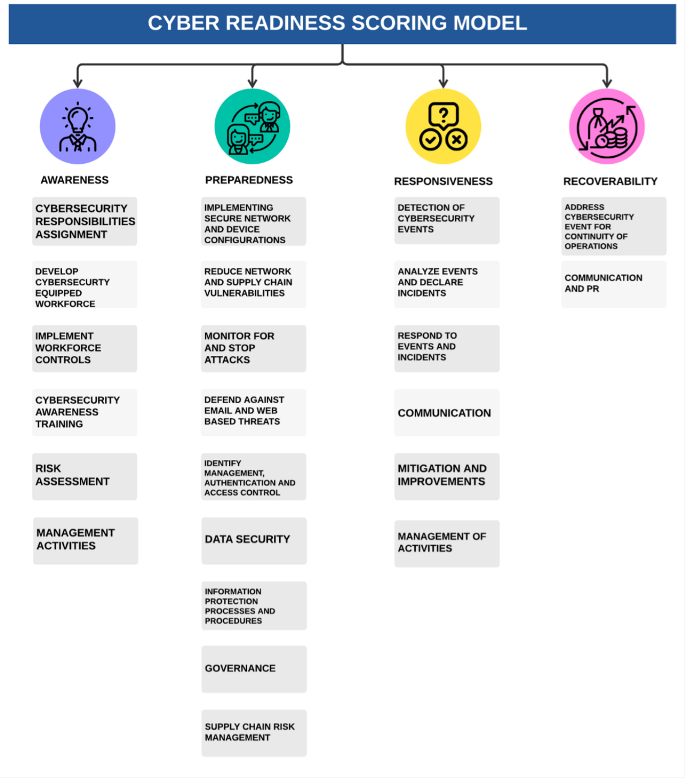
CYBER READINESS SCORING MODEL
AWARENESS
CYBERSECURITY RESPONSIBILITIES ASSIGNMENT
DEVELOP CYBERSECURTY EQUIPPED WORKFORCE
IMPLEMENT WORKFORCE CONTROLS
CYBERSECURITY AWARENESS TRAINING
RISK ASSESSMENT
MANAGEMENT ACTIVITIES
PREPAREDNESS
IMPLEMENTING SECURE NETWORK AND DEVICE CONFIGURATIONS
REDUCE NETWORK AND SUPPLY CHAIN VULNERABILITIES
MONITOR FOR AND STOP ATTACKS
DEFEND AGAINST EMAIL AND WEB BASED THREATS
IDENTIFY MANAGEMENT, AUTHENTICATION AND ACCESS CONTROL
DATA SECURITY
INFORMATION PROTECTION PROCESSES AND PROCEDURES
GOVERNANCE
SUPPLY CHAIN RISK MANAGEMENT
RESPONSIVENESS
DETECTION OF CYBERSECURITY EVENTS
ANALYZE EVENTS AND DECLARE INCIDENTS
RESPOND TO EVENTS AND INCIDENTS
COMMUNICATION
MITIGATION AND IMPROVEMENTS
MANAGEMENT OF ACTIVITIES
RECOVERABILITY
ADDRESS CYBERSECURITY EVENT FOR CONTINUITY OF OPERATIONS
COMMUNICATION AND PR

Fig. 3. Architecture of Cyber Readiness Scoring Model

Preparedness evaluates an organisation’s readiness to respond to a cyber incident. This includes things like incident response plans, tabletop exercises, and the availability of necessary resources and tools. It is calculated based on various parameters, including a review of current incident response plans (IRPs), the effectiveness of call-tree responses, and responses to a preparedness questionnaire from employees, IT, security, legal, and HR departments. The score may also include input from other sources, such as a workflow engine.

Responsiveness assesses an organisation’s ability to respond quickly and effectively to cyber incidents. This includes things like incident response protocols, communication plans, and the use of specialized tools and resources. It is calculated based on various parameters related to the response phase of incident management.

Recoverability evaluates an organisation’s plans and capabilities for restoring services and capabilities that may be impaired due to a cyber incident. This may include things like disaster recovery plans, backup systems, and contingency plans. It is calculated based on a variety of parameters related to the recoverability phase of incident management.

Scoring Criteria The scores used to evaluate an organ-

TABLE I
SCORE RESPONSE AND DESCTIPTION OF SCORING CRITERIA

Response	Implementation Description
Fully Implemented (FI)	Complete
Largely Implemented (LI)	Complete, but with a recognized opportunity for improvement
Partially Implemented (PI)	Incomplete; there are multiple opportunities for improvement
Not Implemented (NI)	Absent; the practice is not performed by the organisation

TABLE II
SCORE-RANGE WITH PROFILE DEPICTION

Scores	Organisation Profile
90 - 100	Best prepared organisations (very low risk)
75 - 89	Low Risk Organisations
65 - 74	Medium Risk Organisations
50 - 64	Medium High-Risk Organisations
Below 50	High Risk Organisations

isation's level of awareness, preparedness, responsiveness, and recoverability are based on responses entered by a self-evaluation tool. These responses are categorized based on the level of implementation of each practice, with options ranging from fully implemented to not implemented. Table I shows the categories include fully implemented (FI), largely implemented (LI), partially implemented (PI), and not implemented (NI).

Upon completion of the evaluation process, participants will be given a score reflecting their organisation's overall cybersecurity posture (Table II). The scoring system will help the organisations to identify their level of preparedness.

B. Prepare

The preparation phase of cyber risk management focuses on helping organisations prepare for a potential cyber incident. It includes several approaches and tools, including:

Gamified Tabletop Exercises: These are simulated cyber incidents that allow organisations to practice and refine their incident response plans. By participating in these exercises, organisations can identify areas of weakness and improve their overall preparedness 4. There are several reasons why gamification [16] is encouraged for educating organisations about cyber-attacks and risks:

- Interactiveness
- Collaborativeness
- Hosted Virtually
- Multisensory
- Real-world Simulaiton
- Continuous Learning

Breach Triage Runs: These are practice sessions that allow organisations to test and familiarize themselves with the breach triage process. This can help them quickly and effectively assess and respond to cyber incidents.

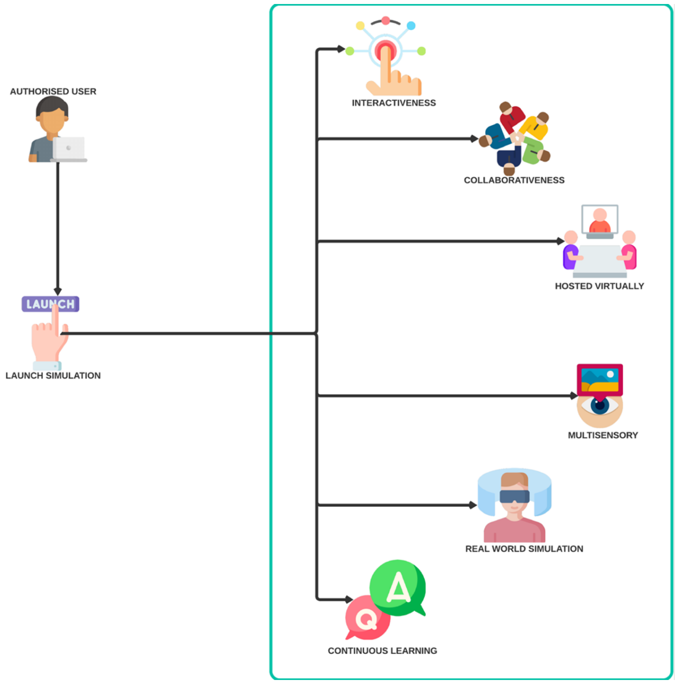

Fig. 4. User flow and key concepts of Immersive Gamification Platform

Preparedness TWILs: These are virtual representations of key individuals or systems that can be used to test and refine incident response plans. By using preparedness TWILs, organisations can ensure that they are prepared to handle various scenarios.

Traversable Document Navigation: Traverse is a crucial tool for responding to a cyber incident. The Traverse platform is designed to help policyholders, agents, and underwriters better understand key terms, concepts, and insights related to insurance policies.

Traverse is a tool that is designed to help users better understand and prepare for unforeseen cyber incidents. It addresses the issue of lengthy document navigation by providing an easily navigable platform with interactive features such as voice and animation and detailed explanations and illustrations. This helps to make the learning process more engaging and efficient (Figure 5).

Key features of Traverse are:

- View
- Navigate
- Learn
- Track
- Act

C. Respond

The response phase of cyber risk management is focused on acting in the event of a cyber incident. It includes several approaches and tools, including:

Breach Response Actions: These are the specific steps that an organisation takes to address a cyber incident. This may include things like disconnecting affected systems, shutting

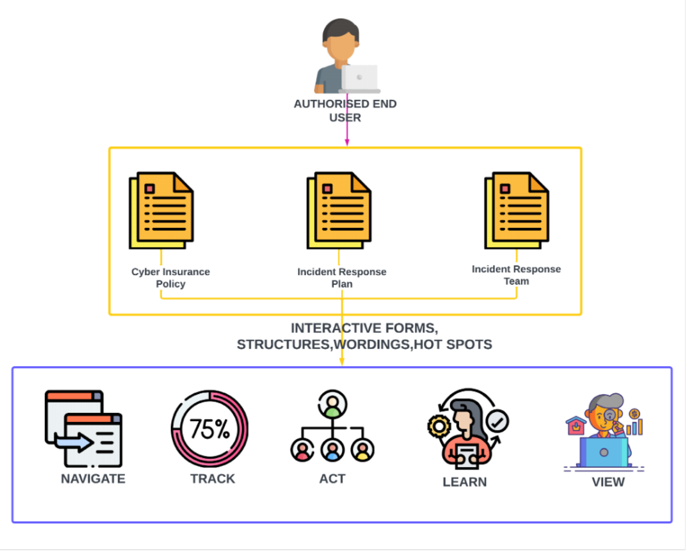

Fig. 5. User flow and key concepts of TRAVERSE- Immersive document navigation platform

down access to certain data, and implementing other measures to prevent the incident from spreading.

Remediations: After a cyber incident has been contained, it is important to take steps to prevent it from happening again. This may involve implementing new security measures, updating policies and procedures, or training employees on cyber risk awareness.

Regulatory Reporting: Depending on the nature of the incident and the regulations that apply to the organisation, there may be a need to report the incident to regulatory authorities. The response phase may include efforts to fulfil any necessary reporting requirements.

Breach Triage Application: The breach triage app is a reliable tool for managing cyber incident response because it provides access to many important features and resources. Some of the key reasons why the app is a valuable component of a cyber incident response plan include:

- Access to all employees
- Ability to report incidents and track actions
- Ability to run trial breach runs
- Access to responsiveness score
- Access to incident metrics
- Access to all teams in breach triage
- Ability to add and track chronological updates

IV. Result and Discussion

A. Cyber Readiness Score Results

Methodology: The testing and results of a cyber readiness [17] score involve the assessment of an organisation's awareness, preparedness, responsiveness, and recoverability in the event of a cyber incident. These four modules are evaluated through a series of questions posed to individuals within the organiation, ranging from C-level executives to employees. During the testing process, the scores for each module are calculated based on the answers received from the employees of the organisation. The final score for the overall model is then curated based on the scores for each individual module. To visualize the results, graphs are used to depict the scores for each module and the overall model. These graphs can help to identify areas of strength and weakness within the organisation and highlight areas that may require improvement. Based on the results of the cyber readiness score, recommendations will be made to the organisation for better preparedness. These recommendations include the implementation of specific security controls, the development of incident response plans to improve the organisation's overall cyber readiness and suggest accurate insurance policies.

Test Results: Scoring Dashboard of the organisation with overall Cyber Readiness Score along with metrics of average degree of importance, average score of each module, weighted score, and step score where step index is set to 50 (Figure 6).

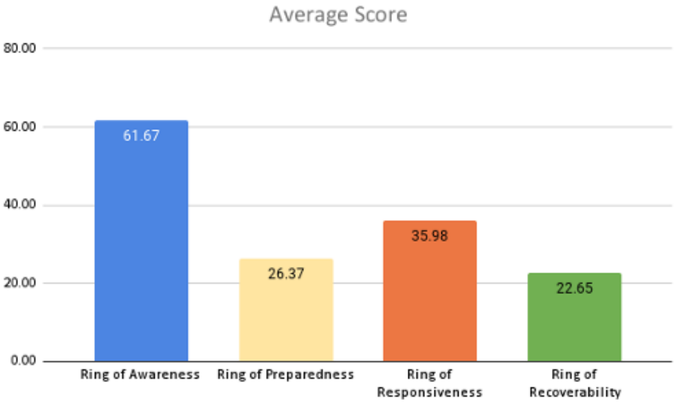

Fig. 6. Cumulative Metrics of X Inc. Organisation

Recommendations: After looking at the metrics and the scores of the organisation we can conclude that this organisation is at HIGH RISK. Hence the following recommendations can be made based on the response received: AWARENESS- Cybersecurity training should include periodic cyber risk drills as part of the program. Overall graph of Awareness (Figure 7)

PREPAREDNESS- To gather more information about a cyber incident, analysers can be run. However, it is important to filter and clean up the data, as there may not be enough time to review and analyse every indicator. It is recommended to focus on the most suspicious activity. Overall graph of Preparedness (Figure 8).

RESPONSIVENESS- Containment strategies should be developed for the most common cyber-attacks, and all evidence related to an incident should be saved and stored for future reference and shared with relevant personnel.

RECOVERABILITY- Eradication and recovery efforts should be carried out in stages to allow for the prioritization of remediation actions. It is important to note that removal and restoration procedures may vary depending on the specific operating system or application being used.

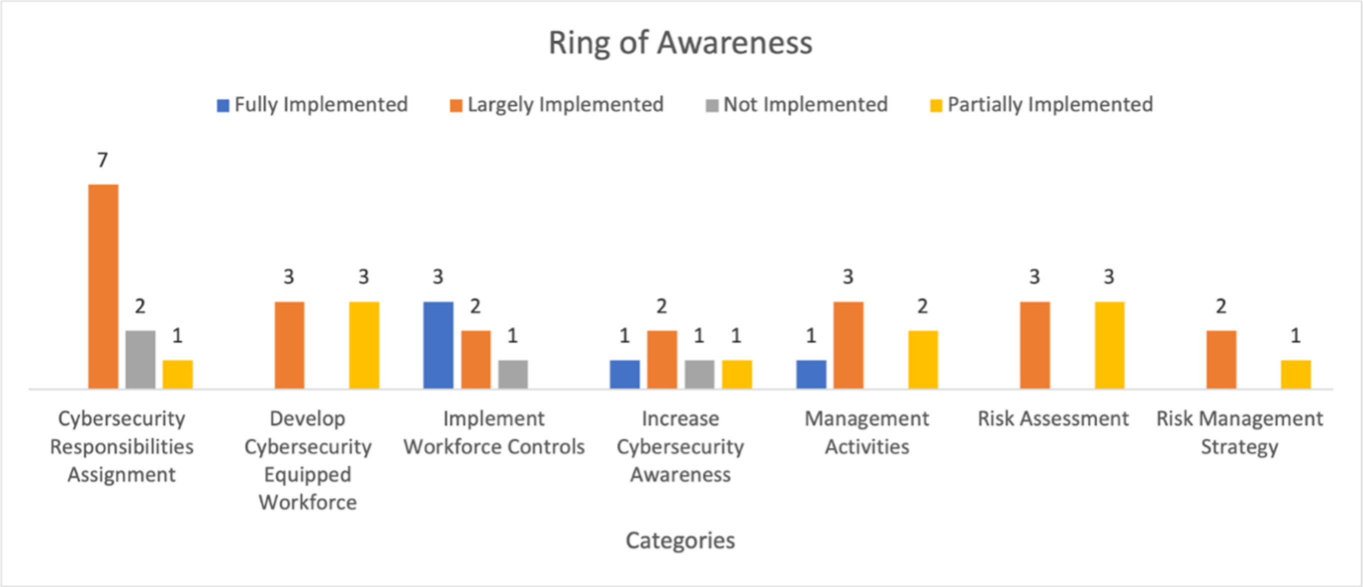

Fig. 7. Awareness Metrics of X Inc. Organisation

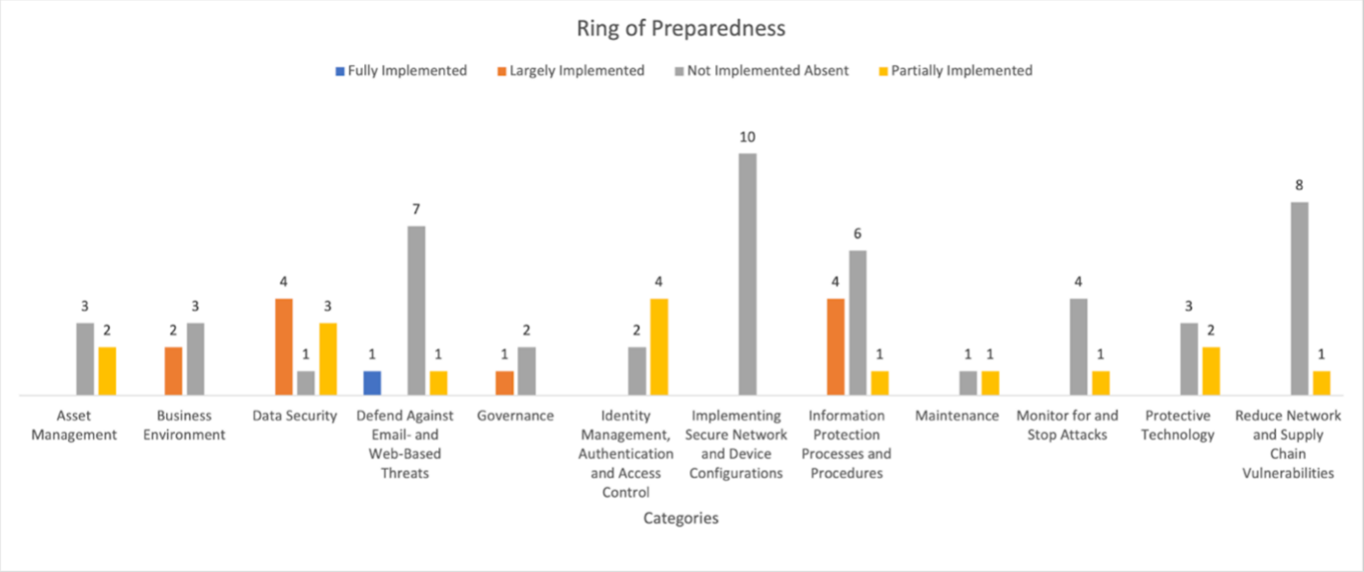

Fig. 8. Preparedness Metrics of X Inc. Organisation

B. *Gamified Tabletop Exercise Results*

Methodology: The gamified tabletop exercise tested a scenario of a ransomware attack and was designed to provide players with an immersive and realistic experience of managing such an incident. During the exercise, users were able to choose their role and permissions and watch a trailer to provide context for the scenario. The animated dialogs simulated real-life conversations that might occur when a breach is detected, allowing players to understand the unfolding of events and consider various questions and considerations before deciding on a course of action. Players were also presented with multiple choice questions and wild cards designed to challenge their knowledge and decision-making skills as they progressed through the simulation. They were able to learn about the process of engaging external parties, which is typically part of a company's incident response plan. The layout of the situation room was provided by an inventory of options, with the flexibility to customize the experience to the organisation's specific needs. The questions, visual renderings, and animations were all determined based on the organisation's requirements. The results of the gamified tabletop exercise demonstrated its effectiveness in providing a realistic and immersive learning experience for managing a ransomware attack. It allowed players to understand the

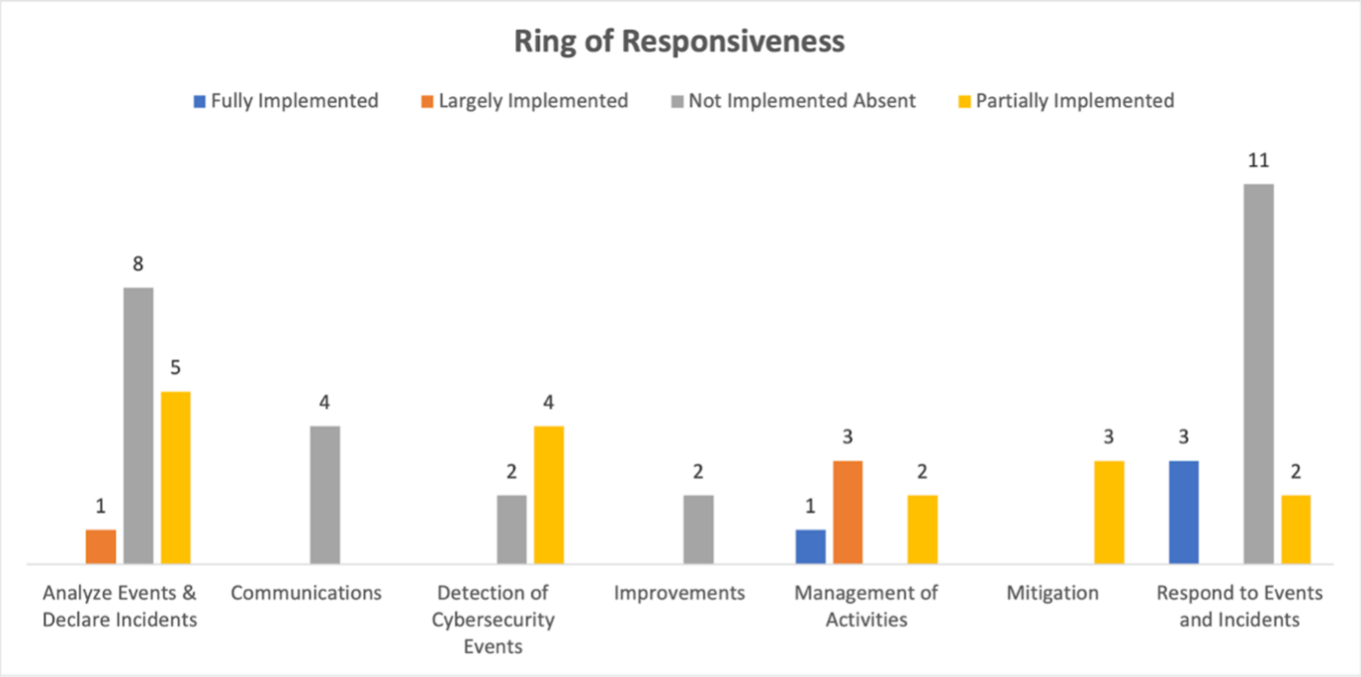

Fig. 9. Responsiveness Metrics of X Inc. Organisation

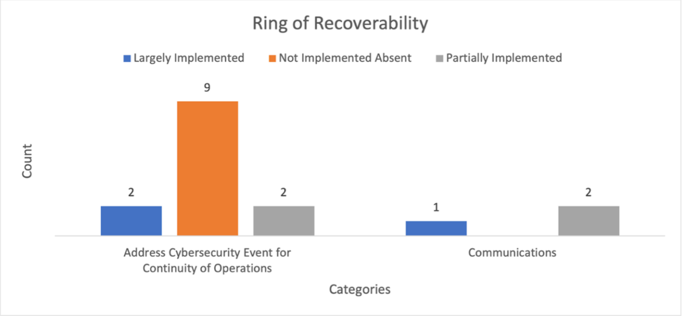

Fig. 10. Recoverability Metrics of X Inc. Organisation

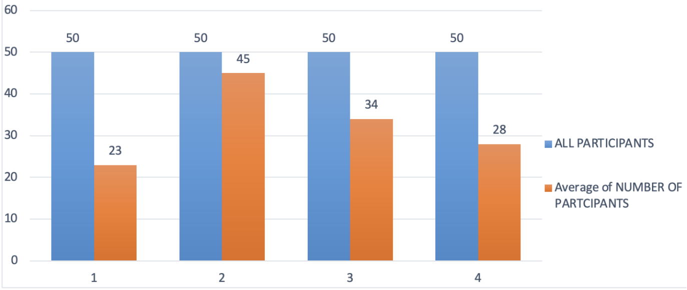

Fig. 11. Overall Participants visual of Gamified Tabletop exercise

process of responding to such an incident and make informed decisions in a simulated environment (Figure 11).

Test Results: The participants for this study were asked to log into the system via an APA link using their personal devices. Once logged in, the questions for the scenario were displayed on their screens. Each participant was asked to choose the desired answer for 4 questions and submit their responses. This process allowed the participants to engage with the material and provide their input in a convenient and accessible way. The use of personal devices also allowed for greater flexibility and allowed the participants to complete the exercise at their own pace. Overall, the use of an APA link and personal devices proved to be

Recommendations: The results of this study showed that not all participants who logged in completed all of the questions. Out of a total of 50 participants, an average of 32 logged in and participated as shows in figure 12. Despite this, these types of sessions can be useful for improving preparedness and resilience. As such, it is recommended to continue conducting similar exercises as part of a continuous learning process. By participating in these sessions, organisations can better understand and prepare for potential cyber threats and improve their overall resilience to such risks. Overall, the results of this study highlight the importance of ongoing training and learning to ensure that organisations are well-equipped to manage cyber risk.

V. Conclusion

In conclusion, the testing and implementation of the Molecules platform have successfully achieved the objectives of this research project. The platform has proven to be an effective tool for helping organisations plan and prepare for cyber risks, while also educating their leadership teams and staff on how to respond to attack situations or incidents. The development of a measurable cyber readiness score has

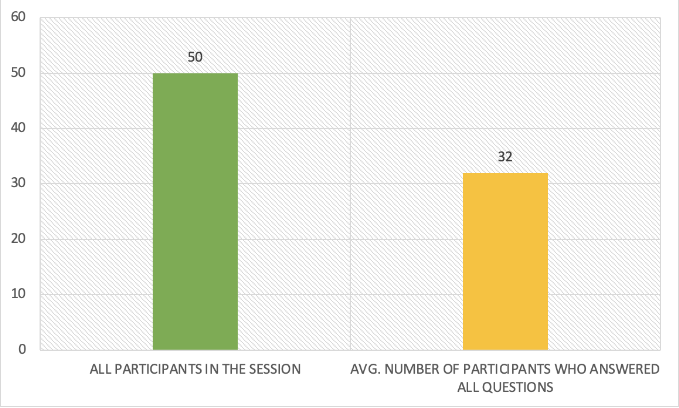

Fig. 12. Average number of participants actively participated during Gamified Tabletop exercise

provided organisations with a valuable means of assessing and enhancing their level of preparedness against cyber risks.

The Molecules platform has addressed organisations' current cyber exposures by offering a comprehensive approach to managing cybersecurity risks. Through gamified cyber simulations created by experienced professionals, the platform facilitates continuous awareness, preparedness, responsiveness, and recoverability training exercises. Traditionally, preparedness exercises and drills have often been neglected, but the escalating scale and intensity of cyber attacks, along with the associated devastating losses, emphasize the urgent need for ongoing improvement through practice. The Molecules platform's immersive attributes, user-friendly interface, and accessibility contribute to better preparedness.

It is crucial to recognize that a cyber breach is deemed an act of terrorism in the UK, regardless of its magnitude. Such attacks disrupt financial operations, diminish employee and client morale, and tarnish an organisation's reputation. Additionally, legal penalties and fines can be imposed if the breached entity is found to be non-compliant with regulations such as the UK's GDPR, Canada's PIPEDA, and the USA's SEC reporting requirements and CCPA. By utilizing the insights gained from the platform's exercises, organisations can avoid unpleasant encounters with these regulatory bodies through proper preparation and proactive actions.

This research demonstrates that the Molecules platform, encompassing its modules, significantly enhances an organisation's ability to defend against cyber risks and effectively manage them, thereby mitigating the financial and reputational impacts of a breach. Notably, the Breach Triage module, gamified tabletop exercises, and the Traverse module have proven instrumental in improving an organisation's defensible positioning and identifying actionable items within their incident response plan.

Future work will involve utilizing the collected data from the current system to develop a machine learning model aimed at enhancing the performance of cyber readiness. By leveraging advanced technologies, the platform can continue evolving to further enhance organisations' cybersecurity posture and their ability to effectively combat emerging cyber threats.

References

[1] Singh, Ashish, and Kakali Chatterjee. ”Cloud security issues and challenges: A survey.” Journal of Network and Computer Applications 79 (2017): 88-115.

[2] Kumar, Rakesh, and Rinkaj Goyal. ”On cloud security requirements, threats, vulnerabilities and countermeasures: A survey.” Computer Science Review 33 (2019): 1-48.

[3] Hassan, Wan Haslina. ”Current research on Internet of Things (IoT) security: A survey.” Computer networks 148 (2019): 283-294.

[4] Alahmari, Abdulmajeed, and Bob Duncan. ”Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence.” 2020 international conference on cyber situational awareness, data analytics and assessment (CyberSA). IEEE, 2020.

[5] Eling, Martin, and Werner Schnell. ”What do we know about cyber risk and cyber risk insurance?.” The Journal of Risk Finance 17.5 (2016): 474-491.

[6] Hubbard, Douglas W., and Richard Seiersen. How to measure anything in cybersecurity risk. John Wiley & Sons, 2023.

[7] Al-Mohannadi, Hamad, et al. ”Cyber-attack modeling analysis techniques: An overview.” 2016 IEEE 4th international conference on future internet of things and cloud workshops (FiCloudW). IEEE, 2016.

[8] IBM Security and Ponemon Institute. ”Cost of a Data Breach Report”. Available at: https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf. (2020).

[9] CISA. ”Cybersecurity and Infrastructure Security Agency (CISA) 2020 Review Report”. Available at: https://www.cisa.gov/sites/default/files/publications/CISA. (2020).

[10] Mariarosaria, T, Francesca, B. We Must Treat Cybersecurity As A Public Good. Here's Why: final report. World Economic Forum. Available at: https://www.weforum.org/agenda/2019/08/we-must-treat-cybersecurity-like-public-good/ . (2019).

[11] NIST, ”National Institute of Standards and Technology, 2020 Cybersecurity and Privacy Annual Report”. U.S. Dept of Commerce, (2020).

[12] Al-Mohannadi, Hamad, et al. ”Understanding awareness of cyber security threat among IT employees.” 2018 6th international conference on future internet of things and cloud workshops (ficloudw). IEEE, 2018.

[13] Luiijf, Eric. Understanding cyber threats and vulnerabilities. Springer Berlin Heidelberg, 2012.

[14] Kumar, Saurabh, et al. ”Antecedents for enhanced level of cyber-security in organisations.” Journal of Enterprise Information Management 34.6 (2021): 1597-1629.

[15] Gordon, Lawrence A., Martin P. Loeb, and Tashfeen Sohail. ”A framework for using insurance for cyber-risk management.” Communications of the ACM 46.3 (2003): 81-85.

[16] Omar, Nurul Suraya, et al. ”Malware awareness tool for internet safety using gamification techniques.” Journal of Physics: Conference Series. Vol. 1874. No. 1. IOP Publishing, 2021.

[17] Makridis, Christos Andreas, and Max Smeets. ”Determinants of cyber readiness.” Journal of Cyber Policy 4.1 (2019): 72-89.

[18] Coronado, Anthony J., and Timothy L. Wong. ”Healthcare cybersecurity risk management: Keys to an effective plan.” Biomedical instrumentation & technology 48.s1 (2014): 26-30.

[19] Kure, Halima Ibrahim, Shareeful Islam, and Mohammad Abdur Razzaque. ”An integrated cyber security risk management approach for a cyber-physical system.” Applied Sciences 8.6 (2018): 898.

[20] Makridis, Christos Andreas, and Max Smeets. ”Determinants of cyber readiness.” Journal of Cyber Policy 4.1 (2019): 72-89.

[21] O'Rourke, Morgan. ”Assessing cyber readiness.” Risk Management 65.3 (2018): 52-52.

[22] Lee, In. ”Cybersecurity: Risk management framework and investment cost analysis.” Business Horizons 64.5 (2021): 659-671.