Utilizing Operation Research for Enhancing Information Security and Combating Cybercrime

Moamar Shakir Mahmood
M.sc, Al-Iraqia University, college of Dentisry of Baghdad
Iraq
moamar.mahmood@aliraqia.edu.iq

Ibtehal Shakir Mahmoud
M.sc, Al-Iraqia University, college of Media Press Department
Baghdad, Iraq
ibtehal.shaker@aliraqia.edu.iq

Zuhair Yaseen Taha
Aliraqia University Baghdad
Iraq
zuhair.taha@aliraqia.edu.iq

Abstract*— this study delves into the dynamic landscape of cybercrime, emphasizing the critical need for proactive methodologies in predicting and mitigating evolving threats. Recognizing the pivotal role of operations research, the research explores its potential to assess vulnerabilities, conduct risk analyses, and develop robust defense mechanisms against diverse cyber threats. The study further aims to address a crucial criterion in information security—the time duration criterion—focusing on formulating strategies to optimize incident response protocols. The research methodology employs a Monte Carlo simulation approach, utilizing Primavera Risk Analysis software, to simulate cyber-attacks. The simulations consider various criteria, including the success rate, attack duration, and time required for attackers to breach a website. The objective is to acquire a probabilistic understanding of potential outcomes and uncertainties in cyber-attack scenarios, contributing valuable insights to enhance information security and combat cybercrime. The results of the cyber-attack simulations reveal the dynamic nature of cyber threats, emphasizing the critical role of time in mitigating and terminating attacks. Key findings include insights into attack success rates, attack durations, and the time required for attackers to breach a website, underscoring the need for time-sensitive responses and adaptive security measures. Based on the findings, the study offers several recommendations to enhance cybersecurity measures. These recommendations include adopting a time-centric strategy, prioritizing early detection and response, strengthening security measures, continuous monitoring, implementing data encryption and obfuscation, adopting adaptive security strategies, investing in cybersecurity training, developing incident response plans, fostering collaboration and information sharing, and conducting regular cyber-attack simulations and testing.

Keywords*— *Cybercrime - Information security - Monte Carlo simulation- Time-sensitive responses - Attack success rates

I. INTRODUCTION

In today's digital landscape, where organizations rely heavily on information technology for their operations, ensuring robust information security has become paramount. However, the proliferation of cyber threats and the sophistication of cybercriminals present significant challenges to maintaining a secure environment. In response to these challenges, researchers and practitioners have increasingly turned to operations research (OR) methodologies to bolster information security measures and combat cybercrime effectively.

Previous works have explored various aspects of utilizing OR techniques in information security, highlighting their potential to optimize resource allocation, enhance risk management, and improve incident response capabilities. However, there remains a need for a comprehensive understanding of how OR can be integrated into cybersecurity practices to address emerging threats and vulnerabilities effectively[1].

In recent years, the escalating frequency and sophistication of cyber-attacks have underscored the imperative for organizations and nations to fortify their information security systems. This imperative is further emphasized in the existing literature, which reveals the profound impact of cybercrime on diverse sectors. [2] Illuminates the severe operational disruptions that cyber-attacks can inflict on an organization's IT environment. The contemporary cybercrime landscape, evolving at an unprecedented pace, poses challenges that often outpace the ability of decision-makers to assess and counter effectively. This study accentuates the critical importance of crafting robust security strategies and proactively addressing issues related to cybercrime within organizational risk management approaches. In [3] explores the burgeoning interest in biometric authentication as a defense mechanism against cyber threats. With a focus on the banking sector, the study delineates the challenges posed by the surge in online financial services and the corresponding need for heightened security. Biometric security emerges as a reliable solution, leveraging distinct physical and behavioral traits for identification verification. The research highlights the effectiveness of biometric authentication in countering security threats in internet banking, emphasizing its accuracy and reliability in the face of evolving cyber risks. Addressing the broader landscape of national cybersecurity strategies, [4] conducts a comprehensive analysis of selected National Cybersecurity Strategic Plans (NCSPs) globally. The study scrutinizes existing cybersecurity education initiatives embedded in these strategic plans and proposes the adoption of the Goal-Question-Outcomes (GQO) + Strategies paradigm to enhance cybersecurity education and training programs. By aligning curricula with national cybersecurity strategic goals, the study envisions a more robust and sustainable national cybersecurity workforce, addressing the critical skills gap in the face of evolving cyber threats. As the threat landscape of cybercrime continues to evolve, the need for proactive methodologies capable of predicting and mitigating future threats becomes imperative. Operations research stands out as a valuable tool, offering the potential to assess vulnerabilities, conduct risk analyses, and develop robust defense mechanisms against diverse cyber threats. Additionally, it enables the enhancement of incident response strategies, ensuring swift and efficient mitigation of damages in the aftermath of a cyberattack [5]. Within this context, the research seeks to address a critical criterion in the realm of information security – the time duration criterion. Recognizing the significance of time as a pivotal factor, this study aims to investigate the time dimension as one of the

most crucial criteria when formulating strategies for organizations to bolster their incident response protocols. The application of operations research techniques is integral to this investigation, as it offers a systematic approach to developing strategies that can be instrumental in safeguarding institutions against the escalating threat of cybercrime. The research aims to uncover insights that will contribute to the effective utilization of operations research in enhancing information security and combating cybercrime, with a specific focus on optimizing incident response protocols.

This research aims to bridge the gap in existing literature by providing a systematic exploration of the application of operations research in enhancing information security and combating cybercrime. By examining relevant methodologies, case studies, and best practices, this study seeks to elucidate the potential benefits and challenges of leveraging OR techniques in cybersecurity contexts.

II. Frameworks and Methodologies Integrating

Security risks based on factors such as frequency, impact, and vulnerability. It provides a structured approach to risk assessment and management, allowing organizations to prioritize security investments effectively. [6]

- Strengths: FAIR offers a systematic methodology for assessing and communicating security risks in a quantitative manner, enhancing decision-making processes. It provides a common language for discussing risk among stakeholders.
- Limitations: FAIR may require significant effort and expertise to implement effectively. Quantifying certain risk factors, such as impact or frequency, can be challenging and may introduce subjectivity into the analysis.

III. STAMP (Systems-Theoretic Accident Model and Processes)

- Description: STAMP is a systems thinking-based approach to understanding accidents and failures in complex systems, including information security systems. It focuses on identifying and analyzing the underlying systemic factors contributing to security incidents.
- Strengths: STAMP provides a holistic perspective on security by considering interactions between system components and organizational processes. It helps uncover latent vulnerabilities and systemic weaknesses that traditional risk assessment methods may overlook.
- Limitations: STAMP requires a deep understanding of systems theory and may be challenging to apply in practice, especially for organizations with limited expertise in systems thinking. It may require substantial resources and time for implementation.

IV. Multi-Criteria Decision Analysis (MCDA)

- Description: MCDA is a decision support methodology that evaluates alternatives based on multiple criteria or objectives. In the context of information security, MCDA can be used to prioritize security investments, select security controls, and allocate resources.
- Strengths MCDA provides a structured approach for considering various factors, such as cost, effectiveness, and regulatory compliance, in security decision-making. It allows stakeholders to compare and evaluate alternatives objectively.
- Limitations: MCDA may require extensive data and expertise to define criteria, weight them appropriately, and assess alternatives accurately. It may also struggle to capture qualitative factors or uncertainties in the decision-making process.

V. Optimization Models for Security Resource Allocation

Description: Optimization models, such as linear programming and integer programming, are used to allocate resources optimally to maximize security effectiveness within resource constraints. These models consider factors such as budget, risk tolerance, and security requirements.

Strengths: Optimization models offer a rigorous approach to resource allocation, identifying the most cost-effective security measures to achieve desired security outcomes. They can accommodate complex constraints and uncertainties.

Limitations: Optimization models may require simplifying assumptions or approximations, which can impact their accuracy and realism. They may also be computationally intensive, requiring specialized software or expertise to implement and solve.

VI. Optimization Models for Security Resource Allocation

In the realm of information security, optimization models are instrumental in allocating resources effectively to maximize security outcomes while operating within constraints such as budgetary limitations and resource availability. Among the various optimization techniques, linear programming, integer programming, and other optimization methodologies play significant roles in addressing resource constraints and enhancing security posture. [1]

Linear Programming (LP): Linear programming is a mathematical technique used to optimize a linear objective function subject to linear equality and inequality constraints. In the context of security resource allocation, LP models can be employed to determine the optimal allocation of resources (e.g., budget, personnel) across different security measures to achieve the highest level of security within predefined constraints.

Integer Programming (IP): Integer programming extends the capabilities of linear programming by allowing decision variables to take integer values, enabling the modeling of discrete decision variables. In security resource allocation, IP models are particularly useful when decisions involve selecting or allocating discrete resources, such as purchasing security tools or deploying security personnel.

Other Optimization Techniques: Beyond LP and IP, other optimization techniques, such as mixed-integer linear programming (MILP), dynamic programming, and metaheuristic algorithms (e.g., genetic algorithms, simulated annealing), can also be applied to security resource allocation problems. These techniques offer flexibility and scalability in modeling complex security scenarios and addressing various types of resource constraints.

VII. Risk Assessment and Management in Information Security

Operations research (OR) offers powerful methodologies for assessing and managing risks in information security. By leveraging decision analysis methods, probabilistic modeling, and simulation techniques, OR facilitates informed decision-making processes that help organizations identify, prioritize, and mitigate security risks effectively. [7]

VIII. Simulation and Results

Case study: Simulation to determine the number of cyber attacks show in Fig. 1.

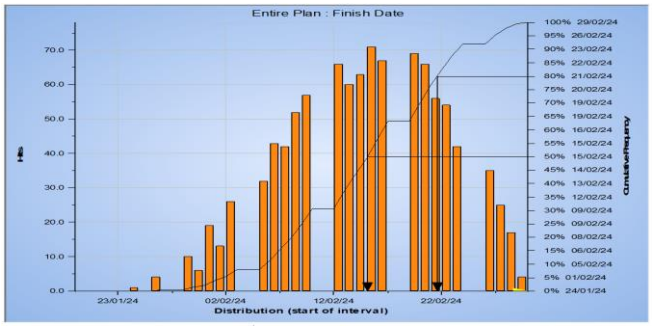

Fig. 1. Cumulative Frequency of Cyber Attack Completion Dates from Primavera Risk Analysis program

After conducting a simulation using Primavera Risk Analysis software to determine the time required for a cyber attacker to penetrate an electronic platform, a Monte Carlo simulation approach was employed shown in Fig. 2.

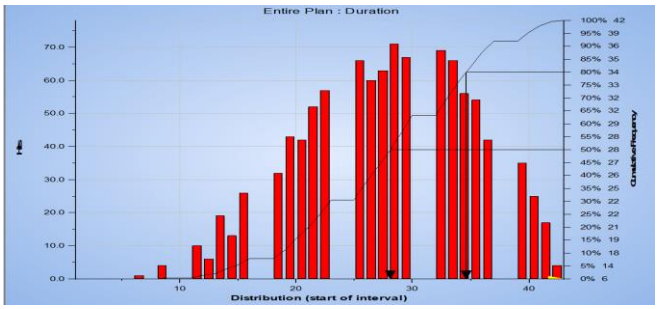

Fig. 2. Distribution of Cyber Attack Durations from Primavera Risk Analysis program

This approach relies on the generation of random numbers. It was assumed that the attacker would require anywhere between 1 to 30 days to successfully breach the website. A total of 1000 simulation runs were executed, revealing that 7% of the attempts might succeed in compromising the site after 11 days, with 79 attempts made. Additionally, 50% of the attempts could be successful after 565 attempts within a 24-day timeframe, while 80% of the attempts might lead to a successful breach after 823 attempts over 30 days. These findings suggest that cybersecurity experts should formulate their strategies based on the 7% success rate, indicating the potential of attackers to compromise the website. After assuming an attack duration ranging from 1 to 30 minutes and conducting 1000 simulation runs, it was revealed that the attack duration spans from 6 to 42 minutes. The average attack duration was found to be 27 minutes, with 50% of the attacks requiring 28 minutes and 80% necessitating 34 minutes to achieve their objectives. This underscores the necessity for shaping security strategy based on the 6-minute timeframe, which proficient hackers may require to compromise any given website for the Fig. 3.

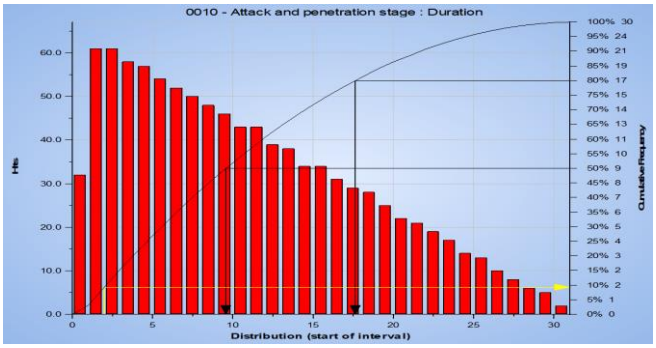

Fig. 3. Distribution of Cyber Attack Durations for Successful Breaches from Primavera Risk Analysis program

Regarding the duration within which an attacker can successfully breach a website, from the initiation of the attack to gaining access to the site, default values were set between 0 and 30 minutes. After conducting a simulation, it was determined that, on average, the attacker requires 10 minutes to breach the website. Specifically, 50% of the attackers may achieve penetration at the 9-minute mark, while 80% may succeed at the 17th minute. Consequently, cybersecurity experts within the organization should implement additional traps and firewalls to prolong the attack duration until it can be halted (Fig. 4).

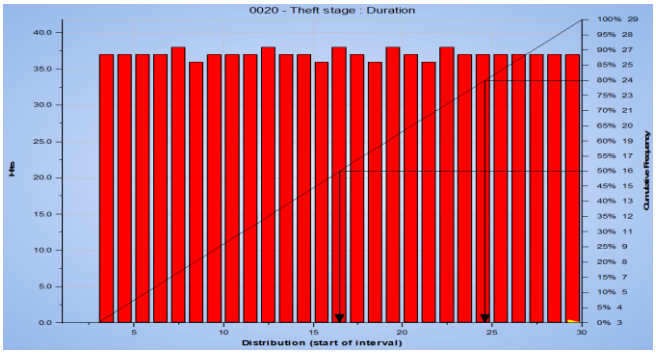

Fig. 4. Probability of Data Theft Initiation by Time After Breach from Primavera Risk Analysis program

In a hypothetical scenario, it is postulated that the attacker initiates data theft three minutes into breaching the website, continuing until the 29th minute, marking the culmination of the assault. Subsequent to the simulation process, the results reveal that 50% of attackers are capable of commencing data pilferage by the sixteenth minute following the breach, while 80% of assailants can commence data theft by the twenty-fourth minute post-intrusion. These findings necessitate cybersecurity experts to implement measures involving data encryption and obfuscation. The objective is to complicate the comprehension of pilfered data by the attacker, consequently delaying replication operations. This strategic delay provides the defending team with sufficient time to successfully conclude the assault (Fig. 5).

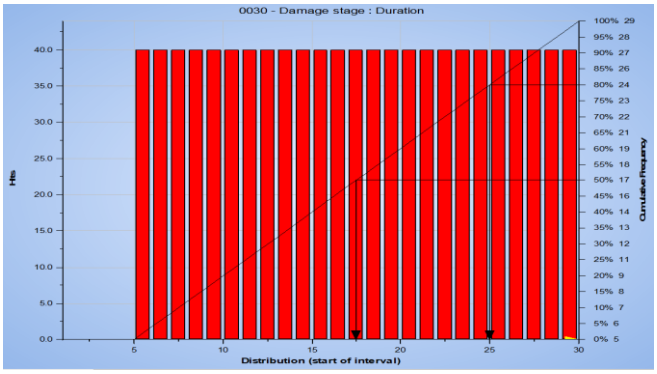

Fig. 5. Probability of Sabotage Initiation by Time after BreachS from Primavera Risk Analysis program.

The determination of a fixed timeframe for the initiation of damage infliction upon an electronic system following its compromise remains elusive, as it hinges upon several variables. These factors encompass the nature of the attack, the objectives of the assailant, the quality of the targeted data, and the assailant's familiarity with the breached system. An assailant may commence executing deleterious actions immediately upon gaining access to a specific system, and immediate impacts may manifest in certain instances. For instance, if the assailant's objective is the rapid disablement of a specific service, they may promptly initiate malicious commands.

In general, ascertaining the extent of damage and the time required to initiate harm to a system constitutes a complex matter contingent upon the attack context, as well as the preparedness and cyber defense capabilities of the targeted entity. However, assuming a hypothetical scenario wherein the duration necessary for executing damage within the system and halting its services commences from the 5th minute of the attack until the termination of the assault at the 29th minute, the outcomes of a simulation conducted through the Primavera Risk Analysis program reveal that 50% of assailants require 17 minutes to commence the sabotage operation and disrupt system services, while 80% necessitate 24 minutes to execute the systematic sabotage operation (Fig. 6).

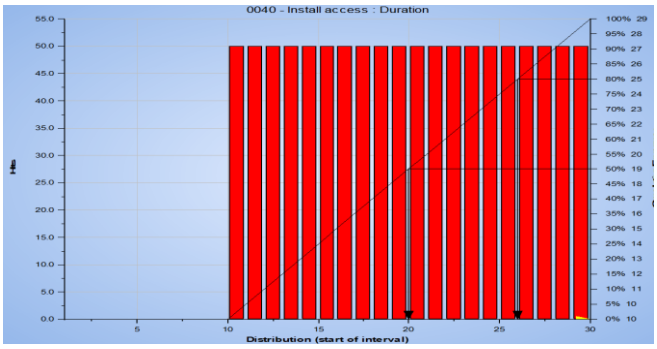

Fig. 6. Distribution of Time to Install Access Points After Breach by Primavera Risk Analysis program

The pursuit of malicious actors and hackers frequently centers on the creation of a point of entry that affords them access to a website, enabling subsequent retrieval and manipulation of data at their discretion. The execution of a simulation process, embedded within the confines of the Primavera Risk Analysis program, reveals discerning insights into this modus operandi. Specifically, the findings illuminate that 50% of assailants initiate the installation of access points by the 19th minute subsequent to the breach, underscoring the temporal nuances of their activities. Furthermore, in parallel, 80% of malevolent actors embark on the establishment of ingress points by the 25th minute, further elucidating the dynamics of their actions in the aftermath of intrusion. This empirical exploration sheds light on the intricacies inherent in the cyber operations orchestrated by different echelons of attackers (Fig. 7).

Fig. 7. Distribution of Cyber Attack Resolution Times

By Primavera Risk Analysis program

The majority of institutions engage cybersecurity firms tasked with repelling electronic attacks and safeguarding digital assets. Despite these measures, hackers continue to exploit technological advancements and leverage their knowledge of website security vulnerabilities, underscoring the persistent susceptibility of digital infrastructures. The element of time assumes a pivotal role in terminating cyber attacks, aiming to mitigate data theft, halt system operations, and forestall the establishment of unauthorized access points. Consequently, a comprehensive exploration involving the execution of 1000 simulation processes through the Primavera Risk Analysis program was undertaken. The primary objective was to ascertain the time required by cybersecurity experts to conclude an attack, presuming that termination could potentially occur anywhere from the initiation (point zero) to the 30th minute of the cyber onslaught. The outcomes indicate that 50% of attacks are successfully terminated by the 15th minute, while 80% are thwarted and concluded by the 24th minute from the onset of the cyber attack. These findings illuminate the critical temporal dynamics involved in cybersecurity operations aimed at mitigating and terminating cyber threats effectively.

Upon conducting a simulation using Primavera Risk Analysis software to determine the temporal requirements for a cyber attacker to infiltrate an electronic platform, the research embraced the Monte Carlo simulation methodology. This approach, relying on the generation of random numbers, models the probabilistic nature of the cyber attack scenario. The study postulated that the successful breach of the website by an attacker could transpire within a temporal window ranging from 1 to 30 days. Through 1000 simulation runs, the outcomes revealed that 7% of attempts could compromise the site after precisely 11 days, with 79 attempts succeeding. Additionally, the study indicated that the median threshold of 50% success could be achieved after 565 attempts, encompassing a 24-day timeframe, while the 80% success rate could manifest after 823 attempts over 30 days. These empirical findings underscore the significance of cybersecurity experts formulating strategies based on the identified 7% success rate, signifying the latent capability of attackers to compromise the security of the targeted website.

After assuming an attack duration ranging from 1 to 30 minutes and conducting 1000 simulation runs, it was revealed that the attack durations spanned from 6 to 42 minutes. The computed average attack duration was

determined to be 27 minutes, with a notable 50% of the simulated attacks necessitating 28 minutes to achieve their objectives. Moreover, 80% of the simulated attacks required a duration of 34 minutes for successful completion. These findings underscore the critical need for shaping security strategies based on the identified 6-minute timeframe, signifying the window within which proficient hackers may potentially compromise the security of any given website. Such insights gleaned from the simulations provide valuable guidance for cybersecurity experts in devising robust and time-sensitive defense mechanisms to fortify electronic platforms against adept adversaries.

In addressing the temporal aspect of an attacker's ability to successfully breach a website, parameters were set within the range of 0 to 30 minutes from the initiation of the attack to gaining access to the site. Following a comprehensive simulation, the average duration for an attacker to breach the website was discerned to be 10 minutes. Specifically, at the 9-minute mark, 50% of simulated attackers achieved successful penetration, while the success rate increased to 80% by the 17th minute. This underscores the exigency for cybersecurity experts within an organization to strategically implement additional defensive measures, such as traps and firewalls. The purpose of such measures is to protract the attack duration, affording the defending team a prolonged timeframe within which they can intervene and successfully halt the intrusion. This strategic approach aligns with the imperative of fortifying digital infrastructures against cyber threats by introducing obstacles that impede swift unauthorized access.

In a theoretical context, the hypothesis posits that an assailant, upon breaching a website, instigates the process of data theft three minutes into the intrusion, persisting until the 29th minute, signifying the culmination of the cyber assault. Post the simulation procedure, the outcomes disclose that 50% of assailants exhibit the capability to initiate data pilferage by the sixteenth minute subsequent to the breach, with the figure escalating to 80% by the twenty-fourth minute post-intrusion. These revelations necessitate cybersecurity experts to institute measures centered on data encryption and obfuscation. The primary objective of these measures is to intricately obfuscate the comprehensibility of pilfered data by the attacker, thereby introducing complexity and delaying replication operations. This strategic delay in the extraction and understanding of sensitive data affords the defending team a more extended temporal window within which they can effectively conclude the cyber assault. Consequently, this strategic approach underscores the critical role of proactive and sophisticated data protection measures in fortifying digital infrastructures against potential breaches, aligning with contemporary cybersecurity imperatives.

The endeavor to establish a fixed timeframe for the initiation of damage infliction upon an electronic system post its compromise proves elusive, contingent upon numerous variables. These variables include the attack's nature, the assailant's objectives, the quality of the targeted data, and the assailant's familiarity with the compromised system. The immediacy of deleterious actions undertaken by an assailant upon gaining access to a specific system varies, with immediate impacts manifesting in specific instances, particularly when the assailant aims for the swift disablement of a particular service, prompting the prompt initiation of malicious commands. In a broader context, the determination of the extent of damage and the time required to initiate harm to a system represents a multifaceted matter reliant on the attack context, as well as the preparedness and cyber defense capabilities of the targeted entity. Nonetheless, hypothetically assuming a scenario where the duration for executing damage within the system and halting its services commences from the 5th minute of the attack until the termination of the assault at the 29th minute, simulation outcomes through the Primavera Risk Analysis program reveal that 50% of assailants require 17 minutes to initiate the sabotage operation and disrupt system services. Furthermore, 80% necessitate 24 minutes to execute the systematic sabotage operation, underscoring the intricate dynamics involved in cyber attacks and their temporal implications on system security and defense measures.

The pursuit of malicious actors and hackers often revolves around the establishment of a point of entry that provides them access to a website, facilitating subsequent retrieval and manipulation of data according to their discretion. The execution of a simulation process, embedded within the framework of the Primavera Risk Analysis program, unveils insightful perspectives into this modus operandi. Specifically, the findings highlight that 50% of assailants commence the installation of access points by the 19th minute following the breach, emphasizing the temporal intricacies of their activities. Additionally, in parallel, 80% of malevolent actors initiate the establishment of ingress points by the 25th minute, further elucidating the dynamics of their actions in the aftermath of intrusion. This empirical exploration illuminates the complexities inherent in the cyber operations orchestrated by different echelons of attackers, providing valuable insights into the temporal aspects of their strategic maneuvers and reinforcing the need for timely and adaptive cybersecurity measures.

The majority of institutions enlist the services of cybersecurity firms dedicated to thwarting electronic attacks and safeguarding digital assets. Despite these precautionary measures, hackers persistently exploit technological advancements and leverage their knowledge of website security vulnerabilities, underscoring the enduring susceptibility of digital infrastructures. The temporal dimension plays a pivotal role in the cessation of cyber attacks, aiming to mitigate data theft, halt system operations, and prevent the establishment of unauthorized access points. In response to this imperative, a comprehensive exploration was undertaken, involving the execution of 1000 simulation processes through the Primavera Risk Analysis program. The primary objective was to ascertain the time required by cybersecurity experts to conclude an attack, presuming that termination could potentially occur anywhere from the initiation (point zero) to the 30th minute of the cyber onslaught. The outcomes of this extensive simulation initiative reveal that 50% of attacks are successfully terminated by the 15th minute, while 80% are thwarted and concluded by the 24th minute from the onset of the cyber attack. These findings shed light on the critical temporal dynamics inherent in cybersecurity operations, emphasizing the need for timely and efficient strategies to mitigate and terminate cyber threats effectively.

REFERENCES

[1] Santucci, Larry. "Quantifying cyber risk in the financial services industry." FRB of Philadelphia Payment Cards Center Discussion Paper 18-3 (2018).

[2] Neghina, Diana-Elena, and Emil Scarlat. "Managing information technology security in the context of cyber crime trends." International journal of computers communications & control 8, no. 1 (2013): 97-104.

[3] Khan, Habib Ullah, Muhammad Zain Malik, Shah Nazir, and Faheem Khan. "Utilizing bio metric system for enhancing cyber security in banking sector: a systematic analysis." IEEE Access (2023).

[4] AlDaajeh, Saleh, Heba Saleous, Saed Alrabaee, Ezedin Barka, Frank Breitinger, and Kim-Kwang Raymond Choo. "The role of national cybersecurity strategies on the improvement of cybersecurity education." Computers & Security 119 (2022): 102754.

[5] Ivanov, Dmitry, Christopher S. Tang, Alexandre Dolgui, Daria Battini, and Ajay Das. "Researchers' perspectives on Industry 4.0: multi-disciplinary analysis and opportunities for operations management." International Journal of Production Research 59, no. 7 (2021): 2055-2078.

[6] Alfonso, G., F. Curti, P. McLemore, and A. Mihov. "Understanding cyber risk: Lessons from a recent Fed workshop." Federal Reserve Bank of New York Liberty Street Economics (2019).

[7] Boot, Arnoud WA, and Anjan V. Thakor. "Financial system architecture." The Review of Financial Studies 10, no. 3 (1997): 693-733.