Decision-making in Ransomware Capability Development: Persona-Driven Simulation

Prem Sagar, Sander Zeijlemaker*, Michael Siegel

* Corresponding author
Cybersecurity at MIT Sloan (CAMS), Sloan School of Management,
Massachusetts Institute of Technology
245 First St., E94-1567, Cambridge, MA 02142
{psagar, szeijl, msiegel}@mit

Abstract
The intricate interdependence observed in supply chains and digital workflows renders every organization vulnerable to cybersecurity threats. In recent years, ransomware (adversarial software that locks down IT systems) has emerged as a significant and impactful threat with specific characteristics, resulting in organizations being caught off guard when dealing with ransomware.
Drawing on grounded and existing system dynamics work, we tailored the cyber risk management simulation to the ransomware threat. Using a persona-driven research approach, we simulated for any chief executive relevant cyber risk management strategies to combat ransomware. Our work identified specific cyber risk management strategies that can mitigate the ransomware threat while maintaining profitability and minimizing cyber risk exposure.

Keywords: cyber risk management, ransomware, personas, simulation, decision-making

1. Introduction
This introduction explains our research motivation, objectives, approach, and contribution.

1.1 Research Motivation

Ransomware attacks have become a significant threat to society and businesses, with a 57x increase in cost impact from 2015 to 2021, reaching $20 billion in 2021 (Freeze, 2021). In May 2017, the WannaCry ransomware spread akin to a digital epidemic, encrypting the files of approximately 250,000 Microsoft Windows users across 150 nations (Katina & Gheorghe 2023). On May 7, 2021, the Colonial Pipeline, an integral American oil pipeline network originating from Houston, Texas, and responsible for transporting gasoline and jet fuel primarily to the Southeastern United States, was forced to halt its operations due to a ransomware incident. Consequently, on May 9, a state of emergency was declared across 17 states. A ransom of 75 Bitcoin, worth $4.4 million at the time, was paid to DarkSide under the supervision of the FBI (Palatty, 2023). Considering the 485% increase in ransomware attacks in 2020, this menace remains a growing concern. Additionally, a discerning observation, corroborated by Kaspersky's

report, identified 60,176 instances of mobile ransomware Trojans, affecting 80,638 users across 150 countries in 2018 (Mobile Malware Evolution 2018, 2019)

The intricate interdependence observed within supply chains and digital workflows renders each organization vulnerable to the cybersecurity vulnerabilities of others. A notable statistic underscores this vulnerability, indicating that 64% of entities that fell victim to a ransomware attack within the past 24 months identified a third-party supply chain compromise as the predominant conduit of initial infection. Moreover, an additional aspect contributing to the lack of preparedness can be attributed to cognitive heuristics characterized by complacency, often manifesting as the erroneous belief in an organization's immunity to cyberattacks. Of the organizations that suffered losses due to ransomware attacks, more than two-thirds (67%) reported combined losses ranging from $1 million to $10 million (USD), while 4% estimated staggering losses ranging from $25 million to $50 million. (Cybereason, 2022)

As our reliance on digital resources grows leading to an increase in the size and value of data, the onus is on the managers to improve their approach to ransomware capability development. Interventions to build such capabilities typically include building cyber defense mechanisms, investing in business continuity resources, purchasing new technology, acquiring talent, and providing training, among other activities.

Research on decision-making dynamics can shed light on the factors that influence CXOs' (any chief executive officer) choices when faced with a ransomware attack. This includes understanding the financial implications of paying the ransom versus investing in recovery efforts. Understanding these dynamics can help organizations make informed decisions about whether to pay the ransom or pursue alternative recovery strategies.
Additionally, research on decision-making dynamics can inform policymaking and law enforcement efforts. Understanding the size and nature of the illicit market for ransom payments can help policymakers make informed decisions on how to address the ransomware threat (Paquet-Clouston et al., 2019). Initiatives such as "No More Ransom!" that provide decryption tools to victims can also limit ransom payments (Paquet-Clouston et al., 2019). The research can lead to the development of more effective decision-making frameworks, better risk management, and improved cybersecurity practices across various industries.

1.2 Research Objective and Approach

The research objectives encompass a multifaceted exploration aimed at enhancing decision-makers' understanding and competencies in the context of ransomware attacks. The first objective is to immerse participants, primarily business managers and decision-makers, in the financial complexities of the ransom payment dilemma. Through simulated scenarios, the research aims to sensitize participants to the pressures of complying with ransom demands while navigating the impact on business continuity. The second objective is to equip participants with the skills to promptly align cyber risk management with organizational imperatives. By exposing participants to scenarios demanding swift risk assessment and iterative decision-making for each year in a 5-year period, the research fosters an appreciation for balancing security measures with business continuity. The third objective examines the efficacy of diverse cybersecurity strategies against ransomware. Participants are encouraged to experiment with preventive and responsive measures, gaining insight into the outcome of each strategy. This exploration fosters critical evaluation of strategy strengths and limitations, equipping participants with a versatile approach to risk mitigation. Finally, the research

aims to unravel the intricate relationship between security strategies, organizational resilience, and performance outcomes. By immersing participants in scenarios where strategies influence operational continuity, and reputation, and have financial implications, the research promotes a comprehensive understanding of the far-reaching effects of decision-making. An experiential approach to cyber risk management is employed to reach these objectives, enabling decision-makers to navigate the evolving ransomware threat landscape with informed and strategic acumen.

The foundational system dynamics model used in this study focuses on decision-making and cognitive biases in cybersecurity capability development, as expounded by (Jalali et al., 2019). This was the basis on which we enhanced and expanded the model, incorporating pertinent components and parameters relevant to ransomware. Notably, while the current research ambit was confined to the development and validation of a simulation game for the assessment of four distinct personas (outlined subsequently), the envisaged utility of this simulation game is as a training tool for executives (CXOs). The game is poised to facilitate their comprehension of the multifaceted repercussions of their strategic decisions within the intricate landscape of ransomware cybersecurity.

Methodologically, the research begins with a comprehensive literature review to explore the various aspects of ransomware, including its impact on businesses, psychological influences, response strategies, and the pivotal role of CXOs. Thereafter, it builds upon the foundational SD model proposed by (Jalali et al., 2019) to integrate ransomware-specific elements. This extended SD model aims to capture the evolving dynamics of CXO decision-making during and after ransomware attacks, including factors like attack propagation, ransom payment decisions, and recovery timelines. By conducting scenario simulations and analyzing their outcomes, this research seeks to provide valuable insights into enhancing decision-making strategies and bolstering organizational resilience against the rising tide of ransomware attacks, ultimately contributing to a more secure digital landscape.

1.3 Research Contributions

Our study contributes significantly to the existing literature by addressing ransomware challenges in businesses through a simulation-based approach. Specifically, our contributions can be summarized as follows:

1. Examination of Decision-Maker Personas in Ransomware Capabilities Development:
Our research takes a comprehensive approach by examining the effects of different decision-maker personas on the development of ransomware capabilities both before and after an attack occurs. This investigation takes into account the uncertainties and delays inherent in building these capabilities. By delving into the decision-making processes of various personas, we offer insights into the complexities of varied resource allocation in prevention, detection, response, and recovery capabilities in the face of ransomware threats. This aspect of our study fills a crucial gap in the literature by shedding light on the behavioral biases and misconceptions that decision-makers may exhibit when building and enhancing cybersecurity measures.

2. Application of System Dynamics Modeling to Ransomware Cybersecurity:
Guided by the systems thinking methodology outlined by (Jalali et al., 2019), our study applies system dynamics modeling to ransomware cybersecurity. Although system dynamics has been harnessed in various spheres of information science and technology (J. Sterman et al., 2012), its application to the intricate complexities of ransomware-

related predicaments, especially in the field of business and management, is still limited. Our simulation game adopts a holistic perspective by considering the problem of investment in ransomware defense and recovery capabilities as an intricate system. Our approach addresses the complexities of decision-making processes in the context of ransomware incidents by incorporating feedback delays related to capability development and consequence identification.

3. Filling a Gap in Decision-Making Biases:
Existing literature has broadly examined cybersecurity investment strategies (e.g., see Bose and (Robert) Luo, 2014; Heitzenrater and Simpson, 2016; Nagurney et al., 2017), including the trade-offs between proactive and reactive approaches (Jalali et al, 2019). However, there is limited research on the biases that individuals exhibit when making decisions about ransomware attacks, especially concerning delays in building recovery capabilities and misconceptions surrounding the time it takes to observe the benefits of defensive and responsive measures. Our research addresses this gap, shedding light on the biases that can influence decision-makers in ransomware cybersecurity.

In summary, our study advances the understanding of decision-making processes in the face of ransomware challenges in businesses. By dissecting decision-maker personas, applying system dynamics modeling, and uncovering biases in investment decisions through personas, our research contributes to both the theoretical and practical aspects of dealing with ransomware incidents. This study extends the boundaries of existing research in cybersecurity and provides insights for practitioners seeking effective strategies to combat ransomware threats.

This paper is structured as follows: We begin with a comprehensive review of the relevant literature and theoretical underpinnings. Subsequently, we outline our research methodology, encompassing the delineation of personas and the design of the simulation game. This is followed by the presentation of our findings, explaining our contributions to both the research domain and the broader literature. We then discuss the limitations of our study and suggest avenues for future research. Finally, we conclude with our synthesized insights and conclusions.

2 Theoretical Background

The field of cyber risk management is considered complex and dynamic, a sentiment that has been echoed in previous research (Eling et al., 2021; Hoppe et al., 2021). This complexity is further exacerbated when dealing with ransomware attacks, which possess specific characteristics such as immediate financial impact, high visibility, emotional urgency, and an immediate threat to business continuity (*Cy-Xplorer - the #1 Cyber Extortion Report*, 2023). These attributes have a significant influence on decision-making processes, especially at the CXO level (*Here's How CEOs Can Improve Organisational Cyber Resilience*, 2022). The effect of these characteristics and dynamics on cyber risk management decisions related to ransomware is immediate and far-reaching. In the following sections, we explore these characteristics, contrasting them with traditional cyberattacks to provide a comprehensive understanding of why ransomware presents a unique challenge for businesses and decision-makers.

2.1 Specific Characteristics of Ransomware

Ransomware, a unique form of cyberattack, is characterized by immediate financial impact, high visibility and emotional urgency, and poses an immediate threat to business continuity (*Cy-Xplorer - the #1 Cyber Extortion Report*, 2023). Ransomware is essentially a medium of digital extortion where your data is encrypted and held hostage until a ransom is paid (Luo and Liao, 2009). Unlike other forms of cyberattacks that may have various aims—stealing data or causing systemic disruptions—ransomware seeks immediate financial gain. The financial consequences of ransomware are immediate and unambiguous: either pay the ransom or lose access to vital data. In 2019, when unidentified hackers infiltrated Baltimore's city servers, effectively sealing off their digital content, the city's online operations came to a standstill for weeks (Sullivan, 2019). The municipal government's email systems were inactive, online transactions for city department payments were unavailable, and real estate dealings were at a standstill because they could not be processed online.

Another element that makes ransomware unique is its high level of visibility and emotional urgency (Laszka et al., 2017). When ransomware strikes, employees and executives are instantly aware of the attack, often leading to a sense of panic due to impaired business operations (Laszka et al., 2017). This emotional atmosphere can make organizations more susceptible to making hurried and ill-advised decisions, such as paying the ransom without adequately exploring alternatives. This state of urgency often conflicts with a company's need for business continuity, as ransomware can disrupt operations within minutes, rendering even the most robust business continuity plans obsolete unless they are explicitly designed to address this unique form of cyber threat. Mitigating and recovering from a ransomware attack is also highly complex. Recovering data after a ransomware attack is difficult without the decryption keys, and even if the ransom is paid, there is no guarantee of data recovery. From a public relations standpoint, ransomware attacks usually necessitate immediate disclosure and can severely damage a company's reputation. In such situations, crisis management and stakeholder management are crucial in limiting exposure (Acquier et al., 2008; Paquet-Clouston et al., 2019).

2.2 Systemic Structures of Managerial Dilemma in Combating Ransomware vs. Cyberattacks

Ransomware and traditional cyberattacks, such as viruses, worms, phishing scams, and DDoS attacks, manifest differently in organizational settings, thereby necessitating distinct managerial approaches. Traditional cyberattacks typically evolve slowly, giving organizations more time, albeit dwindling, to identify and neutralize the threat (Paganini, 2015). Such attacks can be stealthy and persistent, and they do not usually lead to immediate operational disruptions (Singh et al., 2019). Recovery from traditional cyberattacks often involves restoring backups, patching vulnerabilities, and taking other remedial actions. The flexibility in time frames for public disclosure and reputational management also provides decision-makers with more room for long-term strategic planning.

In contrast to traditional cyberattacks, ransomware poses a complex set of ethical and practical dilemmas that demand immediate and multi-faceted decision-making from organizational leaders. For instance, an organization facing a ransomware attack must decide whether to pay the ransom. On one hand, paying the ransom could expedite the recovery process, reducing downtime and the associated financial losses in the short term (Dey and Lahiri, 2021). However, it is important to note that payment does not guarantee complete data recovery. According to a report by Cybereason, only 42% of organizations that reported paying a ransom demand said the payment resulted in the

restoration of all systems and data (Cybereason, 2022). The direct financial impact of paying the ransom could be high as the average ransom in 2023 is $1.54 million (Sophos, 2023). Also, nearly 80% of those who paid were hit by a second attack and close to half the time by the same attackers (Cybereason, 2022; Sgana & Bidar, 2021).

Organizations facing ransomware attacks face a complex paradox that can deeply affect their financial reserves. On one hand, the company experiences a significant revenue shortfall due to disrupted business operations, and on the other, there is a spike in costs as the organization mobilizes resources to counteract the security breach and find alternative means to maintain service and product delivery. This situation places a significant burden on the organization, necessitating intense efforts in crisis management, stakeholder engagement, and strategic communication to navigate through the quandary (Laszka et al., 2017). Setting aside the expenses associated with paying a ransom, organizations have disclosed that the average estimated cost for recovering from ransomware attacks is $1.82 million (Sophos, 2023).

The dilemmas extend beyond the immediate ransom payment to include other layers of complexity. Delays in resolving the ransomware issue can lead to the propagation of the attack across the network, complicating recovery efforts and eroding stakeholder confidence. The characteristics of malicious software enable it to autonomously propagate across various IT assets once it gains a foothold in a given device. This rapid spread is facilitated by seamless and often covert interactions between compromised and yet-to-be-infected IT systems (Zeijlemaker and Siegel, 2023). While measures like anomaly detection and network segmentation can mitigate this spread to some extent, the elusive nature of this risk frequently leads to its underestimation. Consequently, organizations often fail to implement sufficient detection mechanisms and network security measures, which exacerbates the risk of widespread infection (Zeijlemaker and Siegel, 2023).

This is illustrated by the "Petya" ransomware attack on A.P. Moller-Maersk, a leading maritime conglomerate. Maersk was able to contain the malware and reported no data loss (Greenberg 2018). However, the attack significantly disrupted its operational capacities, particularly affecting its container bookings and terminal operations. The firm had to shut down multiple systems to prevent further spread, delaying regular business activities. The downtime had global operational effects on two of its major business units, Maersk Line and APM Terminals, evidenced by their inability to accept new electronic bookings, and by operational disruptions at 17 ports worldwide (The Maritime Executive, 2017). A report by Cybereason revealed that 33% of the organizations surveyed were forced to temporarily suspend business operations (Cybereason, 2022). Quick restoration through backup systems might prove less effective if backups are compromised, a tactic increasingly employed by advanced ransomware actors. A comprehensive, longer-term recovery approach, while more robust, requires significant resource commitments.

Therefore, understanding the nuanced differences between ransomware and traditional cyberattacks is not merely an academic exercise but a practical necessity for decision-makers. This awareness becomes critical for CXOs tasked with cultivating an organizational culture prepared for the diverse challenges presented by the evolving cybersecurity landscape. As we delve into the specifics of ransomware's dynamics and attack-defender characteristics in the subsequent sections, these and other managerial dilemmas will be elaborated upon to provide a more comprehensive understanding of the unique challenges facing modern businesses.

2.3 Behavioral Dimensions: The Role of Biases

Building on the complexities identified in the previous section, it becomes evident that decision-making in the face of ransomware is not merely a function of rational calculations and strategic considerations (Cheng, 2022; Sarter and Schroeder, 2001). With the overwhelming pressure, psychological and behavioral dimensions also come into play, adding another layer of complexity to an already challenging landscape (Cheng, 2022).

CXOs operate under significant pressure, given the time-sensitive nature of ransomware attacks and the high stakes involved (Ahmar, 2023). This heightened stress environment can give rise to a range of cognitive biases that might skew decision-making in unintended ways (Das and Teng, 1999). For example, the "urgency bias" may push decision-makers toward quick, short-term solutions, such as paying the ransom to swiftly regain access to compromised systems (Gagnon and Rochat, 2017). This bias often overshadows long-term considerations like ethical implications or the potential to encourage future cybercrime.

Another pervasive bias is "confirmation bias," where individuals tend to favor information that confirms their existing beliefs (Nickerson, 1998). In the context of ransomware, a CXO may disproportionately weigh advice that aligns with their preconceived notions about the best course of action, possibly disregarding other viable options or strategies. The "sunk cost fallacy" is another bias that can influence decisions, making it difficult to abandon a course of action into which significant resources have already been invested, even when it may no longer be the most advisable strategy (Ariely, 2008).

On a group level, the phenomenon of "groupthink" can also affect decision-making (Turner et al., 1992). The pressure for consensus may lead to premature or poorly considered choices, often discounting outside opinions, or deviating perspectives (Turner et al., 1992). All these biases—be they individual or collective—can profoundly impact the quality of decisions made during a ransomware crisis.

Given this intricate web of psychological pressures and biases, there is a pressing need for more structured and objective decision-making frameworks. This is where simulation-based learning comes into play. By creating a simulated environment that mimics the conditions and pressures of a real ransomware attack, CXOs and their teams can practice decision-making in a less fraught context (J. D. Sterman and Morrison, 1988). This allows for the identification and mitigation of biases, enabling more balanced and reasoned choices when facing an actual ransomware event (Yang et al., 2016). Simulation-based learning thus serves as a powerful tool for honing the behavioral and psychological aspects of decision-making, enhancing the CXO's capacity to navigate the complexities of ransomware attacks more effectively (Jalali et al., 2019).

3. The Ransomware Simulation Training

In the quest to understand and mitigate the complexities of decision-making in cybersecurity, particularly in the realm of ransomware, our current model builds upon the foundational work by Jalali et al. in 2019, which employs a system dynamics approach. This seminal model has already demonstrated its scientific rigor and has been benchmarked against the National Institute of Standards and Technology (NIST) cybersecurity framework (National Institute of Standards and Technology, 2018). In its

original form, the model comprises five capability categories: identify, protect, detect, respond, and recover.

For the sake of manageability in the simulation game format focusing on cybersecurity incidents in general, these capabilities were initially consolidated into three broad categories: prevention capabilities, which combined “identify” and “protect”; detection capabilities; and a bundled category for response/business continuity capabilities, which merged “respond” and “recover.”

However, given the particular characteristics of ransomware attacks—especially their ability to disrupt business operations—it has become increasingly apparent that it is essential to distinguish between response and business continuity capabilities. This separation provides a nuanced understanding that is critical for decision-makers navigating the challenging landscape of ransomware threats. This adaptation along with updated simulation parameters reflects the new goal to address the uncertainties inherent in ransomware and the often-delayed timeline for building comprehensive cybersecurity capabilities. The following sections elaborate on the systemic structures of the existing system dynamics model as well as the three significant changes incorporated in the structure of the simulation model.

3.1 Understanding the Pre-Existing Game Model

As mentioned previously, we leveraged the existing simulation game (Jalali et al., 2019) anchored in a system dynamics model. The Jalali et al. (2019) model consists of three core entities: computer-based information systems, cybersecurity capabilities, and cyber incidents. For simplicity and enhanced gameplay, computer-based information systems are categorized into four generalized groups—ranging from systems with no known vulnerabilities to systems where an attack has been detected.

A unique aspect of the simulation game is its focus on strategic resource allocation. Players are entrusted with the task of dividing their resources among three categories of cybersecurity capabilities: prevention, detection, and response. The decisions made by players in allocating these resources dynamically affect their cybersecurity capabilities. Initial conditions start with all systems in a "not-at-risk" state. However, these can transition to a "systems-at-risk" state if players engage in inadequate security practices. The rate of this transition is calculated through formulae based on players' choices, adding mathematical rigidity to the gameplay.

Another important feature of this simulation is its incorporation of economic variables. Profits serve as the central performance metric, offering an intuitive and tangible way to gauge the effectiveness of cybersecurity investment. Players must navigate a complex landscape where the costs of building cybersecurity capabilities can be easily quantified, but the benefits—often in the form of preventing cyber incidents—are more elusive. This effectively mirrors real-world scenarios where organizational managers find it challenging to value cybersecurity investment in the absence of empirical evidence.

The simulation operates in an interactive online setting, spanning 60 months and encompassing two distinct levels of gameplay. The first level involves deterministic cyberattacks with fixed impacts, allowing players to learn the most effective resource allocation strategies over multiple runs. The second level introduces random attacks, adding a layer of unpredictability that mimics real-world uncertainties.

This cybersecurity simulation game offered us a sound foundation with a harmonious blend of strategic decision-making, economic considerations, and game dynamics. It served as a nuanced pedagogical tool for understanding the intricate trade-offs and decisions involved in cybersecurity investments. With our focus on ransomware, we have updated the system dynamic modeling and the resulting game with updated parameters as elaborated in the next section.

3.2 New Modifications

This section delves into crucial modifications made to our system dynamics model, with a specific focus on three new major components—Business Continuity, the Dilemma of Paying Ransom, and Controlling the Spreading Effect. These upgrades offer nuanced perspectives on ransomware attack mitigation, align the model with empirical data, and introduce layers of complexity that capture the manifold interactions within the ransomware landscape. First, the model now incorporates a "Business Continuity" parameter, crucial for understanding the role of recovery capabilities during and in the aftermath of ransomware attacks. Second, a "Ransom Payment Switch" has been introduced, enabling a more granular analysis of the consequences of paying ransoms. Lastly, the "Spreading Effect" construct has been added to account for the lateral propagation of cyber threats, backed by newly adjusted time-related parameters. Collectively, these enhancements aim to bolster the model's predictive accuracy and practical utility, providing invaluable insights for stakeholders while navigating ransomware attacks.

3.2.1 Introducing Business Continuity

The updated system dynamics model has been fortified with a novel parameter called "Business Continuity," a pivotal element that integrates the domains of business continuity planning and disaster recovery initiatives. In the event of a ransomware attack, organizations frequently face high-level cost expenditures, not only for immediate crisis management but also for the rehabilitation of compromised systems. The detrimental effects of such attacks are not limited to costs; they also plummet revenue levels as business operations come to a grinding halt. Our business continuity parameter aims to quantitatively encapsulate these complexities, providing actionable insights for mitigating both the immediate and prolonged financial and operational impacts of ransomware attacks.

By focusing on both business continuity and disaster recovery, this model parameter serves a dual purpose. It outlines contingency plans aimed at sustaining unhampered business operations and ensuring the seamless provision of products and services, thereby alleviating losses on the revenue front. Simultaneously, it delves into disaster recovery tactics designed to restore functionality with minimized cost outlay. As a result, the business continuity parameter not only aids in immediate response but also contributes to the long-term resilience of an organization's cybersecurity posture (Sophos, 2023).

This refinement in the model is instrumental in enhancing our understanding of the complex interplay between business impact, high-level cost expenditure, and revenue implications. It expands the system dynamics model's capability to incorporate the multi-dimensional aspects of ransomware attacks, serving as an invaluable tool for risk assessment and strategic planning.

3.2.2 Dilemma of Paying Ransom

The updated system dynamics model has an additional component termed the "Ransom Payment Switch." This element embodies the intricate dynamics associated with ransomware payments, encapsulating a financial outlay of $800, with its magnitude proportionally correlated to the extent of system impact—a phenomenon substantiated by the empirical insights outlined in sources such as (Adam, 2021).

This "Ransom Payment Switch" harbors the capacity for discretionary activation, permitting the toggling of ransomware payment instances between an active and inactive status on an annual basis. Upon its activation, a cascade of potential ramifications ensues, intrinsically linked to the act of paying ransoms and previously elaborated in section 2. These consequences encompass a discernible 84% likelihood of the adversary's recurrence. Furthermore, the active status of the switch introduces a substantial 76% probability of complete data recovery following ransom payment, an attribution affirmed by the research findings put forth by Sophos (Adam, 2021).

This complex enhancement to the system dynamics model boosts its ability to analyze ransomware situations. It captures the intricate connections between decisions about paying ransom for ransomware, the chances of those decisions happening, and how they impact the organization's cybersecurity and day-to-day operations.

3.2.3 Controlling the Spreading Effect

In the context of cyber risk assessment, the lifecycle of assets unfolds across four distinct stages, as expounded in scholarly works (Jalali et al., 2019; Sepúlveda Estay, 2023; Zeijlemaker et al., 2022). Firstly, assets categorized as susceptible are subject to compromise by malicious adversaries, thereby transitioning into a state of being “unknown compromised assets.” After detection, these “unknown compromised assets” metamorphose into “known compromised assets.” Following this, defensive measures initiated by the protector attenuate the impact of the cyberattack, effectively rendering these assets as “resolved assets.” Ultimately, these “resolved assets” are reintegrated into the operational milieu as “susceptible assets.” Throughout this sequential progression, the practice of isolation gains paramount importance in curtailing adversarial activities (Zeijlemaker et al., 2022). This strategic isolation proves pivotal due to the propensity of “unknown compromised assets” to propagate compromise to additional “susceptible assets” via mechanisms of lateral movement or propagation associated with automated epidemic ransomware traits, exemplified by the likes of worms.

The revised system dynamics framework has been expanded to encompass a pivotal construct termed the “Spreading Effect.” This component assumes a salient role in the model, accounting for the lateral propagation of infection from compromised assets to vulnerable counterparts. The extent of this propagation is governed by a mathematical model that spans from 0 to 100%, subject to constraints imposed by relevant mitigating measures.

Curbing the spread of this phenomenon is achieved through the implementation of specific strategies, notably network segmentation and anomaly detection. These mechanisms play a decisive role in constricting the lateral transmission of infections across the digital landscape. This strategic integration into the model bolsters its veracity by encapsulating the nuances of how propagation is both influenced and curtailed by operational countermeasures.

Additionally, the time-related aspects within the model have undergone recalibration to better align with evolving contextual considerations. This recalibration is characterized by specific alterations in time parameters. Time 1, which hitherto was set at 10 units, has been revised to 7 units. Similarly, Time 2 has been pruned from 2 units to 1 unit, and Time 3 has been refined from 3 units to 2 units. This recalibration serves to harmonize the time-related dynamics within the model, thus refining its capacity to accurately reflect the time-related aspects of the phenomenon under scrutiny.

3.3 How the Game Works

The game runs online in an interactive environment where players have a decision parameter for each of the four types of capabilities: prevention, detection, response, and business continuity. Players can adjust the value of the parameters representing the percentage of resources to allocate to each capability and when to allocate resources to each capability. Players implement their allocation strategy, advance the simulation for 12 months, monitor changes in profit, and have the option to modify their allocation strategy for the next year and advance another 12 months until 60 months, five trials, have elapsed. Each decision parameter allows the player to invest 0% to 5%, a set range of the typical IT budget, in a specific cybersecurity capability. This is very much similar to the original game as mentioned in section 3.1. However, the current game has only 1 level but incorporates two additional parameters of business continuity resource allocation and a ransom switch, explained in detail in the previous sections.

In the simulation game user interface, the dashboard features a chart designated for "Compromised Systems," which takes into account the spreading effects of ransomware incidents. Concurrently, a financial graph for the organization’s “Profits,” quantified in U.S. dollars, is displayed on the same interface. Both graphical representations are dynamically updated as participants progress through the simulation. Figure 1 provides a visual capture of the simulation game's online interface.

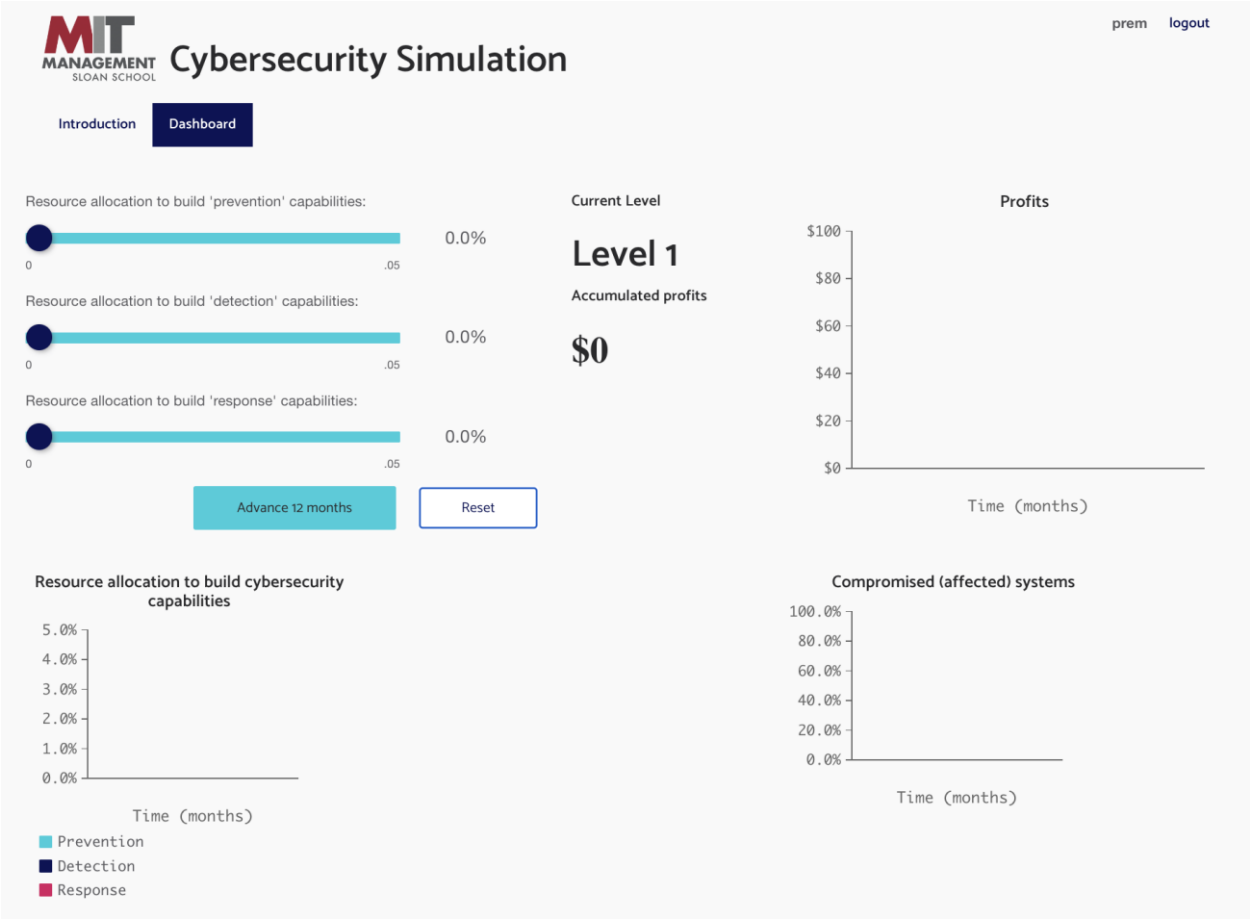


Fig 1. Screengrab of previous user interface (Old game Level 1 [Jalali et al., 2019])

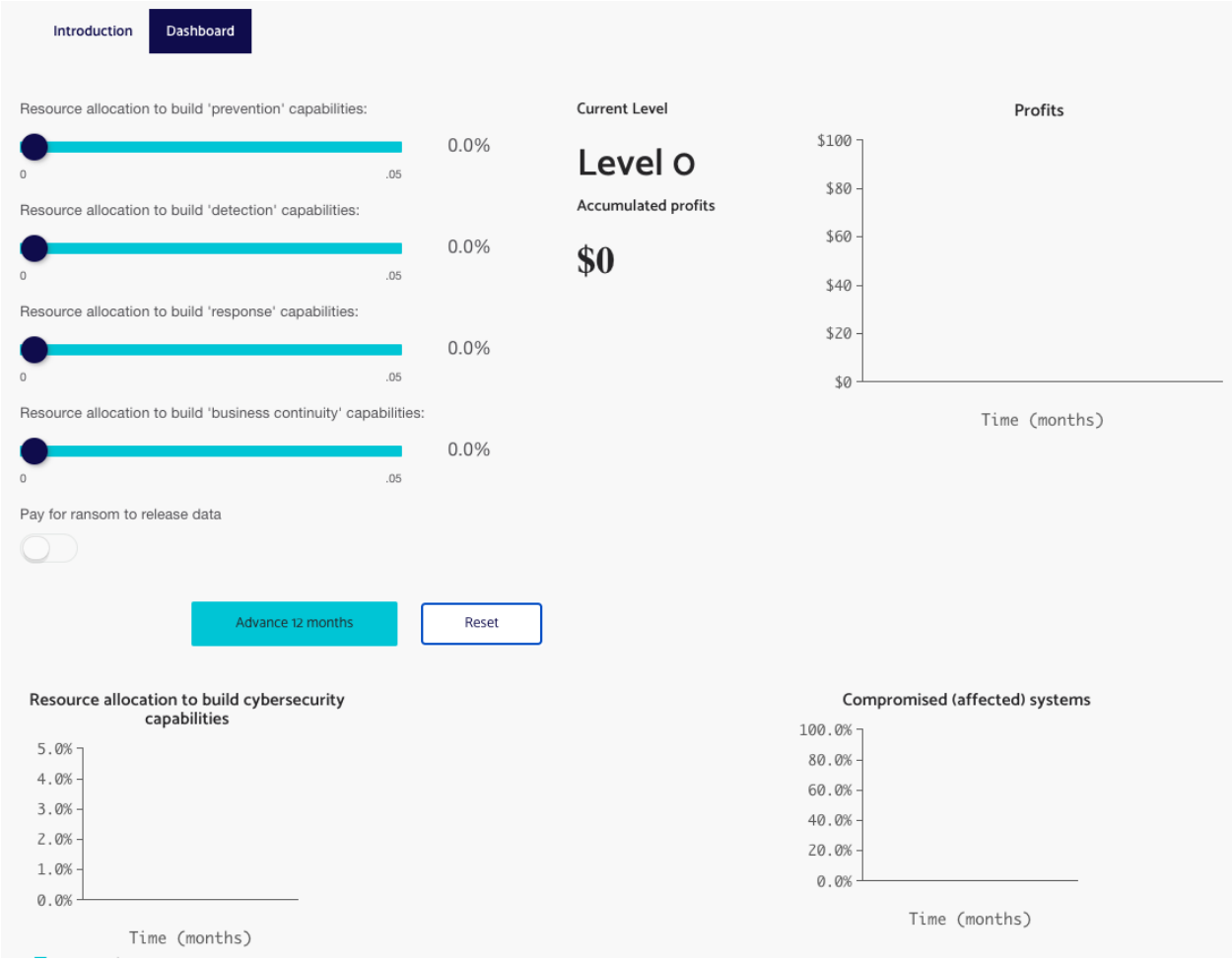


Fig 2. Screengrab of the game's current user interface

4. Persona Creation and Archetypes-Based Simulation

This section delves into the pivotal role of persona-driven strategies in a simulation-based approach for ransomware risk management. Beginning with an exploration of how persona creation and archetypes enhance the learning process in training simulations, the focus then shifts to the application of these persona models in ransomware decision-making among CXOs. Through these lenses, we examine resource allocation strategies tailored to individual strategic inclinations, ultimately presenting a multi-faceted approach to managing cyber risk.

4.1 Persona-Driven Learning Concepts

In the realm of simulation-based training, persona creation and archetypes assume a pivotal role in enhancing learning efficacy and applicability. This elaboration delves into the intricacies of persona creation and archetypal representation within training simulations, elucidating their significance in fostering immersive learning experiences and enabling participants to navigate real-world complexities with a contextualized approach.

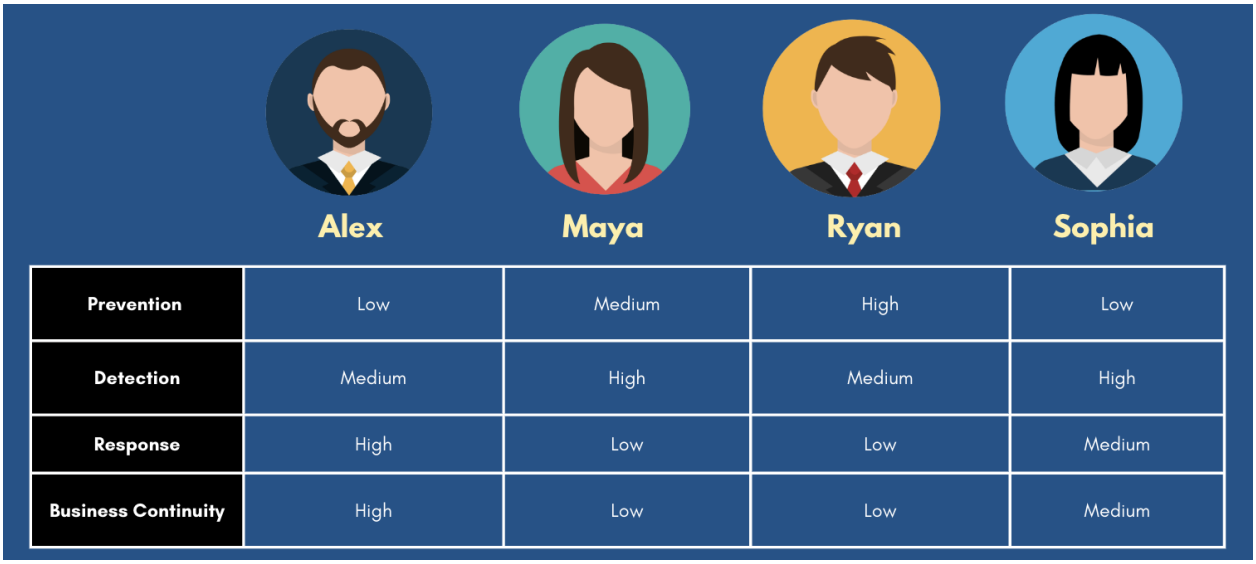
The use of personas in Human Factors Engineering and User Interaction research is justified by the need to prevent biased views that system designers may have of users

(M'manga et al., 2018). Personas are behavioral specifications of archetypical users, providing nuanced representations of their goals and expectations (M'manga et al., 2018). By using personas, system designers can design systems that address the needs and preferences of different user groups.

One of the key justifications for using personas is to facilitate risk-based decision-making. (M'manga et al., 2018) propose an approach for eliciting persona characteristics specifically for risk-based decision-making (M'manga et al., 2018). This approach is based on the Observe Orient Decide Act (OODA) model, which is a decision-making process commonly used in risk management (M'manga et al., 2018). By modeling personas based on decision makers' understanding of risk, the approach enables the design of systems that effectively address risk and uncertainty (M'manga et al., 2018).

4.2 Persona-Centric Cyber Risk Management Strategies

In the landscape of cybersecurity decision-making, a diverse spectrum of personas emerges among CXOs, each embodying distinct strategic approaches to safeguarding their organizations. The following personas encapsulate these distinct archetypes, shedding light on their unique perspectives, priorities, and investment strategies. Here are detailed descriptions of each of the four CXO personas, outlining their resource allocation strategies in terms of prevention, detection, response, and business continuity:



	Alex	Maya	Ryan	Sophia
Prevention	Low	Medium	High	Low
Detection	Medium	High	Medium	High
Response	High	Low	Low	Medium
Business Continuity	High	Low	Low	Medium

Fig 3. Persona mapping with resource allocation choices

1. Alex (Pragmatic Protector):
Alex adopts a strategic approach centered on the establishment of fundamental preventive measures. To this end, Alex directs a "low" level of investment towards prevention strategies, aiming to fortify the organization's defenses against potential cyber threats. Recognizing the importance of early identification, Alex allocates a "medium" level of resources to detection mechanisms, ensuring that any intrusion is promptly spotted. However, where Alex truly excels is in the realm of response and recovery. A "high" investment in response capabilities equips the organization to swiftly counteract any breach and mitigate its impact. Furthermore, by allocating "high" resources to recovery efforts, Alex underscores the importance of post-attack recuperation, fostering operational continuity and reducing downtimes.

2. Maya (Vigilant Warrior):

Maya embodies a data-centric approach, rooted in continuous monitoring and meticulous analysis. Her allocation strategy is characterized by a “medium” investment in prevention strategies, reflecting a recognition of the significance of proactive measures. Notably, Maya places a “high” emphasis on detection mechanisms, underscoring her commitment to staying vigilant and responsive to evolving threats. However, Maya's approach differs in the response and recovery domains. Allocating “low” resources to response underscores her preference for preemptive measures over reactive ones. Similarly, Maya's investment of “low” resources in recovery reflects her prioritization of fortification rather than recuperation.

3. Ryan (Proactive Guardian):
Ryan assumes a proactive stance, channeling the bulk of his investment into preventive strategies. With a “high” allocation towards prevention, Ryan underscores his belief that fortifying the organization's defenses is paramount. While he maintains a “medium” investment in detection capabilities, this balance signifies Ryan's preference for preemptive measures over detection and response. This approach aligns with his conviction that averting attacks altogether is the optimal strategy. In response and recovery, Ryan's emphasis is more restrained, allocating “low” resources to each. This mirrors his perspective that by primarily focusing on prevention, the need for reactive measures can be minimized.

4. Sophia (Agile Detective):
Similarly, to Ryan, Sophia's investment strategy places significant emphasis on prevention as well. Allocating “low” resources to prevention reflects her belief in the importance of building robust defenses. However, Sophia diverges by allocating “high” resources to detection, highlighting her conviction that early identification is crucial. In response and recovery, Sophia strikes a balance by investing “medium” resources in each domain. This signals her recognition of the necessity for responsive measures while concurrently ensuring that business continuity capabilities are aptly bolstered.

These personas collectively illuminate diverse approaches to cybersecurity resource allocation, each uniquely tailored to the individual's strategic inclinations and priorities.

4.3 Experiment methods

The simulation was systematically executed for each distinct persona within the study, encompassing two discrete scenarios that pertained to the persona's decision regarding ransom payment. The parameter governing the ransom payment condition remained constant throughout the simulation time frame. The allocation of resources, categorized into low, medium, and high tiers, was intricately determined in relative terms. As shown in Table 1, the baseline allocation thresholds were initially established as 0.5% for low, 1% for medium, and 2% for high, with corresponding upper bounds of 3%, 4%, and 5% respectively. Over the stipulated five-year duration of the simulation, these values were incrementally adjusted based on relative delta increments, adhering to a systematic progression. This dynamic resource allocation framework was designed to encapsulate varying investment intensities across the simulated personas and scenarios, thus rendering a comprehensive exploration of the decision space.

Resource allocation	Lower-Bound	Upper-Bound
Low	0.5%	3.5%

Medium	1 %	4%
High	2 %	5%

Table 1. Parameter boundaries for resource allocation

For 60 months, each persona was subjected to two distinct scenarios: one in which the ransom was paid, and another where it was not. The decision to either pay or abstain from paying the ransom remained consistent throughout the entire 60-month period for each persona examined.

4.4 Simulation Results

In the following section, we present the findings derived from simulation exercises concerning ransomware attacks, focusing specifically on four distinct personas. These personas serve as representative models to explore various strategic approaches to ransomware incidents. By maintaining a constant decision-making strategy concerning ransom payment over a 60-month simulation period for each persona, we offer a nuanced comparative analysis. This examination aims to illuminate the differential outcomes and implications of the strategies adopted, thereby providing valuable insights into the multifaceted nature of ransomware decision-making.

4.4.1 Alex's Simulation

Fig 4. The output of Alex's resource allocation strategy under conditions of paying and not paying the ransom

The results of this scenario are shown in Figure 4. In the scenario where the ransom was not paid, prioritizing business continuity through robust preventive measures resulted in substantial profits. The organization's resilience, fortified by a comprehensive security framework, facilitated swift containment, and controlled the spread of the attack, expediting recovery. By abstaining from ransom payment, the organization preserved both financial interests and operational integrity, underscoring the benefits of timely recovery.

Conversely, choosing to pay the ransom led to lower profits and cyclic vulnerability. Although this choice temporarily restored operations, recurring attacks eroded profitability and prolonged recovery. Increased spread of the attack contributed to extended recovery timelines, exacerbated by reliance on attackers' promises.

4.4.2 Maya's Simulation

Fig 5. The output of Maya's resource allocation strategy under conditions of paying and not paying the ransom

The results of Maya's resource allocation strategy are shown in Figure 5. In the scenario of not paying the ransom a disruption in business continuity unfolds, with extended recovery timelines. Despite the delayed recovery, indications of improvement are discernible. Low allocation to response and recovery functions results in approximately 90% of systems being compromised.

Conversely, opting to pay the ransom results in suboptimal consequences. A combination of low response and recovery allocation, coupled with ransom payment, fails to generate positive profits. Moreover, significant spread of the attack persists, accompanied by recurring assaults. This scenario highlights the intricate interplay between investment allocation, response dynamics, and the enduring impact of ransom payment on Maya's cybersecurity strategy.

4.4.3 Ryan's Simulation

In the case of not paying the ransom, a strategic blend of prevention and detection initiatives yields swifter profit recovery. Nevertheless, compromised systems remain notably higher, encompassing approximately 60% of the total.

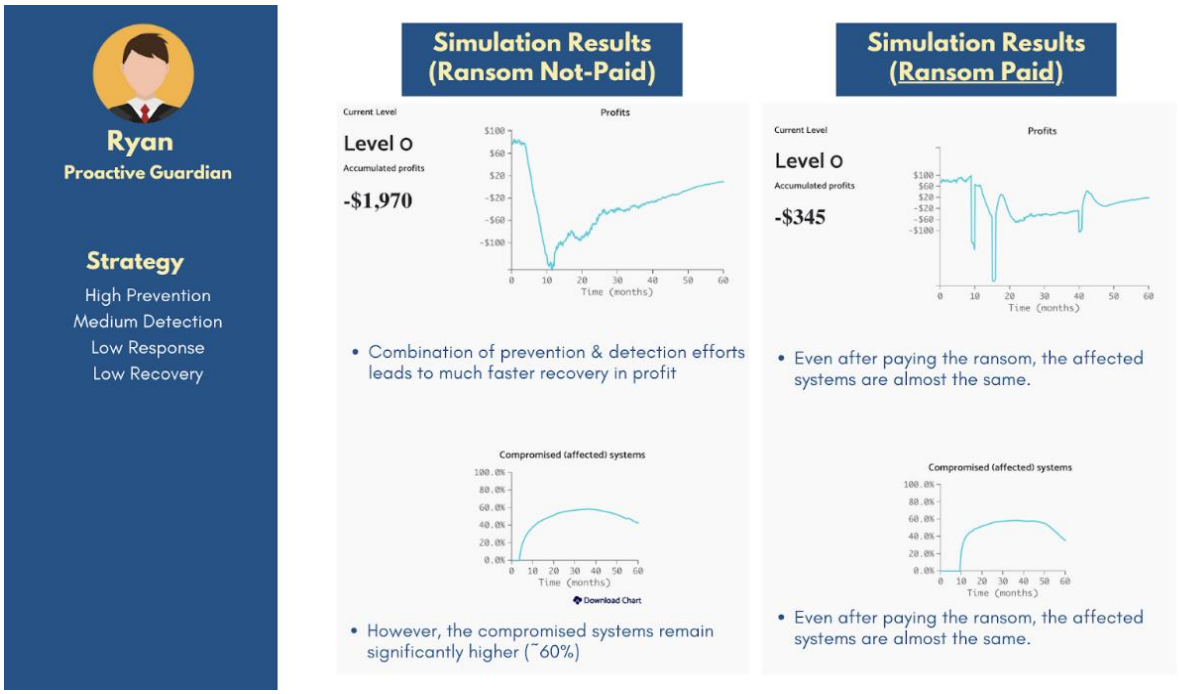


Fig 6. The output of Ryan's resource allocation strategy under conditions of paying and not paying the ransom

Conversely, opting for ransom payment does not alter the scenario significantly. Despite the payment, the impacted systems maintain a similar status. This underscores the minimal influence of ransom payment on mitigating system compromise. These results, which are shown in Figure 6, spotlight the pivotal role of prevention and detection strategies in influencing recovery and system security in Maya's cybersecurity approach.

4.4.4 Sophia's Simulation

The result of Sophia's resource allocation strategy is shown in Figure 7.

Fig 7. The output of Sophia's resource allocation strategy under conditions of paying and not paying the ransom

In the scenario where the ransom was not paid, directing resources towards recovery, coupled with a heightened detection rate, effectively curtails the spread of the attack. This, in turn, drives profit recovery due to controlled impact.

Conversely, in the ransom payment scenario, paying the ransom leads to delayed recovery due to the recurrence of attacks and a limited allocation to prevention measures. This highlights the complex interplay between resource allocation, prevention strategies, and the impact of ransom payment in Sophia's cybersecurity strategy.

4.4.5 Simulation Comparison

In the comparative analysis below, the metrics of profit generated and the spreading effect of the ransomware across the four personas provide illuminating insights into the outcomes of various strategic approaches. This aspect of the study serves to enhance our understanding of how different strategies yield distinct financial and operational impacts, thereby offering a nuanced view of effective ransomware management.

4.4.6 Summary of Findings

Figure 8 shows a summarized overview of all simulation results when the ransom is not paid, and Figure 9 shows the results under the condition of paying the ransom. In conclusion, the research underscores the critical significance of investment in recovery efforts as an indispensable component of tackling ransomware attacks. The findings reveal that even a marginal 1% increase in resource allocation towards recovery efforts can yield substantial advantages. Specifically, this modest increase translates into a remarkable 28% surge in profits in scenarios where the ransom is not paid, and an even more significant 90% increase in profits when the ransom is paid. Conversely, the repercussions of a 1% decrease in resource allocation to recovery efforts are starkly evident, resulting in a staggering 129% reduction in profits for instances where the ransom is withheld, and an alarming 158% plummet in profits when the ransom is met. These results emphasize the importance of recovery investments in shaping the financial outcomes of ransomware incidents.

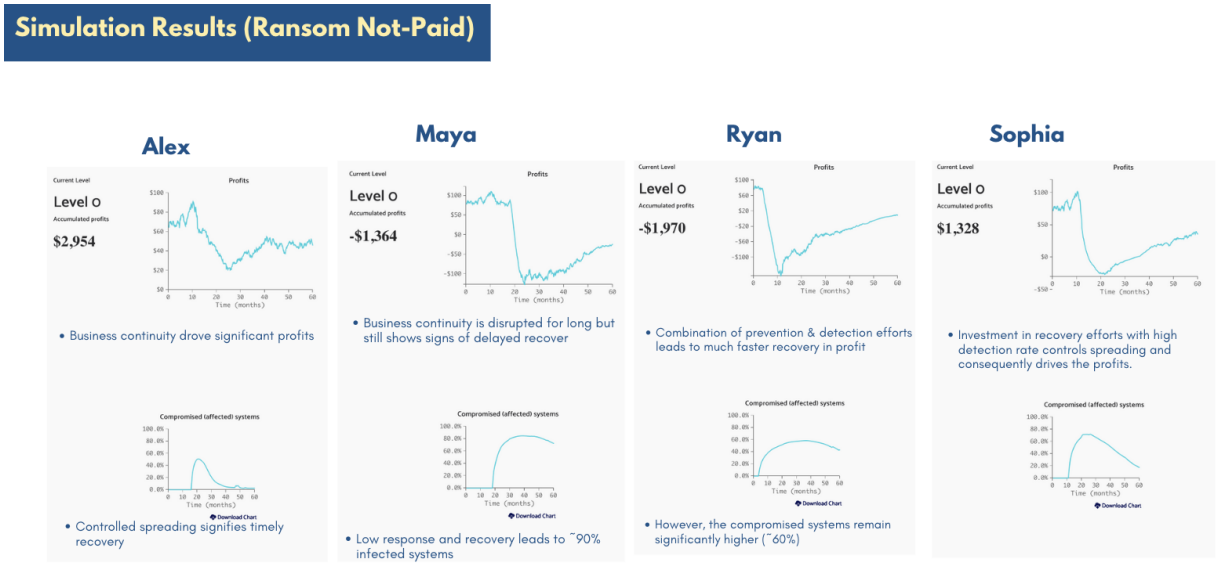


Fig 8. Summarized results under conditions of not paying the ransom.

Furthermore, the act of paying the ransom, although providing a route to short-term recovery, exposes organizations to a cycle of vulnerability. The payment route often incites repeated attacks, necessitating sustained and continued recovery efforts. The research thus highlights the paradoxical nature of ransom payment—a short-term solution that perpetuates long-term vulnerability. Therefore, it is imperative to adopt a proactive stance by strategically balancing investments across all four dimensions: prevention, detection, response, and recovery. Such planning ahead is crucial in cultivating a resilient posture against ransomware attacks. This holistic approach acknowledges the interconnectedness of these facets and emphasizes the importance of orchestrating a harmonized investment strategy to combat ransomware threats effectively.

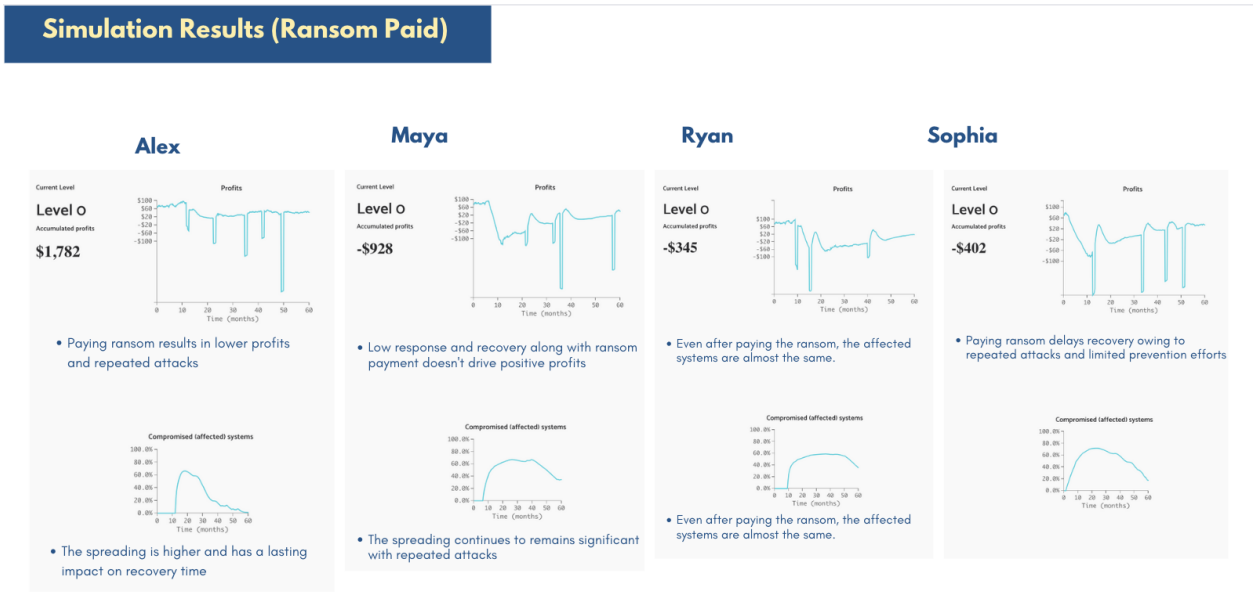


Fig 9. Summarized results under conditions of paying the ransom.

In conclusion, this study provides crucial insights into the evolving landscape of ransomware countermeasures, emphasizing the pivotal role of recovery investments. It underscores the nuanced dynamics of investment decisions, revealing that even marginal shifts can have significant consequences. As organizations face the complex challenges posed by ransomware attacks, this research provides a compass for strategic decision-making—one that steers towards a well-calibrated equilibrium among prevention, detection, response, and recovery efforts. It emphasizes the importance of foresight and a multifaceted approach in fortifying organizations against the escalating threats of ransomware.

5 Discussion and Future Research Opportunities

This research study, while providing valuable insights into the dynamics of decision-making in the context of ransomware attacks, has certain limitations that offer avenues for future research.

One significant constraint lies in the nature of the simulation itself, which is self-run and does not engage real CXOs in the decision-making exercise. The lack of actual business leaders participating in the simulation means that certain behavioral complexities and nuances specific to executive decision-making during cyber incidents may not be fully captured. To obtain richer insights, future research could involve real CXOs, expanding not only the scope but also our understanding of the behavioral aspects at play in these high-stakes situations.

Another area that the current study leaves unexplored is the detailed methodologies by which organizations can build prevention, detection, and response/recovery capabilities. While the need for these capabilities is acknowledged, the study does not provide a comprehensive guide on how to develop them, thereby leaving a gap that future research could aim to fill. Such an endeavor would have practical implications, offering organizations a structured pathway to improve their resilience against cyber threats.

Additionally, the study confines its lens to four specific personas, neglecting the wide variety of roles that populate the business world. The limited scope of these personas restricts the comprehensiveness of the strategic options reviewed and their potential implications. Future research would benefit from incorporating a more diverse array of personas to provide a comprehensive view of decision-making dynamics in ransomware scenarios.

These limitations not only provide context for interpreting the findings of the current study but also pave the way for further research. Addressing these gaps could result in a more holistic understanding of ransomware decision-making dynamics and contribute to the development of more effective strategies for managing cyber risks.

6 Conclusion

In conclusion, this research explores the intricate terrain of decision-making dynamics in the context of ransomware attacks, a subject that is increasingly relevant and urgent in today's business landscape. The study adopted a system dynamics model originally developed by Jalali et al. in 2019, to address the unique challenges and dynamics of ransomware incidents. The study focuses on the characteristics of ransomware attacks that amplify complexity, including the immediacy of financial impact, the direct threat to business continuity, high visibility within and outside the organization, and the emotional urgency generated. Moreover, the study enriches the existing model by introducing three elements crucial to understanding ransomware dynamics: the concept of business continuity, the dilemma associated with the decision to pay or not pay a ransom, and the importance of controlling the spread of the ransomware attack within an organization's network. These additions offer a more nuanced framework for assessing the impact of ransomware, making the study a valuable resource for academia and practitioners alike.

Through the lens of four carefully selected personas, the study offered illuminating comparative analyses, giving particular attention to the long-term consequences of strategic decisions such as whether to pay a ransom or not over a 60-month simulation period.

The study serves as a foundational step, inviting subsequent research to delve into the behavioral aspects, decision-making dynamics, and capability development strategies

tailored to ransomware incidents. Thus, the study lays critical groundwork for developing resilient organizations that can adeptly navigate the precarious cyber threat landscape we face today.

Understanding these dynamics extends beyond academic inquiry to impact the practical world. It is crucial to decipher these complexities in an era where ransomware attacks are becoming more frequent and sophisticated. Subsequent research that addresses the identified limitations and expands on the preliminary insights of this study will be crucial in developing more effective and nuanced risk management strategies in the cyber domain for modern organizations.

Bibliography

Acquier A, Gand S, Szpirglas M. 2008. From stakeholder to stakesholder management in crisis episodes: A case study in a public transportation company. *Journal of Contingencies and Crisis Management* **16**(2): 101–114. https://doi.org/10.1111/j.1468-5973.2008.00538.x

Adam S. 2021. The state of ransomware 2021. *Sophos News*. https://news.sophos.com/en-us/2021/04/27/the-state-of-ransomware-2021/

Ahmar M. 2023. CISOs under pressure: An overview - ET CIO. *ETCIO.Com*. https://cio.economictimes.indiatimes.com/news/strategy-and-management/cisos-under-pressure-an-overview/98377596

Ariely D. 2008. Predictably irrational: The hidden forces that shape our decisions. https://doi.org/10.5860/choice.46-0969

Bose R, (Robert) Luo X. 2014. Investigating security investment impact on firm performance. *International Journal of Accounting & Information Management* **22**(3): 194–208. https://doi.org/10.1108/IJAIM-04-2014-0026

Cheng J. 2022. The social and psychological consequences of ransomware attacks. *ISACA*. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/the-social-and-psychological-consequences-of-ransomware-attacks

Cybereason. 2022. Ransomware the true cost to business 2022. *Report*. https://www.cybereason.com/ransomware-the-true-cost-to-business-2022

Cy-Xplorer—The #1 cyber extortion report. 2023. https://www.orangecyberdefense.com/global/white-papers/cy-xplorer-2023

Das TK, Teng BS. 1999. Cognitive biases and strategic decision processes: An integrative perspective. *Journal of Management Studies* **36**(6): 757–778. https://doi.org/10.1111/1467-6486.00157

Dey D, Lahiri A. 2021. Should we outlaw ransomware payments? http://hdl.handle.net/10125/71414

Eling M, McShane M, Nguyen T. 2021. Cyber risk management: History and future research directions. *Risk Management and Insurance Review* **24**(1): 93–125. https://onlinelibrary.wiley.com/doi/abs/10.1111/rmir.12169

Freeze D. 2021. Global ransomware damage costs predicted to exceed $265 billion by 2031. *Cybercrime Magazine*. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

Gagnon J, Rochat L. 2017. Relationships between hostile attribution bias, negative urgency, and reactive aggression. *Journal of Individual Differences* **38**(4): 211–219. https://doi.org/10.1027/1614-0001/a000238

Greenberg. A. (2018, August 22). The Untold Story of NotPetya, the Most Devastating Cyberattack in History, Wired. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Heitzenrater C, Simpson A. 2016. Software security investment: The right amount of a good thing. *2016 IEEE Cybersecurity Development (SecDev)*, 53–59. https://doi.org/10.1109/SecDev.2016.020

Here's how CEOs can improve organisational cyber resilience. 2022. *World Economic Forum*. https://www.weforum.org/agenda/2022/11/as-cyber-attacks-increase-heres-how-ceos-can-improve-cyber-resilience/

Hoppe F, Gatzert N, Gruner P. 2021. Cyber risk management in SMEs: Insights from industry surveys. *The Journal of Risk Finance* **22**(3/4): 240–260. https://doi.org/10.1108/JRF-02-2020-0024

Jalali MS, Siegel M, Madnick S. 2019. Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. *The Journal of Strategic Information Systems* **28**(1): 66–82. https://doi.org/10.1016/j.jsis.2018.09.003

Katina, P. F., & Gheorghe, A. V. (2023). Blockchain-enabled Resilience: An Integrated Approach for Disaster Supply Chain and Logistics Management. CRC Press.
Laszka A, Farhang S, Grossklags J. 2017. On the economics of ransomware. In Rass S, An B, Kiekintveld C, Fang F, Schauer S. (eds.) *Decision and Game Theory for Security*. Springer International Publishing, 397–417. https://doi.org/10.1007/978-3-319-68711-7_21
Luo X, Liao Q. 2009. Ransomware: A new cyber hijacking threat to enterprises. In *Handbook of Research on Information Security and Assurance*. IGI Global, 1–6. https://doi.org/10.4018/978-1-59904-855-0.ch001
M'manga A, Faily S, McAlaney J, Williams C, Kadobayashi Y, Miyamoto D. 2018. Eliciting persona characteristics for risk-based decision making. https://doi.org/10.14236/ewic/HCI2018.158
Mobile malware evolution. 2018. https://securelist.com/mobile-malware-evolution-2018/89689/ (2019, March 5).
Nagurney A, Daniele P, Shukla S. 2017. A supply chain network game theory model of cybersecurity investments with nonlinear budget constraints. *Annals of Operations Research* **248**(1): 405–427. https://doi.org/10.1007/s10479-016-2209-1
National Institute of Standards and Technology. 2018. *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* (NIST CSWP 04162018; p. NIST CSWP 04162018). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018
NetDilligence. 2022. Cyber claim study 2022. https://netdiligence.com/cyber-claims-study-2022-report/
Nickerson RS. 1998. Confirmation bias: A ubiquitous phenomenon in many guises. *Review of General Psychology* **2**(2): 175–220. https://doi.org/10.1037/1089-2680.2.2.175
Paganini P. 2015. Identity fraud cost US consumers $16 billion in 2014. *Security Affairs*. https://securityaffairs.com/34449/cyber-crime/javelin-study-2015-identity-fraud.html
Palatty, N.J. (2023, February 24). 10 of the Biggest Ransomware Attacks in History, Astra. https://www.getastra.com/blog/security-audit/biggest-ransomware-attacks/
Paquet-Clouston M, Haslhofer B, Dupont B. 2019. Ransomware payments in the Bitcoin ecosystem. *Journal of Cybersecurity* **5**(1): tyz003. https://doi.org/10.1093/cybsec/tyz003
Sarter NB, Schroeder B. 2001. Supporting decision making and action selection under time pressure and uncertainty: The case of in-flight icing. *Human Factors* **43**(4): 573–583. https://doi.org/10.1518/001872001775870403
Sgana, N. & Bidar, M. (2021, June 17). 80% of ransomware victims suffer repeat attacks, according to the new report, CBS news.
Sepúlveda Estay DA. 2023. A system dynamics, epidemiological approach for high-level cyber-resilience to zero-day vulnerabilities. *Journal of Simulation* **17**(1): 1–16. https://doi.org/10.1080/17477778.2021.1890533
Singh S, Sharma PK, Moon SY, Moon D, Park JH. 2019. A comprehensive study on APT attacks and countermeasures for future networks and communications: Challenges and solutions. *The Journal of Supercomputing* **75**(8): 4543–4574. https://doi.org/10.1007/s11227-016-1850-4
Sophos. 2023. 2023 ransomware report: Sophos state of ransomware. *SOPHOS*. https://www.sophos.com/en-us/content/state-of-ransomware
Sterman JD, Morrison B. 1988. *People express management flight simulator*. Sterman.
Sterman J, Fiddaman T, Franck TR, Jones A, McCauley S, Rice P, Sawin E, Siegel L. 2012. Climate interactive: The C-roads climate policy model. *Prof. Sterman via*

Alex Caracuzzo. https://dspace.mit.edu/handle/1721.1/77626
Sullivan E. 2019. Ransomware cyberattacks knock Baltimore's city services offline. *NPR*. https://www.npr.org/2019/05/21/725118702/ransomware-cyberattacks-on-baltimore-put-city-services-offline
The Maritime Executive. 2017. Maersk's cargo operations hit hard by cyberattack. *The Maritime Executive*. https://maritime-executive.com/article/maersks-cargo-operations-hit-hard-by-cyberattack
Turner ME, Pratkanis AR, Probasco P, Leve C. 1992. Threat, cohesion, and group effectiveness: Testing a social identity maintenance perspective on groupthink. *Journal of Personality and Social Psychology* **63**(5): 781–796. https://doi.org/10.1037/0022-3514.63.5.781
Yang MM, Jiang H, Gary MS. 2016. Challenging learning goals improve performance in dynamically complex micro world simulations. *System Dynamics Review* **32**(3–4): 204–232. https://doi.org/10.1002/sdr.1559
Vardham, R & Tonogbanua, L. 2024, Jan 02. How Many Cyber Attacks Happen Per Day in 2024?, Techjury.com.
Zeijlemaker S, Rouwette EAJA, Cunico G, Armenia S, von Kutzschenbach M. 2022. Decision-makers' understanding of cyber-security's systemic and dynamic complexity: Insights from a board game for bank managers. *Systems* **10**(2): Article 2. https://doi.org/10.3390/systems10020049
Zeijlemaker S, Siegel M. 2023. Capturing the dynamic nature of cyber risk: Evidence from an explorative case study. https://hdl.handle.net/10125/103372

Appendix: model changes

The foundational system dynamics model used in this study focuses on decision-making and cognitive biases in cybersecurity capability development, as expounded by (Jalali et al., 2019). In this appendix we explained the model changes that have been made to do our analysis regarding ransomware in terms of parameters and model structure.

Parameters

Model Parameter	Jalali, et al (2019)	Ransomware model	Justification
Time 1 (average time for risk propagation)	10	7	Updated statistics based on average time breach live cycle. Vardham, R & Tonogbanua, L. (2024). Strengthened by NDA covered threat intelligence.
Time 2 (average time to detect system at risk)	2	1	
Time 3 (average response time)	3	2	
Damage factor	1	2	Based on NetDiligence (2022). Cyber claim study 2022 ransomware is more impactful compared to an unspecified cyber event.

Substructures

The model contains the three additional sub-structures:

(1) *Recovery capability*. The accumulation of the investments in the recovery capability follows the same structure as the accumulation of prevention capability in the model. The output of the recovery capability affects the impact of the ransomware attack following Sophos (2023) research.

(2) *Ransom payments*. The option of paying the ransom to the adversary, where paid ransom amount follows NetDiligence (2022) and Sophos (2023), to mitigate the impact has two effects:
   a. Following Sgana & Bidar (2021) and Cybereason (2022) there is a 80% probability the adversary will attack again in the next round on top of the current adversarial attack structure in the model.
   b. Following Cybereason (2022) there is a 60% probability the ransomware payment is not fully effective.

(3) *Epidemic properties of ransomware attacks***.** Ransomware attacks have epidemic properties that allows the malware to spread across technologies (Greenberg 2018; Katina & Gheorghe, 2023). Mimikatz showed that even secure technology assets can be impacted by malware is it is attacked from an compromised asset (Greenberg 2018). These epidemic properties are reflected in the model by an interaction term between compromised systems at one hand and the combines systems at risk and systems not at risk at the other side. This interaction term exponentially increases the growth of compromised systems. These epidemic properties can be limited through significant investments in prevention and detection as it represents the implementation of network segmentation and anomaly detection respectively (Zeijlemaker and Siegel, 2023).