Balancing Risk and Reward in Cybersecurity Investment Decisions

Completed Research Paper

Goeun Kim, Dr. Sander Zeijlemaker, Dr. Jeffrey G. Proudfoot, Dr. Ranjan Pal, Dr. Michael Siegel

Abstract

Cyber risk management continues to be an intractable problem for organizations. Practitioners grapple with understanding the complexities of cyber risk and making investment decisions to minimize it. In this study, we explore this complexity by (1) qualitatively investigating cyber risk management decision-making through interviews with thirty five cybersecurity and strategy experts, and (2) leveraging data from a digital twin technology simulation game designed to extract insights on profits and risks associated with cyber risk investment. Our study identified four significantly distinct investment profiles, each exerting different influences on risk management and financial gain. The most effective investment strategy in prevention, detection, and response shows a differentiating result profile of high financial gains and low risks (in terms of compromised systems), which echoes the principles of the Bowman Paradox. Overall, our findings offer a solution and practical implications to address the investment challenges of cyber risk management.

Keywords

Cyber risk management, simulation, cyber strategy, prevention, detection, response, decision-making, portfolio approach.

Balancing Risk and Reward in Cybersecurity Investment Decisions

Completed Research Paper

1. Introduction

"*We really need to improve the art of cyber risk management and the practice of risk management because it is woefully negligent, and people don't do a particularly good job at it. They lack imagination. Some companies do it well but they're outliers. It's a higher-order skill to think about all of the elements of your business. What things could impact it? How can you mitigate them? How do you think about it? It requires a different cognitive model than I think we generally have and train people for. So, we just don't have the workforce and the leaders who are ready to do that type of thinking*." (Executive VP, Consulting)

The pervasive integration of computer technology into our society has fundamentally reshaped our way of life. Businesses and operations are increasingly reliant on computer technology, from data storage to machine learning. However, despite the implementation of identification methods aimed at safeguarding data, the world is experiencing an alarming surge in cyberattacks (Madnick, 2024). At the current growth rate, the financial impact of cyberattacks is projected to reach approximately $10.5 trillion per year by 2025 (Morgan, 2022).

Confronted by this challenge, cybersecurity investments reached $150 billion in 2021 and continue to grow annually at 12.4% (Aiyer et al., 2022). On average, businesses allocate approximately 10% of their yearly Information Technology (IT) budget to cybersecurity and $2,700 per full-time employee (Bernard et al., 2020). For example, this results in cybersecurity expenses of $300,000 out of a $3 million IT budget (Triumph, 2023). Unfortunately, recent incidents show that these already costly efforts are inadequate. The Clorox case is an example (Barsky, 2023). This global manufacturer and marketer of consumer and professional products invested $500 million in IT and security upgrades because of its inclusion on the 2023 Forbes Most Cyber Secure Companies List. However, the company was impacted by a ransomware attack in August 2023, resulting in significant disruptions to its business and supply chain. The Clorox case raises questions about optimizing investments to reduce cyber risk while enhancing financial performance.

Despite offering systematic methodologies, multiple cybersecurity frameworks, such as Center for Internet Security (CIS) Controls, International Organization for Standardization (ISO) 27000, and International Organization for Standardization (NIST), primarily focus on qualitative standards rather than guiding optimal investment amounts and allocations for effectively mitigating cyberattacks (Disterer, 2013; Gros, 2021; Taherdoost, 2022). These frameworks, per se, provide hundreds of different investment options for prevention, detection, and response measures. In addition, defending organizations need to cope with an uncertain business environment characterized by evolving adversaries, changing organizations (people, processes, technology, and suppliers), emerging incidents, and shifting strategic priorities (Zeijlemaker & Siegel, 2023). These factors make finding an optimal investment strategy for cyber risk management even more challenging, raising questions about whether a substantial investment in cybersecurity guarantees a significantly effective outcome.

This study unravels the conundrum of optimally balancing risk and rewards in cyber risk management investment. First, we establish the backdrop of this problem space by discussing relevant literature and providing a sample of quotes from thirty-five cybersecurity and strategy experts. Next, we use a simulation that leverages digital twin technologies to replicate real-world corporate decision-making environments to analyze the results of mock investment choices (Yan et al., 2022).

Simulation-aided approaches and digital twin technology have been in use for over two decades. The existing literature suggests the tremendous potential associated with the "digital twin" concept, encompassing cost and risk reduction, enhanced efficiency, heightened security, reliability, and resilience, along with support for the decision-making process (VanDerHorn & Mahadevan, 2021).

This technology has previously been used to create a virtual replica of an organization's digital infrastructure, enabling the simulation of cyber threats, vulnerabilities, and investments in security

measures. By employing advanced simulation capabilities, these models effectively replicate real-life scenarios even before their implementation and enable the presentation of comprehensive risk and reward assessments (Armenia et al., 2018; Jalali et al., 2019). In this study, we will use simulations to observe real-life scenarios that reflect the magnitude of various proportions of investments in cybersecurity management on profits and cyberattacks.

In Section 2, we will explore the managerial challenges associated with investing in cyber risk management. In Section 3, we will explain our simulation-aided learning environment using digital twin technology. Section 4 will analyze the investment strategies of seventy-two participants who used the simulation tool to operationalize cyber risk management. In Section 5, we report our findings reflect on the results. Finally, this paper concludes with practical implication, scientific reflections and conclusions.

2. Managerial Challenges in Investing in Cyber Risk Management

This section explores the complex managerial challenges associated with investments in cyber risk management. Section 2.1 helps to unfold the scientific debate surrounding the balance between risk and reward in the investment paradigm. This is achieved by elucidating the intricate decision-making process that organizations face when allocating resources to cybersecurity and striving to balance security and innovation. Next, the discussion extends to the realm of human behavior in decision-making in Section 2.2 by examining the psychological underpinnings that shape individuals' perceptions of and responses to cyber risks and potential rewards. This exploration aims to recognize factors that influence decision-making (e.g., cognitive biases) and acknowledge their profound impact on strategic choices for formulating effective management approaches. Finally, we emphasize the ecological validity of our research in Section 2.3 by including a selection of representative quotes collected from interviews with thirty-five cybersecurity and strategy experts. These experts shared insights on the challenges and complexities of decision-making in cyber risk management.

2.1 Balancing Risk and Reward in the Investment Paradigm

Investigation into the relationship between risk and reward is a fundamental aspect of the investment paradigm (Zou, 2000). Does taking high risks guarantee high profits? Economic scholars have fervently debated this issue, presenting contrasting perspectives on whether companies that achieve greater rewards are indeed undertaking higher risks.

A dichotomy of viewpoints emerges in this academic discourse. Some assert that an inclination toward risk correlates with proportionate gains, suggesting that a braver, risk-taking approach could lead to enhanced profitability (Samuelson, 1977). This perspective aligns with the idea that calculated risks, when managed strategically, can lead to substantial returns. However, an opposing viewpoint contends that there is a negative correlation between risk and reward (Bowman, 1980). This challenges the notion that a cautious, risk-averse approach may be equally or even more effective in achieving favorable outcomes. Even more, low performance seems to be more vulnerable to negative shocks and shows negative risk-return relationships when accounting for this endogeneity (Becerra & Markarian, 2021).

The juxtaposition of these perspectives underscores the need for organizations to critically assess their risk appetite (Gontarek, 2016), recognizing that the relationship between risk and reward is not a one-size-fits-all proposition (Sullivan-Taylor & Branicki, 2011). In the realm of cybersecurity investments, our research aims to address the intricate debate between risk and reward. We seek to investigate whether risk and reward unfold in a positive or negative relationship and offer insightful perspectives for informed decision-making in the dynamic digital landscape. We aim to offer practical guidance on navigating the delicate balance between fortifying defenses against cyber threats and optimizing returns.

Transitioning into Section 2.2 on the behavioral aspects of investing in cyber risk management, the human factor must be recognized as a significant influencer in decision-making processes. This is exemplified by the prevailing risk aversion observed among typical business executives (Samuelson, 1977). Even as we navigate the intricacies of resolving the risk-reward controversy, we must acknowledge that human behavioral tendencies, particularly risk avoidance, play a crucial role in shaping these dynamics (Kissoon, 2021). Understanding and addressing these behavioral aspects becomes paramount to achieving a comprehensive understanding of the risk-reward paradox in cybersecurity investments.

2.2 Behavioral Aspects of Investing in Cyber Risk Management

Human behavioral aspects also play a crucial role in decision-making. Concerning cyber risk in the business arena, leaders confront the complexities of balancing risk and reward, often navigating an intricate landscape marked by pervasive uncertainty (Zeijlemaker et al., 2022). Despite our access to extensive data and analytical tools, the human factor, driven by emotions and cognitive biases, significantly molds the decision-making paths (Größler et al., 2011; Kahneman et al., 1982; Martínez-Moyano et al., 2015; Repenning & Sterman, 2002; Sterman, 1989, 2006; Zeijlemaker et al., 2022). The risk-averse attitude can be explained by prospect theory, which introduces the concept of loss aversion. According to this theory, people are more averse to losses than they are motivated by potential gains (Kahneman & Tversky, 1979). The hesitancy to embrace risks, deeply ingrained in human nature, indicates a formidable obstacle to establishing purely rational decision-making processes.

In understanding human decision making, the dual-process theory adds another layer. It suggests that decision making consists of two processes: one intuitive and automatic (System 1) and the other analytical and deliberate (System 2) (Kahneman, 2011). In the realm of cyber risk management investment, decision-makers could rely on quick, intuitive judgments and mental shortcuts to assess risk levels and make decisions. Yet, they also engage in deeper analytical thinking when weighing the potential costs and benefits of various cybersecurity investments. This interplay between instinctive reactions and thoughtful analysis shapes how decisions are made in the complex landscape of cyber risk management. The landscape itself is already very complex, dealing with multiple interconnected and dynamically changing dimensions that complicate the decision-making process. This complexity includes evolving adversarial behavior, emerging incidents, and changes within organizations in terms of people, processes, technology, suppliers, etc.

As companies strive to find an equilibrium between risk and reward, we must recognize and navigate the human element to accurately capture the decision-making process and achieve optimal results. Simulation-aided approaches can be beneficial as they assist in developing optimal strategies in this complex and dynamic landscape.It is also crucial that they translate system science, control theory, and simulation modeling into a learning experience that captures decision-making behavior in a strategic environment (Jalali et al., 2019; Sterman, 2000; Zeijlemaker et al., 2022).

Many strategic cyber risk challenges have been addressed through simulation-aided and model-based research. Examples include the optimization of a security control portfolio (Zhang & Malabarian, 2021), risk assessments for small-medium business entities (Armenia et al., 2021), security operations (Kannan & Swamidurai, 2019), breach exposure assessment in healthcare (McLeod & Dolezel, 2018), evaluation of security control effectiveness (Fielder et al., 2016), specific capabilities (Nazareth & Choi, 2015), or cyber insurance usage (Mukhopadhyay et al., 2013). Nevertheless, assessing how strategic investment decisions in cyber risk management affect the risk-reward paradigm remains elusive. Our work differentiates from previous work as it considers a strategic perspective and a forward-looking approach to how investment decisions affect risk exposure and financial performance.

2.3 A Qualitative Investigation of the Cyber Risk Management Landscape

To better understand the landscape of cyber risk mitigation and reinforce the themes presented in Sections 2.1 and 2.2, we spoke with cybersecurity and strategy experts. These experts were high-ranking executives and board members representing a variety of industries to ensure the generalizability of their insights. Semi-structured interviews were conducted, during which we engaged with participants to discuss their perceptions of the complexities of cyber risk management. Their responses strongly resonated with the risk-reward and behavioral themes presented in Sections 2.1 and 2.2, respectively.

Specifically, several of our experts made comments evidencing the risk-reward calculus that organizations conduct to determine how investment in cyber risk mitigation coincides with other types of risk and business strategy. A common theme was the need for organizations to determine their holistic risk appetite, considering the interconnectedness of cyber risk with other types of risk. This would enable them to decide how to respond by carrying out their risk-reward calculus to mitigate risks exceeding that appetite. A CISO in the finance industry highlighted the importance of identifying broader organizational risks. They pointed out a problematic tendency where security executives focus solely on cyber risks without considering broader detrimental impacts, including revenue. The CISO stated:

"*So, a CISO can sometimes, you know, have blinders on because they see technology risk. They see IT risk. They see compliance risk. But oftentimes, a CISO may not see revenue risk outside of cybersecurity, and that's where the risk committee comes in. And these are basically folks that, you know, really put up a business lens on a cyber security program and really help guide it in the right direction, so that a CISO doesn't go too far in a certain direction without making sure that it's still aligned well with the business.*" (CISO, Financial Services)

As a second example, a product manager operating in the education sector noted the significance of considering how cyber risks, such as noncompliance and security breaches, will impact the organization. This includes making decisions about resource allocation between security and product development. This expert specifically commented:

"*So, when I think about cybersecurity, I think about it in terms of how it impacts sales. Like, are people asking us for compliance and we don't have it? And then if that's blocking the sale. I also think about it in terms of risk, which is separate from whether it's blocking the sale or not, which is, if we get this deal and then somebody hacks us, our whole company could be finished. So that's an existential risk, potentially. And then I also think about it in terms of resource allocation. So, if I have my engineer spend time working on security or compliance, those engineers can't be working on new features which are also needed to compete in the marketplace, and so I think about it in each of those different ways*." (Product Manager, Education)

Our experts' commentary also emphasized the importance of behavioral aspects (e.g., emotions and cognitive biases) and their effect on investments in cyber risk management. The key behavioral elements that our interviewees reported to us include: (1) a tendency for organizational cybersecurity fatigue to diminish investment prioritization and (2) the effect of the psychological discount rate, which causes an organizational de-emphasis on addressing risks that appears to be minimally present or unlikely to happen in the near term. The following two quotes, stated by a division chief in financial services and a board member in communication, respectively, help to further illustrate these phenomena in more detail:

"*The risk management department was chatting with me saying, hey, can you explain why cybersecurity fell out of the top two risks? And I said, you took it out of the top two risks. I know I didn't take it out. You want me to give you an answer? I'll give you an answer, and actually had to point back to them because I heard that they eyed cybersecurity as a top risk, but then they see very little realization of the risk, so I think they were just getting tired of reporting it*." (Division Chief, Financial Services)

"*One of the things we know is that if you hear about let's say an earthquake somewhere else, you will immediately try to figure out, does this matter to me or not? And if you are in a risky area, it will heighten your preparedness a little bit. But if you have experienced an earthquake, it will really heighten your awareness and preparedness for around 3 years. And then the impact tends to fatigue and expire. There is something called the psychological discount rate, which is basically anything that is more than 3 years out, or 3 years old, tends to get discounted close to zero. And if you think about it, go back 500 years, which is about where our brains are still located. If I go to you and say, if you don't prepare right now, 3 years from now you will not have enough food. Are you going to prepare…really*?" (Board Member, Communications)

Overall, investing in cyber risk management is complicated due to various factors, including risk-reward calculations and inherent behavioral characteristics that may obscure decision-makers from choosing an optimal risk-mitigation strategy. The following methodology section describes a simulation tool we developed to (1) explore how returns on cybersecurity risk mitigation investments can be maximized and (2) disentangle the factors that may prevent a decision-maker from choosing an optimal strategy.

3. Methodology

3.1 Simulation Modeling Background

Simulation modeling is a powerful method for advancing theories and conducting research on intricate behaviors and systems (Harrison et al., 2007). Unlike conventional simulations, digital twin technology operates in a virtual environment while mirroring the real-time state of its physical counterpart (Singh et al., 2021). Our digital twin is rooted in system dynamics, which uses differential equations to track the

changes of tangible variables with their interconnections depicted through feedback loops (Forrester, 2009). The creation of a quantified simulation of a business grounded in system dynamics, highlighting inter-dependencies and feedback points, can be considered a digital twin (Gejo-García, 2022; System Dynamics Society, 2024a, 2024b). Yet, there are other forms of digital twin setups where system dynamics contribute to a larger whole (Jinzhi et al., 2022).

The system dynamics approach was originally developed in the mid-1950s by Jay Forrester at the Massachusetts Institute of Technology. This methodology has evolved into a robust tool for comprehending dynamic systems (Martínez-Moyano & Richardson, 2013; Randers, 2019), with applications in business, engineering, public policy, and the social sciences (Randers, 2019). It provides a powerful tool for analyzing the complex nature of systems, offering a holistic view of how different components within a system influence each other (Cosenz & Noto, 2016). Our work builds on the existing grounded and validated research by Jalali et al. (2019). The following section describes the study we designed using a simulation modeling approach.

3.2 Cyber Risk Management Simulation

In simulation, each participant assumes the role of Chief Executive Officer of a virtual hypothetical company tasked with crafting their unique investment strategy in cyber risk management. Their objective is to achieve the highest possible accumulated profit. The participants navigate a dynamic interface that allows them to adjust their investment range in each category annually, ensuring a nuanced and adaptable approach to risk management. The simulation unfolds over a five-year timeline, providing a realistic projection of the consequences of strategic choices in terms of profits and risks. At regular intervals of 12 months, participants make informed decisions about resource allocation. This is symbolized by moving bars to indicate the proportion of their investment in prevention, detection, and response. These investments range from none (0) to extremely low (0.5) and extremely high (5.0) in five-point increments as a percentage of total IT resources (see Figure 1 for a screenshot of our simulation interface).

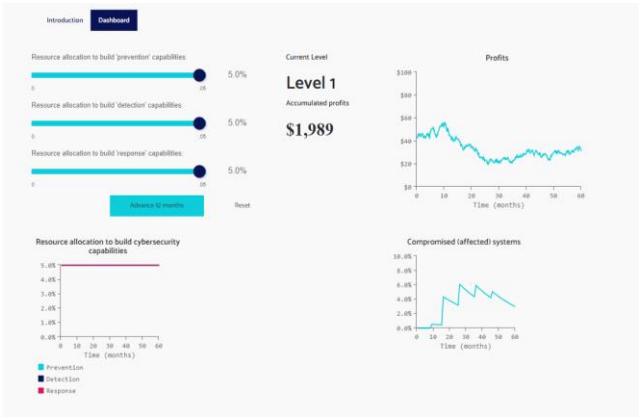

Figure 1. Sample Simulation Page

The core structure of this simulation is that systems that are initially secure may become vulnerable over time, while systems that are already at risk can be compromised by adversaries. When adversarial threats are properly mitigated, compromised systems can be restored to a secure state (Jalali et al., 2019; Sepulveda Estay, 2021; Zeijlemaker, 2022). The amount of investment made in prevention, detection, and response will drive this sequence. Compromised systems, as well as investments in cybersecurity, can affect the profits generated over time.

Recognizing that real-world attack patterns are often unpredictable, we conducted separate but similar simulations—Levels 1 and 2. Thus, each participant took part in two simulations with a noticeable difference. The key distinction between these levels lies in the nature of cyber-attack patterns. In Level 1, the focus is on deterministic attack patterns—well-established, known, and predictable methods. These patterns are consistent and identifiable, enabling security systems to effectively recognize and defend against them. On the other hand, Level 2 mirrors real-life scenarios by dealing with randomly emerging

attack patterns that are dynamic, evolving, and unpredictable. These emerging threats require a more adaptive and proactive security approach, as they may not conform to established patterns.

3.3 Data Collection

We ran a cyber risk management simulation with seventy-two participants who had over five years of management experience. This was a sample of the thousands or executions of this model by a wide range of professionals. Each participant could play the simulation an infinite number of times but was required to share their best results for both Levels 1 and 2. In total, participants played 668 games and shared the seventy-two best exercises with us for Level 1, Level 2, or both. From these shared games, we captured data on annual investments in prevention, detection, and response, as well as the accumulated profit and vulnerable systems after five years. This provided us with a dataset for the Level 1 and 2 simulation results. We plotted the outcomes of different games based on above- and below-average scoring on risk and profitability, as shown in Figure 2.

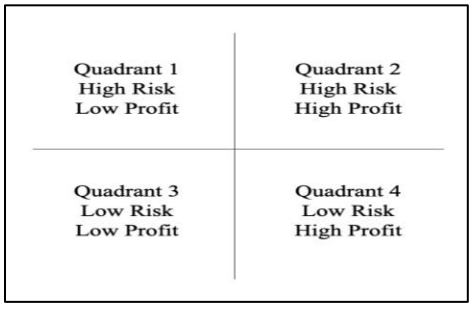

Figure 2. Quadrant Illustration

We used Cronbach's alpha (Collins, 2007) to verify that participants consistently and reliably conveyed their preferences across the diverse dimensions of cyber risk management. As Cronbach's alpha was above 0.78, we were able to compare the results of the Levels 1 and 2 exercises across the different quadrants. We used a t-test to compare the Levels 1 and 2 outputs. The results are shown in Table 1. We observed a significant difference between the accumulated profit and compromised systems at Level 1 and 2 outputs but found no significant difference in total investment in cyber risk management across the different exercises.

t-test	5Y - Accumulated Investments	Systems at Risk After 5Y	5Y - Accumulated Profit
Level 1 Average	40.592	0.092	2,375.78
Level 1 Variance	202.254	0.002	28,476.24
Level 1 Observations	36	35	36
Level 2 Average	38.56	0.17	2,794.39
Level 2 Variance	181.18	0.01	28,049.07
Level 2 Observations	36	35	36

Table 1. T-test Comparing Level 1 with Level 2

In summary, (1) we can compare the different risk and reward outcomes for the Levels 1 and 2 datasets; (2) there is no significant difference in total investments between the Levels 1 and 2 datasets; and (3) equivalent investment strategies can yield different outcomes in terms of risk and performance.

4. Results

In this section, we report our findings from three different types of analysis: (1) quadrant analysis, (2) regression analysis, and (3) Monte Carlo simulation. Details about each are provided in the following subsections.

4.1 Quadrant Analysis

Thanks to the robustness of the Cronbach's alpha test and the t-test, we successfully analyzed our four distinct quadrants, considering the compromised systems and accumulated profits at the final year level.

4.1.1 Quadrant 1: High Risk and Low Profit

The high-risk and low-profit quadrant resembles a situation where inadequate investments in cyber risk management lead to the realization of cyber threats, impacting the organization's risk profile and financial performance. Figure 3 shows the average investment strategy for both Level 1 and 2 exercises. The level 1 exercise was comprised of 26% of participants, while the Level 2 exercise accounted for 6% of them.

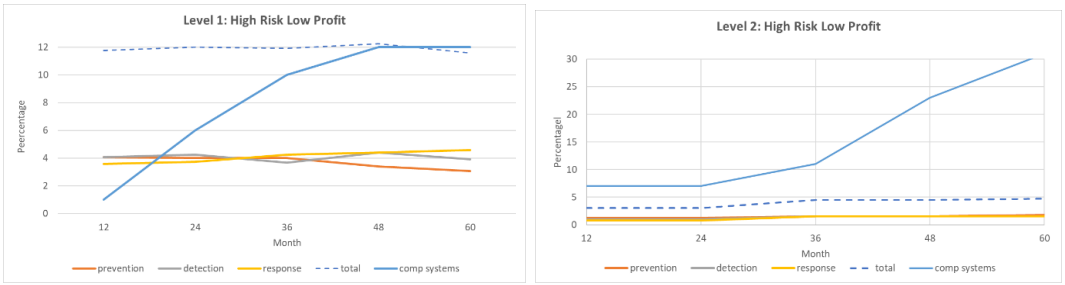

Figure 3. Quadrant 1: High Risk and Low Profit for Levels 1 and 2

In the Level 1 environment, high but inefficient levels of investment allowed the adversary to maintain a foothold, with up to 12% of systems being compromised. Stabilization of compromised system trends occurs only after differentiating investments in prevention, detection, and response. In the Level 2 environment, initial low levels of investment allow the adversary to secretly establish a foothold. Future investments were too limited and too late; therefore, they have a very limited effect on the adversary, as the organization has already been breached. Their foothold extends beyond the 30% threshold of compromised systems.

4.1.2 Quadrant 2: High Risk and High Profit

The high-risk and high-profit quadrant resembles a situation where the adversary is not fully aware of the poor state of the cyber risk management strategy. The adversary has not yet fully exploited this state of underinvestment to its full potential. Figure 4 shows the average investment strategy for both Level 1 (17% of participants) and Level 2 (43% of participants) exercises.

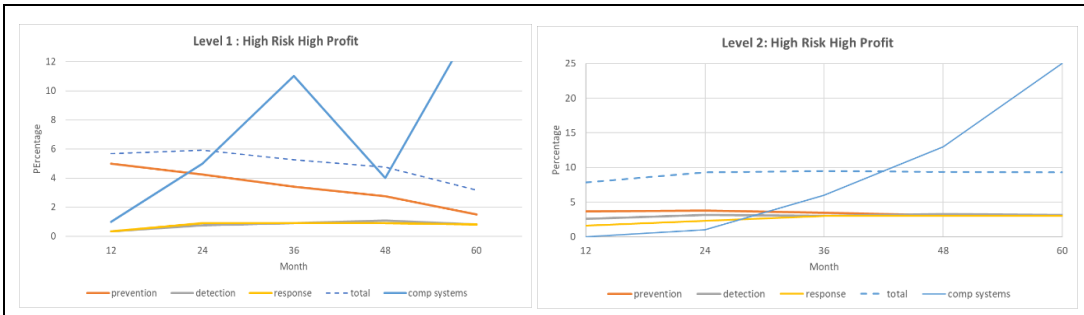

Figure 4. Quadrant 2: High Risk and High Profit for Levels 1 and 2

In the Level 1 environment, the initial investment plans provided a base to limit adversarial behavior over time. Unfortunately, in the last few years, the low investment levels have once again provided adversarial opportunities to exploit more systems—up to 15% of the total. A second observation is that the focus of the cyber risk management strategy is prevention in this situation. In the Level 2 environment, investment levels were not aligned over time with evolving adversarial behavior. This negligence allowed the attacker-defender gap to increase exponentially.

4.1.3 Quadrant 3: Low Risk and Low Profit

The low-risk and low-profit quadrant resembles a situation where excessive investment in cyber risk management limits adversarial behavior at a high cost. Figure 5 shows the average investment strategy for both exercises. Quadrant 3 applies to 17% of Level 1 participants and 37% of Level 2 participants.

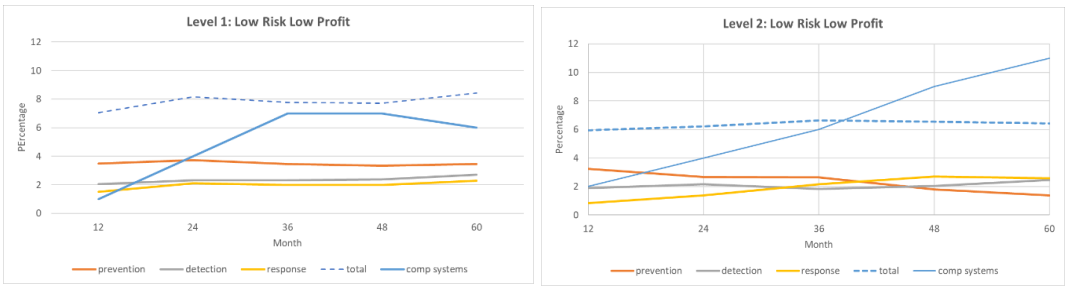

Figure 5. Quadrant 3: Low Risk and Low Profit for Levels 1 and 2

Both Levels 1 and 2 environments show relatively high levels of investment that limit adversarial behavior over time. Where Level 1 shows a decline, Level 2 demonstrates initial signs of stabilization. Additionally, both Levels 1 and 2 exercises mainly indicate varying investment patterns over time in prevention, detection, and response, to a certain extent.

4.1.4 Quadrant 4: Low Risk and High Profit

The low-risk and high-profit quadrant represents a situation where cyber risk management investments are optimized. This is shown in Figure 6. Forty percent of the participants in the Level 1 exercise and 14% of the participants in Level 2 achieved these results.

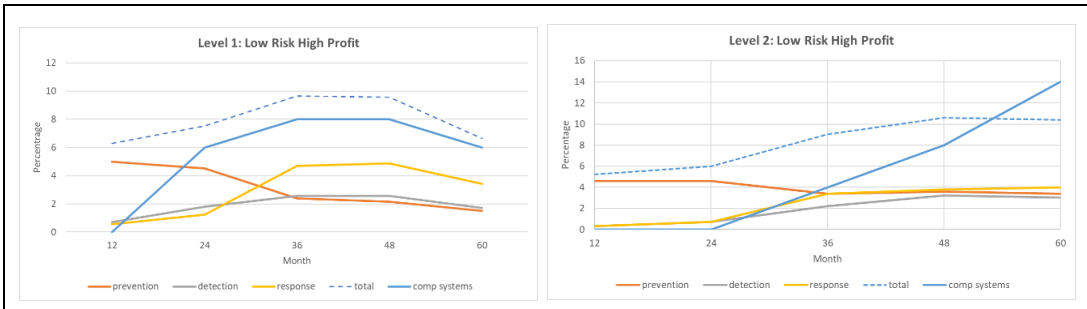

Figure 6. Quadrant 4: Low Risk and High Profit for Levels 1 and 2

Both Levels 1 and 2 exercises show a more tailored approach to investing in prevention, detection, and response over time. Specifically, in the Level 1 exercise, investment levels increase when compromised system levels appear to be still too high and vice versa. For both exercises, the investment levels in prevention decline over time while detection and response efforts increase. Regarding the Level 2 exercise, the levels of compromised systems are lower compared to similar exercises in the other quadrants. In this uncertain environment, there is a longer tail effect that limits the increase in compromised systems. This will take effect in 60 months.

Overall, we observe that 6–10% of the IT budget should be invested in cyber risk management. Our work shows that these investment sizes yield favorable results in terms of risk exposure and financial performance when collected promptly and adequately across prevention, detection, and response measures. This is especially evident in the low-risk and high-profit quadrant. More importantly, building security capabilities takes time. This emphasizes the importance of tailoring allocation over time among prevention, detection, and response.

Another observation is that increasing uncertainty drives decision-makers to a space where they take either too much risk or avoid too much risk, as shown in Table 2. This is evident because most participants shift to Quadrant 2 and Quadrant 3, respectively, when comparing Level 1 and Level 2 exercises.

	Quadrant	1	2	3	4	
	Risk	High	High	Low	low	
	Profit	Low	High	Low	high	
Level	Adversary					Total
1	Deterministic	26%	17%	17%	40%	100%
2	Emergent	6%	37%	43%	14%	100%
	Delta	**-20%**	**20%**	**26%**	**-26%**	0%

Table 2. Comparison of Participants Per Quadrant Between Levels 1 and 2

4.2 Regression Analysis

In our research, we employed regression analysis as a robust statistical tool to assess the intricate relationships in the domain of cyber risk management. Specifically, we sought to estimate the connections between a dependent variable, namely cyber risk management investments, and an independent variable, the ability to generate profit. See Figure 7 for the regression model and the corresponding formula.

$$a = B_0 + B_1(pc) - B_2(pdr) + B_3(r) + e$$

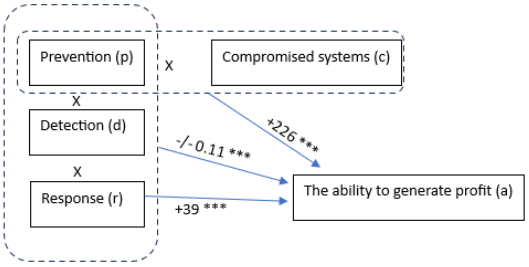

Figure 7. Regression Model and Formula

We found the following results: F-statistic: 13,681, p-value: 4.4E-07, and adjusted R-squared: 0.3488. There is no significant relationship between the error term and the ability to generate profit (r = 0.78).

Our regression model suggests that the ability to generate profit is (1) lowered by any investments in cyber risk management while recognizing the interdependence between prevention, detection, and response capabilities; (2) increased by investments in prevention capabilities that enable the lowering of the number of compromised systems; and (3) enhanced by any investment in response capabilities. This regression model indicates that there are limitations to the role of prevention as well as to the overall investment. It also advocates a societal emphasis on promoting resilience over protection (Annarelli et al., 2020; Bonime-Blanc & Saban, 2022; Dupont, 2019), given the role of response in the regression model. Nevertheless, it is essential to invest in different capabilities, including prevention, detection, and response. This aligns with our findings, where the best-performing participants (high-profit and low-risk) are in Levels 1 and 2. Both the regression model and quadrant analysis highlight that the optimal approach initially involves prioritizing high investments in prevention and lower investments in detection and response. Over time, this strategy transitions to one with increased investments in detection and response and decreased investments in prevention.

4.3 Monte Carlo Simulation

To explore the robustness of our results, we performed a sensitivity analysis. We applied a uniform distribution in a Monte Carlo simulation with 10,000 iterations to model the observed investment strategy for each quadrant in Level 1 outcomes. We only focus on Level 1 outcomes because the sensitivity analysis regarding emerging adversarial behavior incorporates the Level 2 gaming option. We used a uniform distribution because we wanted to generate random numbers within predefined boundaries, and we did not find any evidence to justify using a different distribution. We performed this analysis ceteris paribus in four areas:

(1) How does a change in management or management bias affect the outcome? This assumes that the observed investment strategy will (i) allow for up to a 1% increase or decrease in investment in prevention, detection, and/or response and (ii) these decisions can be made up to three months earlier or later.

(2) How does emerging adversarial behavior affect the outcome? This assumes random attack patterns are launched with varying attack strengths and timing. This is a more advanced analysis, comparable to the Level 2 exercise.

(3) How does the size of the organization affect the outcome? This assumes that organization size varies between 50% less and 200% more in terms of employees and/or systems.

(4) How do economic conditions affect the outcome? This assumes that there are changes in the volatility of the economy as well as the duration and strength of periods of crisis and prosperity.

Figure 8 shows the results of our Monte Carlo simulation. In any situation, we show both the output for compromised systems followed by the profit over time. The sensitivity analysis, as depicted in Figure 8, uses different colors (yellow (50%), green (75%), blue (95%), and gray (100%) coverage of all possible results) to illustrate the distribution of potential outcomes.

The sensitivity analysis shows, in general, that our simulation insights are robust. Specifically, it reveals that adversarial threat behavior and managerial decisions on how to mitigate such threats significantly impact the financial performance and risk exposure of the organization. The following section discusses these results in more detail.

The absence of adversarial behavior only demonstrates the potential for improved financial performance in organizations that yield high profits (Quadrants 2 and 4), where the level of risk taken by the organization affects the extent of this potential growth. The disparity in the upward potential is indicated by the blue area in the high-risk and high-profit quadrant. These insights are in line with expectations. In Quadrant 2, the high-risk profile suggests fewer investments in security capabilities, which makes the impact of adversarial behavior an important driver of accumulated profits. In Quadrant 4, the low-risk and high-profit profile suggests a solid base where security investments are balanced compared to adversarial behavior, enabling upward potential.

The size of the organization benefits most in terms of risk and financial performance from a low-risk and high-profit investment strategy in cyber risk management (Quadrant 4). This is the only quadrant where (i) the accumulated profit curve shows exponential growth and (ii) has the highest level. A cyber risk management strategy associated with low profit and low risk (Quadrant 3) may elevate the organization's risk exposure beyond management expectations. In some scenarios, marked by the blue and gray areas, the adversary may compromise a significant number of systems. We believe these insights are intuitive for Quadrant 4. The exponential growth of accumulated profit in Quadrant 4 suggests that the balance between prevention, detection, and response is optimal compared to adversarial behavior. Additionally, as the organization grows, the relative size of these cybersecurity investments compared to IT assets is decreasing over time. For Quadrant 3, the results are counterintuitive. The increasing risk exposure suggests that lateral movement across the technology stack by adversaries becomes more likely as the organization expands. The analysis shows that there are certain tipping points where detection and response capabilities are essential for organizations of a certain size to minimize risk exposure.

Quadrant 1	Quadrant 2	Quadrant 3	Quadrant 4
High risk	High risk	Low risk	Low risk
Low profit	High profit	Low profit	High profit

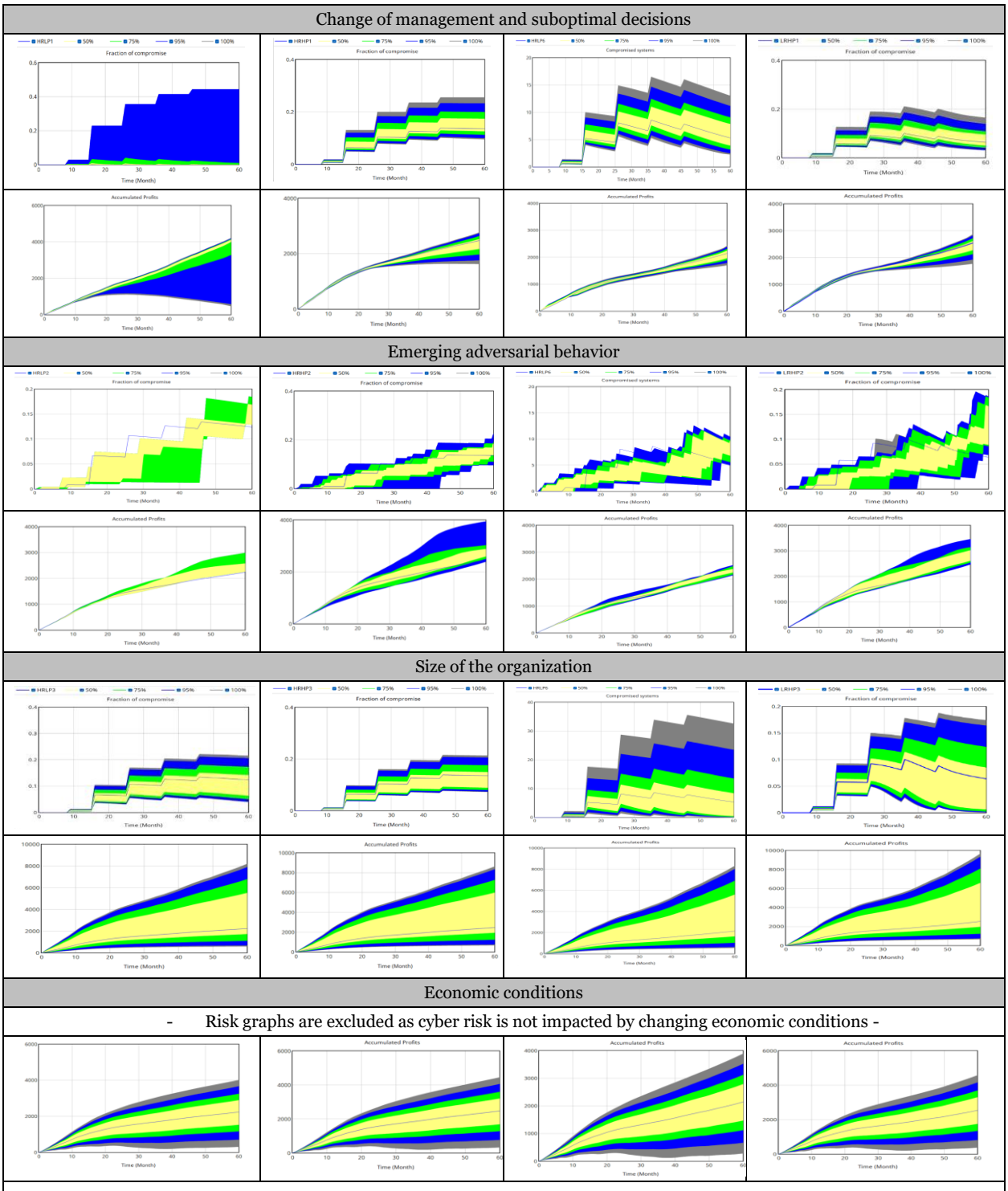

Figure 8. Monte Carlo Simulation

In the case of management bias and changes in management, the risk and performance outcomes tend to balance around the original quadrant output, except for the low-profit and high-risk quadrants (Quadrant 1). In the scenarios depicted by the blue area, adversaries can compromise a significant number of systems, leading to a critical impact on financial performance. Nonlinearities and tipping points exist due to inertia and the complex network of causal relationships within the system. Under certain conditions, they can cause a state of collapse, also known as the capability trap (Repenning & Sterman, 2002). This outcome is

counterintuitive because Quadrant 1 only represents a scenario where there is a collapse in security capabilities, with a significantly high percentage of compromised systems and low accumulated profit levels.

5. Discussion

Our simulation results offer valuable insights for both research and practice on the potential impact of various cyber risk management strategies on a firm's financial performance and overall risk exposure. Our work makes an important contribution to the existing literature in this problem area by demonstrating the existence of a continuous spectrum where strong cyber risk management strategies can transition into weak ones and vice versa. This transition affects the risk profile and financial performance of the firm over time. This continuous space can be explained by the complex and dynamic nature of the underlying system. We also observed that when uncertainty increases, decision makers tend to both overinvest and accept higher risks, which allows the firm to move into a more unfavorable space in terms of risk exposure and financial performance. This indicates that the timing, size, and allocation of investments across prevention, detection, and response have a greater impact, both positively and negatively, as uncertainty increases.

Additionally, economic conditions have a significant impact on the financial performance of the organization, regardless of its cyber risk management strategy. They have no impact on the risk exposure of the firm. We believe these insights align with expectations, as cyber risk management aims to limit adversarial behavior to drive business performance. This is independent of economic conditions.

Overall, the timing and selection of categories are of critical importance in strategic investments to achieve the most effective outcomes for cybersecurity risk management. We observed significant differences in risk and profit levels, even though the related cyber risk investments are similar. Approximately 8% of IT expenses[1] invested in cyber risk management seems optimal. However, the outcome can vary between low-risk exposure and high financial performance or high-risk exposure and low financial performance, depending on the timing and budget allocation. Through regression analysis, we noted that risk and profits are driven by investments in prevention, detection, and response. The timing and size of each individual component, as well as their combined total, are critical factors. Within the four different quadrants portraying various levels of risk and profit, we observed through sensitivity analysis that conditions such as management bias, management change, adversarial behavior, company size, and economic conditions affect risk and profit levels differently. This depends on the underlying investment strategy in cyber risk management.

Our findings identified strategies that achieve high profits with low risk. This underscores the importance of proactive prevention in mitigating the risks posed by adversarial behavior. However, there is a reduction in prevention investments in later years. In response to this, the most efficient strategies allocate more resources toward detection and response in later years. This balanced approach ensures that the total investment remains within reasonable bounds while effectively controlling risks over the next five years. Finally, only this low risk and high profit quadrant can foster upward potential or even exponential growth under certain conditions of economic growth, adversarial behavior, organization size, and management behavior.

6. Recommendations for Solving Investment Challenges

Our work allows the enhancement of investment decision-making in the following manner:

- It is essential to understand the business, operational, and financial consequences of materialized cyber threats. Our research shows that when it comes to managing cyber risks, risk exposure and financial performance behave differently. Especially when management compares investments in cyber risk management with other strategic options and opportunities within the firm, financial insights can provide a common, understandable denominator that helps prioritize. Our research connected risk exposure with financial performance and investments. This advocates for the use of cyber quantification techniques to manage investments in cyber risk management.

[1] In practice, the IT budget can vary depending on the year, sector, and size of the organization. The security budget as a percentage of the total IT budget can range between 7.2% and 19.4% (Irei, 2023).

- Frequently re-access your cyber risk management strategy. Although we were able to identify four different investment profiles and an optimal amount to invest, sensitivity analysis shows that there is a continuous spectrum where strong cyber risk management strategies can become weak and vice versa. Moving across this space is highly affected by uncertainty, including adversarial behavior, management bias, organizational change, and economic conditions, which in turn affect the risk profile and financial performance of the firm over time. This means that seemingly optimal cyber risk management strategies can evolve interchangeably in situations with low-risk exposure and high financial performance or high-risk exposure and low financial performance. Our results show that timely (re-)sizing and (re-)allocating investments in prevention, detection, and response by management are critically important in this space.
- A proactive approach to cyber risk management is essential. Business simulations can be beneficial. The complex cyber risk management landscape consists of many hard-to-observe nonlinearities and often hides tipping points due to inertia and many causal relationships in the system. Our research revealed, through sensitivity analysis, that under specific conditions, a state of collapse of the cyber risk management strategy and very high financial performance are both possible. Here, simulation-aided approaches can help. Unlike the real world, where a bad choice may cause a business to fail, simulations allow managers to test how their cyber risk management strategy decisions evolve in real life (Armenia et al., 2018; Jalali et al., 2019). In our research, the simulation solution considered a future period of five years.

7. Future Research

Future research can enhance our model by incorporating elements that specifically address the challenges posed by AI-powered attacks. Cybercriminals are increasingly leveraging AI techniques to navigate cyberspace, causing more significant damage while remaining undetected. Traditional cyber defense infrastructures are becoming inadequate in light of the escalating speed and intricate decision logic employed by AI-driven attacks (Thanh & Zelinka, 2019). AI-powered cyberattacks encompass a wide range of sophisticated techniques. Recent studies highlight that AI attacks can occur at all stages, with a predominant demonstration in the access and penetration phases (Guembe et al., 2022). For instance, one prevalent attack is adversarial machine learning, where attackers manipulate AI algorithms to deceive systems into misclassifying data or making erroneous decisions. These attacks may be image-based, text-based, or malware-based, subverting system controls over inputs and disrupting identification systems in different ways (Anthi et al., 2021). These threats can easily manipulate medical images to falsely identify cancer and generate deceptive traffic signals aimed at influencing the safety of autonomous vehicles (Yamin et al., 2021). Given the broad scope of the impact of these attacks, it is useful to include AI-powered cybersecurity infrastructures in our model to effectively counter emerging threats. Following the attacker-defender interaction principles, equivalent ideas can be suggested from the defender's perspective.

The integration of supplier dependencies into cybersecurity model structures could also enhance organizational resilience and risk management strategies. This approach entails expanding the scope of analysis to encompass the intricate relationships with third-party logistics and service providers (Leuschner et al., 2014). Since its emergence in the 1980s, the notion of third-party logistics has become a dominant method for storing goods and information in modern supply chains (Leuschner et al., 2014). Recent research involving surveys of over 2,000 industry executives discovered that more than 54% of shippers' transportation expenses and 39% of their expenditure on warehouse operations were outsourced (Langley, 2012). Considering this, integrating supplier dependencies into our model could enhance our understanding of the potential risks and vulnerabilities stemming from a deeper comprehension of the supply chain. This integration can create more detailed risk profiles and lead to robust security measures.

Software-as-a-service providers are an example of supplier dependencies (Sun et al., 2007). By utilizing an external cloud platform, they could intricately influence our model's structure, introducing complexity (Bhardwaj et al., 2010). Mitigating these dependencies could entail evaluating risks across all levels of the supply chain, devising contingency strategies for supplier shortcomings, and implementing monitoring systems to detect anomalies originating from supplier-related challenges. These preemptive actions could bolster the model's resilience, fortifying it against potential disruptions in the supply chain. Consequently, organizations can holistically evaluate the dependability and security of their systems

8. Conclusion

Our research presents a compelling narrative emphasizing the intricate interplay among cyber risk, profit, and investment strategies in the realm of cybersecurity. Based on our quadrant analysis of seventy-two investment decisions made by experts in the field over five years, augmented by digital twin simulations, we gained valuable insights into the dynamics of this domain. We conclude that successful management hinges on strategic investment allocation and timing rather than simply the total amount invested. Optimal strategies, which yield high profits while minimizing vulnerabilities, entail proactive investments in prevention alongside reactive investments in detection and response. Ultimately, the findings of our research empower industrial leaders to make more efficient decisions about safeguarding their digital assets and maintaining resilience in the face of evolving cyber challenges. By contributing to a safer and more secure digital environment for society, our findings pave the way for continued advancements in cybersecurity and risk management practices.

References

Aiyer, B., Caso, J., Russell, P., and Sorel, M. 2022, October 27. New Survey Reveals $2 Trillion Market Opportunity for Cybersecurity Technology and Service Providers. McKinsey & Company.

Annarelli, A., Nonino, F., and Palombi, G. 2020. "Understanding the Management of Cyber Resilient Systems," *Computers & Industrial Engineering* (149), p. 106829.

Anthi, E., Williams, L., Rhode, M., Burnap, P., and Wedgbury, A. 2021. "Adversarial Attacks on Machine Learning Cybersecurity Defenses in Industrial Control Systems," *Journal of Information Security and Applications* (58), p. 102717.

Armenia, S., Angelini, M., Nonino, F., Palombi, G., and Schlitzer, M. F. 2021. "A Dynamic Simulation Approach to Support the Evaluation of Cyber Risks and Security Investments in SMEs," *Decision Support Systems* (147), p. 113580. https://doi.org/10.1016/j.dss.2021.113580.

Armenia, S., Ferreira Franco, E., Nonino, F., Spagnoli, E., and Medaglia, C. M. 2018. "Towards the Definition of a Dynamic and Systemic Assessment for Cybersecurity Risks," *Systems Research and Behavioral Science* (36:4), pp. 404–423. ISSN: 1099-1743, doi: 10.1002/sres.2556.

Barsky, N. 2023, October 6. Clorox Crisis Shows Cyber Risk's Harsh Business Downside. Forbes.

Becerra, M., and Markarian, G. 2021. "Why Are Firms with Lower Performance More Volatile and Unpredictable? A Vulnerability Explanation of the Bowman Paradox," *Organization Science* (32:5), pp. 1327–1345.

Bernard, J., Golden, D., and Nicholson, M. 2020, July 24. Reshaping the Cybersecurity Landscape. How Digitization and the COVID-19 Pandemic Are Accelerating Cybersecurity Needs at Many Large Financial Institutions. Deloitte.

Bhardwaj, S., Jain, L., and Jain, S. 2010. "An Approach for Investigating Perspective of Cloud Software-as-a-Service (SAAS)," *International Journal of Computer Applications* (10:2), p. 40.

Bonime-Blanc, A., and Saban, T. 2022, July 20. Building a Cyber Resilience Strategy for a Geopolitically Unstable World. World Economic Forum, Cyber Security Working Group.

Bowman, H. 1980. A Risk/Return Paradox for Strategic Management. In Sloan Management Review.

Collins, L. M. 2007. Research Design and Methods. In Elsevier eBooks (pp. 433–442).

Cosenz, F., and Noto, G. 2016. "Applying System Dynamics Modelling to Strategic Management: A Literature Review," *Systems Research and Behavioral Science* (33:6), pp. 703–741.

Disterer, G. 2013. "ISO/IEC 27000, 27001 and 27002 for Information Security Management," *Journal of Information Security* (04:02), pp. 92–100. https://doi.org/10.4236/jis.2013.42011

Dupont, B. 2019. "The Cyber-Resilience of Financial Institutions: Significance and Applicability," *Journal of Cybersecurity* (5:1), p. tyz013.

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., and Smeraldi, F. 2016. "Decision Support Approaches for Cyber Security Investment," *Decision Support Systems* (86), pp. 13–23. https://doi.org/10.1016/j.dss.2016.02.012.

Forrester, J. W. 2009. Some Basic Concepts in System Dynamics. Sloan School of Management, Massachusetts Institute of Technology.

Gejo-García, J., Reschke, J., Gallego-García, S., and García-García, M. 2022. "Development of a System Dynamics Simulation for Assessing Manufacturing Systems Based on the Digital Twin Concept," *Applied Sciences* (12:4), p. 2095.

Gontarek, W. 2016. "Risk Governance of Financial Institutions: The Growing Importance of Risk Appetite and Culture," *Journal of Risk Management in Financial Institutions* (9:2), pp. 120–129.
Gros, S. 2021. "A Critical View on CIS Controls," in *2021 16th International Conference on Telecommunications (ConTEL)*. https://doi.org/10.23919/contel52528.2021.9495982
Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., and Pospelova, V. 2022. "The Emerging Threat of Ai-Driven Cyber-Attacks: A Review," *Applied Artificial Intelligence* (36:1). DOI: 10.1080/08839514.2022.2037254
Harrison, J. R., Lin, Z., Carroll, G. R., and Carley, K. M. 2007. "Simulation Modeling in Organizational and Management Research," *Academy of Management Review* (32:4), pp. 1229–1245.
Irei, A. 2023, November 21. Cybersecurity Budgets Lose Momentum in Uncertain Economy, Tech Target. https://www.techtarget.com/searchsecurity/feature/Cybersecurity-budget-trends
Jalali, M. S., Siegel, M., and Madnick, S. 2019. "Decision-Making and Biases in Cyber-Security Capability Development: Evidence from a Simulation Game Experiment," *The Journal of Strategic Information Systems* (28:1), pp. 66–82.
Jinzhi, L., Zhaorui, Y., Xiaochen, Z., Jian, W., and Dimitris, K. 2022. "Exploring the Concept of Cognitive Digital Twin from Model-Based Systems Engineering Perspective," *The International Journal of Advanced Manufacturing Technology* (121:9), pp. 5835–5854.
Kahneman, D. 2011. *Thinking, Fast and Slow*, Farrar, Straus and Giroux.
Kahneman, D., Slovic, P., and Tversky, A. 1982. *Judgement under Uncertainty: Heuristics and Biases*, Cambridge University Press.
Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. Econometrica, 47(2).
Kannan, U., and Swamidurai, R. 2019. "Empirical Validation of System Dynamics Cyber Security Models," in *2019 SoutheastCon*, IEEE, pp. 1–6.
Kissoon, S. T. 2021. "Optimum Spending on Cybersecurity Measures: Part II," *Journal of Information Security* (12:01), p. 137.
Langley, C. J. 2012. *Third-Party Logistics Study: Results and Findings of the 19th Annual Study*, Phoenix, AZ: Capgemini.
Leuschner, R., Carter, C. R., Goldsby, T. J., and Rogers, Z. S. 2014. "Third-Party Logistics: A Meta-Analytic Review and Investigation of its Impact on Performance," *Journal of Supply Chain Management* (50:1), pp. 21–43.
Madnick, S. 2024, March 15. If Companies Are So Focused on Cybersecurity, Why Are Data Breaches Still Rising? The Wall Street Journal. https://bit.ly/4aCq2S0.
Martínez-Moyano, I. J., Oliva, R., Morrison, D. M., and Sallach, D. L. 2015. "Modeling Adversarial Dynamics," in *Proceedings of the 2015 Winter Simulation Conference*, Huntington Beach, CA, USA.
Martinez-Moyano, I. J., and Richardson, G. P. 2013. "Best Practices in System Dynamics Modelling," *System Dynamics Review* (29:2), pp. 102–123.
McLeod, A., and Dolezel, D. 2018. "Cyber-Analytics: Modeling Factors Associated with Healthcare Data Breaches," *Decision Support Systems* (108), pp. 57–68. https://doi.org/10.1016/j.dss.2018.02.007.
Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., and Sadhukhan, S. K. 2013. "Cyber-Risk Decision Models: To Insure IT or Not?" *Decision Support Systems* (56), pp. 11–26. https://doi.org/10.1016/j.dss.2013.04.004.
Nazareth, D. L., and Choi, J. 2015. "A System Dynamics Model for Information Security Management," *Information and Management* (52:1), pp. 123–134.
Randers, J. 2019. "The Great Challenge for System Dynamics on the Path Forward: Implementation and Real Impact," *System Dynamics Review* (35:1), pp. 19–24.
Repenning, N. P., and Sterman, J. D. 2002. "Capability Traps and Self-Confirming Attribution Errors in the Dynamics of Process Improvement," *Administrative Science Quarterly* (47:2), pp. 265–295.
Samuelson, "The Slow-Investment Economy", Business Week, October 17, 1977, p. 62
Sepulveda Estay, D. A. 2021. "A System Dynamic, Epidemiological Approach for High-Level Cyber Resilience to Zero-Day Vulnerabilities," *Journal of Simulation* (17:1), pp. 1–16. DOI: 10.1080/17477778.2021.1890533
Singh, M., Fuenmayor, E., Hinchy, E. P., Qiao, Y., Murray, N., and Devine, D. 2021. "Digital Twin: Origin to Future," *Applied System Innovation* (4:2), p. 36.
Sterman, J. D. 1989. "Modeling Managerial Behavior: Misperceptions of Feedback in a Dynamic Decision-Making Experiment," *Management Science* (35:3), 321–339.

Sterman, J. 2000. *Business Dynamics: System Thinking and Modelling for a Complex World*, Irwin McGraw-Hill.
Sterman, J. D. 2006. "Learning from Evidence in a Complex World," *American Journal of Public Health* (96:3), pp. 505–514.
Morgan, S. 2022 January 19. 2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions, and Statistics. Cybercrime Magazine.
Sullivan-Taylor, B., and Branicki, L. 2011. "Creating Resilient SMEs: Why One Size Might Not Fit All," *International Journal of Production Research* (49:18), pp. 5565–5579.
Sun, W., Zhang, K., Chen, S., Zhang, X., and Liang, H. 2007. Software as a Service: An Integration Perspective. In Lecture Notes in Computer Science (pp. 558–569).
System Dynamics Society. 2024a. A Digital Twin Business Model in 40 Hours. Website consulted on April 9th, 2024, at https://systemdynamics.org/a-digital-twin-business-model-in-40-hours/
System Dynamics Society. 2024b. Digital Twin Business Models for Strategy and Operational Management. Website consulted on April 9th, 2024, at https://bit.ly/442Hw7L/.
Taherdoost, H. 2022. "Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview," *Electronics* (11:14), p. 2181. https://doi.org/10.3390/electronics11142181
Thanh, C., and Zelinka, I. 2019. "A Survey on Artificial Intelligence in Malware as Next-Generation Threats," *MENDEL* (25:2), pp. 27–34. doi:10.13164/mendel.2019.2.027.
Triumph, K. 2023, November 3. Cybersecurity Costs for Small Businesses. Atlantic-IT.
VanDerHorn, E., and Mahadevan, S. 2021. "Digital Twin: Generalization, Characterization, and Implementation," *Decision Support Systems* (145), p. 113524.
Yamin, M. M., Ullah, M., Ullah, H., and Basel Katt. 2021. "Weaponized AI for Cyber-Attacks," *Journal of Information Security and Applications* (57), p. 102722.
Yan, M. R., Hong, L. Y., and Warren, K. 2022. "Integrated Knowledge Visualization and the Enterprise Digital Twin System for Supporting Strategic Management Decisions," *Management Decision* (60:4), pp. 1095–1115.
Zeijlemaker, S. 2022, March 16. Unravelling the Dynamic Complexity of Cyber-Security: Towards Identifying Core Systemic Structures Driving Cyber-Security Investment Decision-Making. Radboud University (342 pages.) (S.l.: s.n.) Supervisor(s): Prof. Dr. E.A.J.A. Rouwette & Prof. Dr. M. von Kutzschenbach.
Zeijlemaker, S., Hetner, C., and Siegel, M. 2023, June 2. 4 Areas of Cyber Risk That Boards Need to Address. Harvard Business Review.
Zeijlemaker, S., Rouwette, E. A., Cunico, G., Armenia, S., and 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), p. 49.
Zeijlemaker, S., and Siegel, M. 2023. "Capturing the Dynamic Nature of Cyber Risk: Evidence from an Explorative Case Study," in *Hawaii International Conference on System Sciences (HICSS) – 56, 2023 January 3rd – January 6th*, Hawaii.
Zhang, Y., and Malacaria, P. 2021. "Bayesian Stackelberg Games for Cyber-Security Decision Support," *Decision Support Systems* (148), p. 113599. https://doi.org/10.1016/j.dss.2021.113599.
Zou, L. 2000. Inherent Reward and Risk (Part I): Towards a Universal Paradigm for Investment Analysis. Tinbergen Institute Discussion Paper, No. 00-050/2, Tinbergen Institute, Amsterdam, and Rotterdam.