Combating Ransomware with an Interactive Gaming Environment

Sander Zeijlemaker[1], Prem Segar[1], Abhishta Abhishta[2], Yasir Haq[2], Michael Siegel[1], Michiru Ishikawa[1], Annet Chau[1] (To be evaluated based on contribution)

[1]Cybersecurity at MIT Sloan (CAMS), MIT Sloan School of Management

[2]University of Twente, NL

Abstract

In today's technology-dependent society, ransomware is one of the biggest cyber risk. Increasing societal impact shows organizations have a hard time governing and overseeing cyber risk. We repurposed a well-documented system dynamics model to raise board-level awareness to combat ransomware. Our simulation realism was significantly boosted by its ability to cover real-life cyber risk management standards and practices to combat ransomware as well as strengthening the core model parameters based on data analyses results of 635 K malware and ransomware detection samples and industry reports. We acquired 734 simulated runs from 100 business leaders and executives who played different simulated games in group settings or on their own. Our work provides insights into defining effective strategies for combating ransomware threats and strengthening cyber risk governance and oversight at the board level.

Key words:

Cyber risk governance, cyber risk management, ransomware, system dynamics, serious gaming

Ransomware is on the Rise

In today's interconnected and technology-dependent society, computers and software significantly affect our daily lives. We use wearables, smartphones, tablets, and other portable devices. Millions of lines of software code are essential for driving modern cars. Concepts such as Industry 4.0, E-health, and smart cities incorporate technology into manufacturing, healthcare, and living spaces. This situation makes managing cyber risk essential for implementing successful business strategies and delivering products and services.

Criminals are also evolving, replacing the crowbar with a laptop, and creating new tools, techniques, and procedures (TTPs) to commit crimes in the digital space. One of these TTPs is called ransomware, digital extortion in which your data is encrypted and held hostage until a ransom is paid (Luo and Liao, 2009). Due to this encryption, defenders' services and product delivery are disrupted, as critical systems cannot function without this data. Unfortunately, ransomware risk is on the rise. Every 11 seconds, a ransomware attack is launched across the globe (European Commission, 2022). Last year, the top five ransomware toolkits (Lockbit 3.0, AlphVM, CL0P, PLAY, and BlackBasta) showed over a 500% increase in usage on average in emerging cyber incidents (Chapman, 2024). Over the 2015–2021 period, the global damage from ransomware rose by 5700% to $20 billion per year and is expected to increase to $265 billion a year by 2031 (Morgan, 2023). The opportunities for extortion are also evolving into double or triple extortion (Kerner, 2024), such as publicly leaking private or sensitive data, notifying the regulator of the breach, or informing important customers about the breach if the ransom is not paid. Overall, ransomware can be considered the biggest cyber risk (ENISA, 2023), as our efforts are not enough to thwart this risk.

On one hand, evolving adversaries, human behavioral limitations, and imperfections in security-boosting technology make organizations prone to cyberattacks (Zeijlemaker et al., 2024). On the other hand, securing a dynamic organization in terms of changing people, processes, and technology suppliers, shifting priorities, and emerging events is very hard (Zeijlemaker and Siegel, 2023). In such situations, business leaders and executives can often be overwhelmed by the complexity and pressure to act when dealing with cyber risk issues. Considering such events, the risk of blind spots when dealing with cyber risk exists. Hence, decision-makers tend toward decisions that yield immediate, easy-to-observe gains at the expense of long-term, hard-to-measure improvements (Sterman, 2001). This attitude may explain why organizations often apply a reactive approach to cybersecurity and improve only after being significantly impacted by a cyber risk. In real life, normalization of the likelihood of organizations being impacted by cyberattacks and overconfidence in best practices exists. Currently, 90% of decision-makers have confidence in the best practices implemented by their organization, and more than half of them expect that their organization will be hit by a cyberattack (Travelers, 2024). Simultaneously, half of these organizations lack essential security measures, such as incident response plans or anomaly detection. Consequently, 72% of businesses worldwide were affected by ransomware in 2023 (Petrosyan, 2024). This finding shows that the defense status of many organizations is lagging adversaries (Casanovas and Nghiem, 2023; Geller, 2023). Overall, strategic awareness is strongly needed to govern and oversee cyber risks.

This research focuses on addressing this need. We repurposed an existing and well-accepted cybersecurity simulation model (based on System Dynamics approach) to analyze strategic decision-making to combat ransomware risk. We calibrated critical model parameters based on insights retrieved through data analysis techniques from a large repository with over 635K data points on the detection of malware and ransomware families by security solutions. Next, we compared cybersecurity theory-backed strategic policy options with the decision-making behavior of experienced cybersecurity executives and senior managers, acquired through simulation. We employed a sensitivity analysis in a uniform distribution-drawn Monte Carlo simulation setup with another 20,000 runs to explore the robustness of our findings. Our work provides insights into strengthening cyber risk governance and oversight efforts to combat ransomware.

Governing and Overseeing Cyber Risk

Societal exposure to cyber threats has motivated legislators to push cyber risk management to the board level. Yet, new management tools are needed to raise appropriate awareness and strengthen the board level to govern and oversee cyber risks.

Cyber Risk Enters the Board Room

The large societal impact of cyber threats, particularly ransomware, and many lagging organizations have pushed governments to act. Through regulations (European Commission, 2020; Fleischer-Black, 2022; Pearlson and Hetner, 2022; Proudfoot et al., 2023, 2024) and white papers (World Economic Forum, 2021), both government and industry bodies push for governing and overseeing cyber risks at the board level.

Governing and overseeing cyber risk becomes a group process (Bezemer et al., 2014) in which not all group members have a solid background in information technology or cybersecurity (Gale et al., 2022), and their dialog focuses on the business, operational, and financial context of cyber risk (Pearlson and Hetner, 2022; Zeijlemaker et al., 2023).

Business leaders and executives use decision-support tools for governing and overseeing cyber risks. For example, allocation and prioritization approaches are based on adherence to frameworks (such as National Institute of Standards and Technology (NIST), Cybersecurity Capability Maturity Model (C2M2), etc.), positioning in comparative benchmarks, adherence to legislation, and acting after suffering breaches (Moore et al., 2016). Although some available tools and approaches can manage more complexity (Wang et al., 2020) or connect financial context to cyber risks (Orlando, 2021), they still have limitations (Wolthuis et al., 2019). They are often static, not accounting for the complex dynamic nature of cyber risk (Falco et al., 2019; Homeland Security, 2018), and have limited ability to align cyber with business needs (Zeijlemaker et al., 2022). From a strategic perspective, a long-term view is needed on managing cyber risks. The dynamic, complex nature of cyber risk cannot be covered in traditional risk management approaches (Lambert et al., 2013; Linkov et al., 2014).

Next Generation of Cyber Risk Management Tools

We used an interactive gaming environment grounded in a system dynamics (SD) approach to help business leaders and executives understand the ransomware threat and explore long-term effective cyber risk management strategies to combat this threat. SD is a modeling approach that describes, simulates, and analyzes complex issues in terms of process, interdependence, information, organizational boundaries, and strategies (Zeijlemaker et al., 2022). It helps to understand socio-technical non-linear complex systems (Sterman, 2000) under the assumption that their underlying systemic structure drives their behavior (Paich et al., 2009).

SD has a long and robust history of SD-based serious games aiming to improve the understanding of systems in various formats: single-player, multiplayer, board games, and virtual games (Cunico et al., 2021; Lane, 1995; Meadows, 2007). Examples of well-known games are Stratagem2 (Sterman and Meadows, 1985), the Beer Game (Sterman, 1992), Sustain game (Papathanasiou et al., 2019), Red versus Blue cybersecurity game (Zeijlemaker et al., 2022), and cybersecurity game (Jalali et al., 2019). These games are known for, among other things, acquiring a deeper understanding of content, improving decision-making skills, fostering behavioral changes, and developing soft skills (Connolly et al., 2012; Meadows, 2007; Qudrat-Ullah, 2010; Wouters et al., 2013).

Specific SD simulations in the field of cybersecurity focus on general cyber threats (Armenia et al., 2021; Delvecchio et al., 2024; Jalali et al., 2019; Zeijlemaker et al., 2022). However, currently available serious gaming and simulation solutions do not capture the specific complex nature of ransomware attacks and the associated business challenges. The next section explains more about these specifics. This is why we repurposed an existing and well-accepted simulation in the community (Jalali et al., 2019).

Model Structure and Parameters

Our work repurposes an existing scientifically grounded, well-accepted, and validated cybersecurity game by incorporating specific structures and parameters relevant to ransomware.

The original cybersecurity game structure

In the original game (Jalali et al., 2019), business leaders can win by achieving the highest accumulated profit. They must allocate their yearly budget to build security capabilities in prevention, detection, and response to survive cyber threats. This approach aligns with commonly used security frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, the Center for Internet Security Controls (CIS), and the International Organization for Standardization 2700X series. During the game, decision-makers must survive generalized cyber threats (measured by the percentage of compromised systems) and maximize their financial performance (measured by accumulated profit) over five years (one game of five rounds). Each year, a budget allocation between 0% and 5% of their IT budget can be invested in prevention, detection, and/or response. The game model structure is shown in Figure 1.

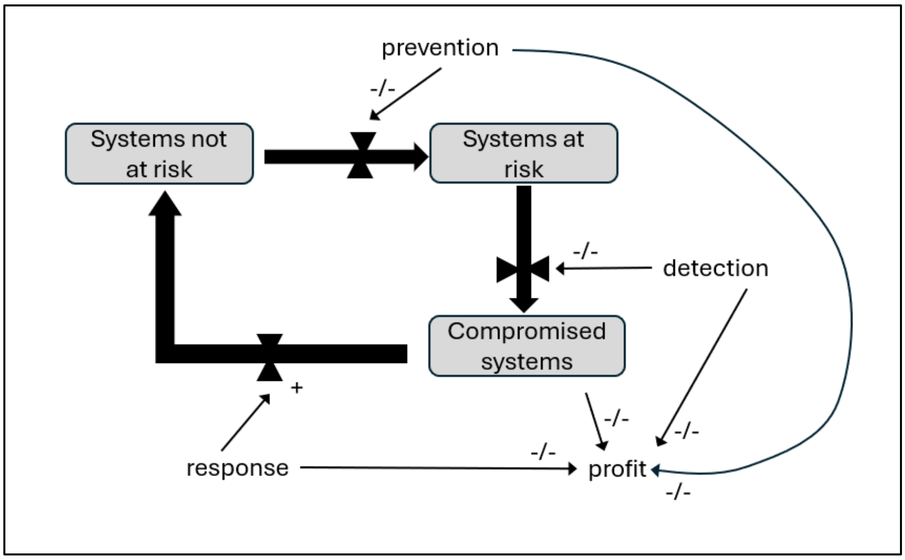


Figure 1. Simulation game structure (Zeijlemaker et al., 2024).

Prevention (CIS, 2021; Office of the Government Chief Information Officer (GCIO), 2020; Muneer, 2021; Pascoe, 2023) involves developing and implementing measures that help the organization understand and manage cybersecurity risks to systems, accounts, assets, data, and capabilities. It includes appropriate safeguards to ensure service delivery and IT hygiene. Detection (CIS, 2021; GCIO, 2020; Muneer, 2021; Pascoe, 2023) involves developing and implementing activities to identify the occurrence of a cybersecurity event and adverse behavior. Response (CIS, 2021; GCIO, 2020; Muneer, 2021; Pascoe, 2023) focuses on developing and implementing appropriate activities to act against an observed cyber event, such as identifying the attack, minimizing its effects, containing damage, and implementing measures to prevent similar incidents in the future. In summary, investing in prevention, detection, and response allows an organization to mitigate risk exposure to identified cyber threats, but it comes at a cost. However, not investing in cybersecurity also incurs costs.

The specifics of combating ransomware

Ransomware attacks have three specific characteristics compared to generalized cyber threats:

(1) Ransomware affects both the cost and revenue sides of the organization. Encrypted computers may cripple revenue generation processes while the company faces additional costs to respond to and recover from the ransomware impact. Ransomware attacks are twice as harmful compared to other cyber threats (NetDiligence, 2022; Sophos, 2023). This fact makes recovery capability critically important. Recovery differs from response. Recovery (CIS, 2021; GCIO, 2020; Muneer, 2021; Pascoe, 2023) focuses on implementing activities to maintain resilience and restore any capabilities or services impaired due to a cybersecurity event. Until full recovery, alternative ways to deliver the impacted services are used and communicated with stakeholders. In this version, between 0% and 5% can also be invested in recovery.

(2) Ransomware attacks often can spread across the technology stack of the firm. For example, in the Maersk case, ransomware spread across the Microsoft stack and crippled a globally operating shipping company within several hours (Steinberg et al., 2021). Especially, Mimikatz

functionality allowed compromised systems to affect systems at risk and systems that were not at risk at all (Steinberg et al., 2021). Another example is the Maastricht University case, in which the adversary could allocate ransomware on critical payment systems, research repositories, and student and employee administrative systems while disabling anti-virus and anti-malware solutions and backup systems (Dijkstra and Van Dantzig, 2020). In terms of the simulation, systems at risk become compromised.

This epidemic substructure is well-known in virus-spreading research (Acemoglu et al., 2020; Sterman, 2000) and applied in malware attack analysis (Zeijlemaker, 2022). It acts as a reinforcing feedback loop that pushes systems (not) at risk of becoming compromised systems.

To mitigate this spreading effect, defenders need different defensive capabilities such as network segmentation and anomaly detection. Anomaly detection requires mature monitoring and logging capabilities, while network segmentation requires mature network security and architecture capabilities (CIS, 2021; Muneer, 2021; Zeijlemaker and Siegel, 2023). Anomaly detection software can detect abnormal communication between devices, within the device, or with malicious domains (Gardiner et al., 2014), while network segmentation is an architectural approach to dividing a larger network into smaller segments of subnetworks that act independently and limit infectivity (Antrosio and Fulp, 2005; Zhang et al., 2014).

(3) Depending on the state of the defender's cyber risk management strategy and the impact of the ransomware attack, there is a strategic question about paying the ransom versus not paying and recovering from the attack. While the cost of recovery can be very high, paying the ransom might not guarantee prompt and full recovery and may allow the adversary to return. There is approximately an 80% probability the adversary will attack again (Cybereason, 2022; Sganga and Bidar, 2021) if the ransom is paid, and a 62% probability that not all data will be recovered (Cybereason, 2022). Paying the ransom reinforces the feedback loop for both the attacker (as success encourages future attacks) and the defender (as recovery efforts may go faster and become less costly). The attacker and defender have opposite roles in this ecosystem, both reinforcing and balancing this loop.

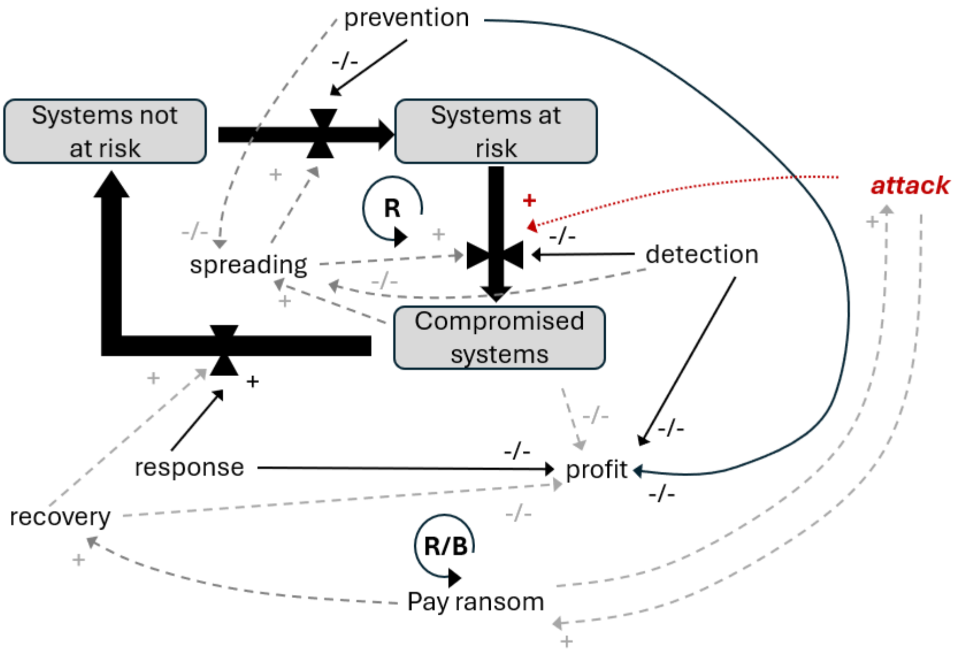


Figure 2. Simulation game structure tailored to ransomware threat. Changes are visible in gray.

These three characteristics have been incorporated into the repurposed model structure of the simulation. This game structure tailored to combat ransomware is visible in Figure 2. Appendix 1 contains more details about the substructures and parameter changes.

Boosting simulation reality through data analytics

Akin reality the core is our simulation model is driven by ransomware attack and defense behavior including multi layer defense option that considers end-point detection and response, segmentation, basic hygiene, back-up and restore of critical business processes (Nagar, 2024; CIS, 2021; GCIO, 2020; Muneer, 2021; Pascoe, 2023).

To tailor the simulation model to real-life ransomware threats and its detection, we utilized two significant large datasets about ransomware and other malware from more than 80 scanners: a large dataset of 635K samples of detection quality and a 90-day longitudinal dataset of 1.5K most recent samples (Haq et al., 2024). Figure 3 shows the time needed for what fraction of scanners to detect a specific ransomware or malware sample. This analysis shows that the scanners can detect 67% of the malware and ransomware families. An average elapsed time of approximately 2 months is needed to achieve such results. However, there is a dependency on ransomware families when it comes to detection quality. This is visible in Figure 4. Figure 4 shows what proportion of detection solutions was able to detect specific families. For instance, emotet, agenttesla, and dridex are widely recognizable families, while sload, encdoc, and sneaky are not. The model parameters relevant to detection, being critical to our simulation, have been tailored accordingly.

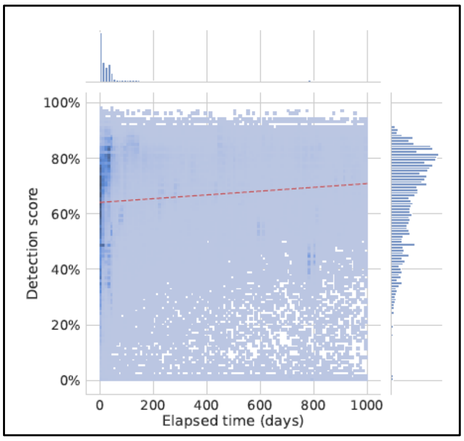


Figure 3. Elapsed time detection (Haq et al., 2024).

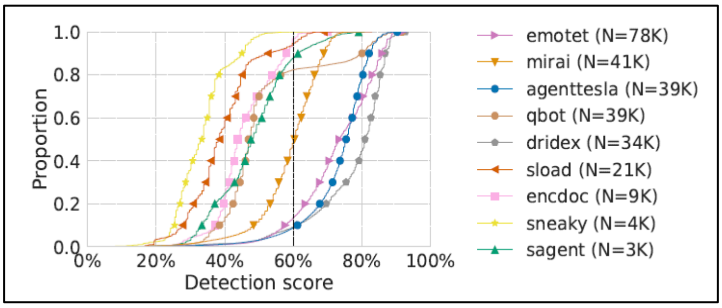


Figure 4. Detection scores (Haq et al., 2024).

Other specific model parameters relevant to combating ransomware, such as recovery and threat impact have been adjusted in line with recent industry insights and research such as Sganga and Bidar (2021), Cybereason (2022), NetDiligence (2022), and Sophos (2023). Details on model parameter changes compared to the original model can be found in Appendix 1.

Policy Analysis

Current available cyber risk management standards, practices, and research provide critical insights regarding the importance of timing, recovering from ransomware attacks, understanding the consequences of ransom payments, and advanced defenses (network segmentation and anomaly detection). Our simulation environment must capture these insights to strengthen managerial awareness.

Importance of timing when combating cyber threats

The debate about proactive and reactive security management is well known, and a reactionary approach to managing cyber risks is often more costly (Böhme and Moore, 2016; Kwon and Johnson, 2014; Zeijlemaker, 2022). Figure 5 shows an exercise with generalized cyber threats in which average investments over five years in prevention, detection, and response (3% per year each, blue) are compared with delayed investments of 5% per year in prevention, detection, and response to each, which start after two years (red). Figure 5 shows that this delayed investment yields lower financial results (profits) and higher risk (as a surrogate compromised systems) over the five-year period. In this last scenario, it is clearly visible that prior to the delayed investments, a large attack occurred in month 15. Our simulation results align with these insights.

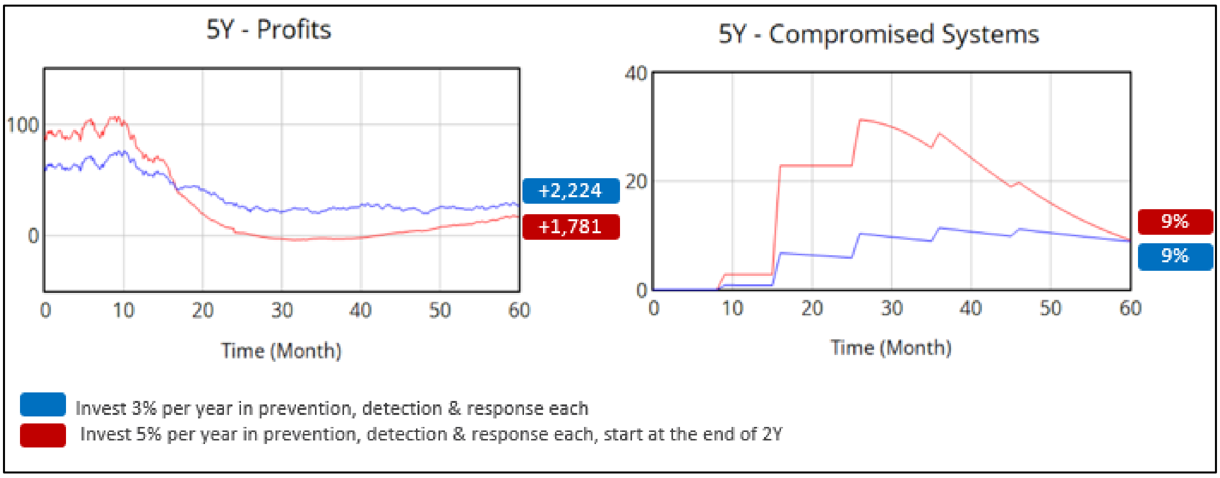


Figure 5. Simulation output: impact of timing.

Investing in ransomware mitigation through recovery capability

Following general cybersecurity standards, the recovery capability has a critical role in mitigating the ransomware threat (CIS, 2021; GCIO, 2020; Muneer, 2021; Pascoe, 2023). Figure 6 shows a simulation exercise in which the ransomware threat impact is shown under the previous investment scenario (3% in prevention, detection, and response per year each—red) and an investment scenario in which recovery is also added to this strategy (blue).

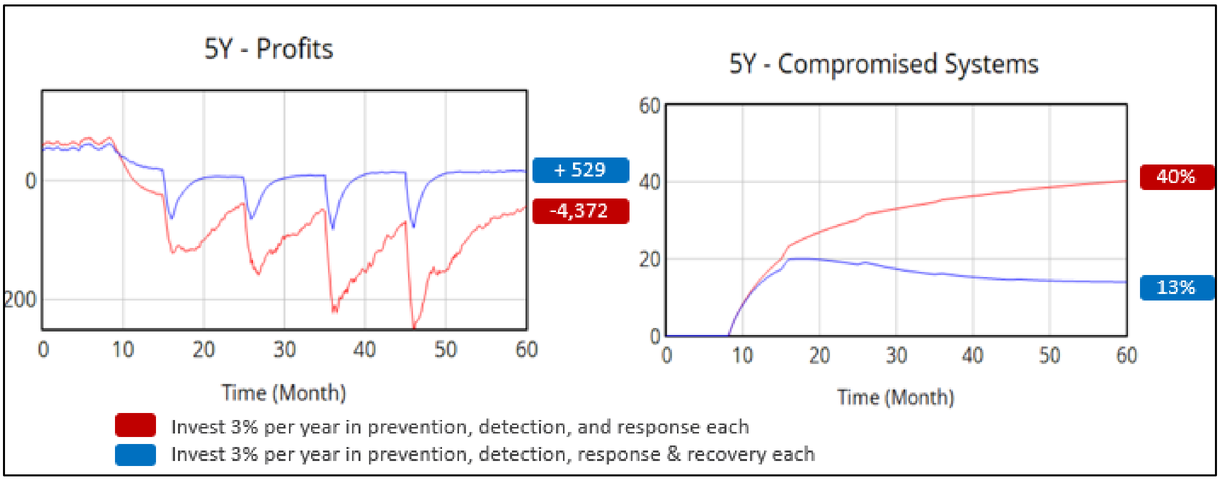


Figure 6. Simulation output: impact of recovery.

Figure 6 shows that recovery has a critical role in limiting the impact of ransomware, as financial results are higher, and risk exposure is lower compared to the other scenario. When comparing Figure 5 (general cyber threat) with Figure 6 (ransomware threat), the nature of ransomware attacks shows a larger financial impact (due to the cost and revenue impact of ransomware attacks) and risk profile (due to the epidemic properties of ransomware attacks).

Dealing with ransomware payments

As previously explained, the ransomware threat presents two options: pay the ransom or recover from the attack through the defenders' own efforts. Figure 7 shows the comparison between paying the ransom (blue) and recovering through defenders' efforts (red). Both simulated runs follow a similar base strategy of investing 3% of their IT budget in prevention, detection, response, and recovery each year for five years.

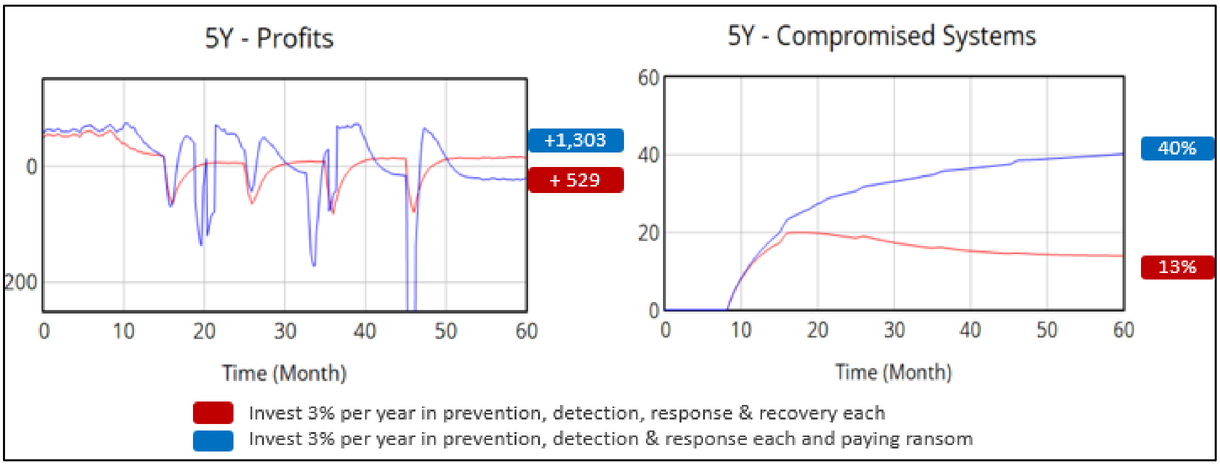


Figure 7. Simulation output: impact of paying the ransom.

Several observations arise when paying the ransom. Financial performance shows significantly more spikes in decline, reflecting that adversaries will attack probabilistically more frequently when ransom is paid (Cybereason, 2022; Sganga and Bidar, 2021). The severity of this decline varies over time, indicating that payment does not always guarantee full access to all data (Cybereason, 2022). If not all data is available, recovery by the defender is still needed, causing additional costs. This cost increase is due to both the payment of the ransom and the recovery efforts. Additionally, when the defender opts to pay the ransom, the defenders' risk profiles do not decline. Ransom payment is a short-term fix, and without additional measures, the adversary will attack again to maintain its revenue source. Adversaries can plan future attacks during the initial one (Hyce, 2023). One example of such preparation is including back doors in the ransom key received by the defender after paying the ransom to decrypt its data. A back door allows access to a targeted system even if the initial infection is detected or removed (Herr, 2014; Microsoft, 2016).

Anomaly detection and network segmentation

Paying the ransom is one option. The defender also has other mitigation measures. As previously explained, ransomware attacks can be mitigated not only by recovery but also by network segmentation and anomaly detection (CIS, 2021; Muneer, 2021; Zeijlemaker and Siegel, 2023). Figure 8 compares the difference between paying the ransom (blue) and strengthening defenses (red). Both scenarios have a base strategy of investing 3% of their IT budget in prevention, detection, response, and recovery each for five years. Strengthening defenses involves an additional investment of 1.5% in prevention and detection, reflecting the implementation of network segmentation and anomaly detection. These defensive measures require more mature capabilities, which is reflected in the significantly higher investments compared to the average of 3%.

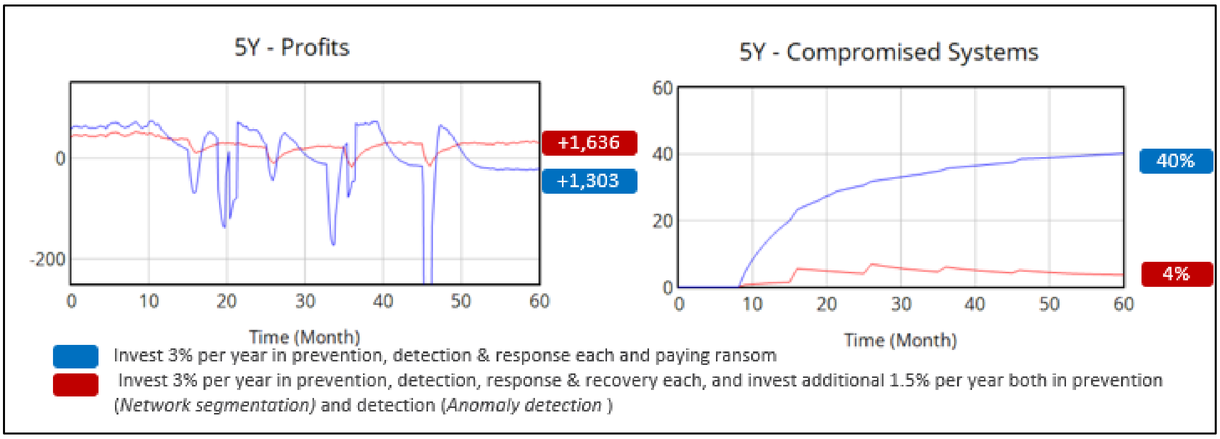


Figure 8. Simulation output: impact of anomaly detection and segmentation.

Figure 8 shows that strengthening defenses provides the best financial results and lowest risk exposure. More importantly, when investments in cyber risk management are sufficient, paying the ransom becomes an option for the defender.

Overall, the simulation structure aligns with generally accepted cyber risk management standards, practices, and research, allowing us to rely on the simulation output. To combat ransomware, the timing of security efforts is essential, recovery capability is critical, and strong defenses (including anomaly detection and network segmentation) make paying the ransom an option for consideration. The question remains: to what extent are these insights applied by decision-makers?

Behavioral Analysis

We used our simulation with board members and senior managers to explore how they combat the ransomware threat.

Participants and gaming scenarios

We played our simulation game with 76 cybersecurity strategists. These individuals have at least five years of experience in cybersecurity or cyber risk management at the executive, senior management, or board level. They had experience in healthcare (25), finance (10), or other industries (41). Another group of participants involved eight groups, each consisting of three executives with backgrounds in finance, risk management, and technology. They played the simulation as a group and decided together. All participants and groups combined played 734 games.

Game	Cyber threat	Adversary
Cyber threat	Generalized threats	Deterministic attack pattern
Random cyber threat	Generalized threats	Random launched attacks
Ransomware	Ransomware threat only	Deterministic pattern
Pay ransom	Ransomware threat only	(1) Deterministic and additional attacks are random (80% probability) (2) Adversary is paid for decrypting data or systems (3) Recovery by paying ransom (62% probability not fully recovered)

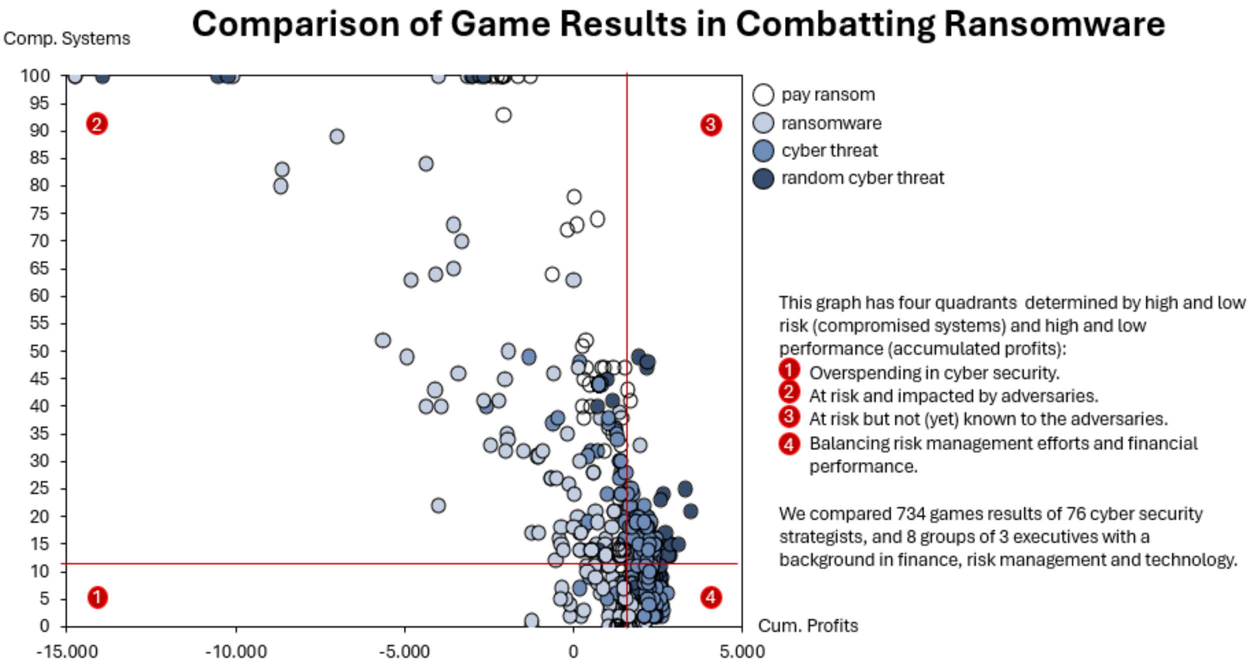
Table 1. Different game formats.

Participants played up to four different games. Table 1 explains the different games. A deterministic attack pattern does not change if a game restarts (TTPs, strength, and time remain the same). In a simulation with randomly launched attacks, the total attacks launched after five years will be the same as in the game with deterministic attacks. When comparing both simulation the random attack simulation allows for greater variance in financial performance as random scenarios allows for concentrated attack behavior at the beginning or the end of simulation. On average the simulation perform comparable.

In the game in which ransom is paid, the total attacks after five years are no more than 80% higher compared to the other games. Not all participants played all the game formats. We used scenarios involving generalized cyber threats to familiarize participants with the simulation game, followed by ransomware and paying the ransom games.

Game results

To analyze the game results, we made a relative comparison from our game dataset and recognized four areas: high and low risk based on the percentage of compromised systems and low and high accumulated profits. The low-risk and low-profit quadrant (1st) is where very high security expenditures yield low financial results. The high-risk and low-profit quadrant (2nd) is where a lack of security investments benefits the adversary significantly. The high-risk and high-profit quadrant (3rd) is where the defender is potentially exposed to cyber threats, and this opportunity has not been fully utilized by the adversary. The low-risk and high-profit quadrant (4th) is where cyber risk management efforts are balanced and aligned with business needs. We determined the cutoff by the average compromised systems and accumulated profits in our dataset. Figure 9 shows the game results after five years per type of game, and Figure 10 shows the same results per participant type.



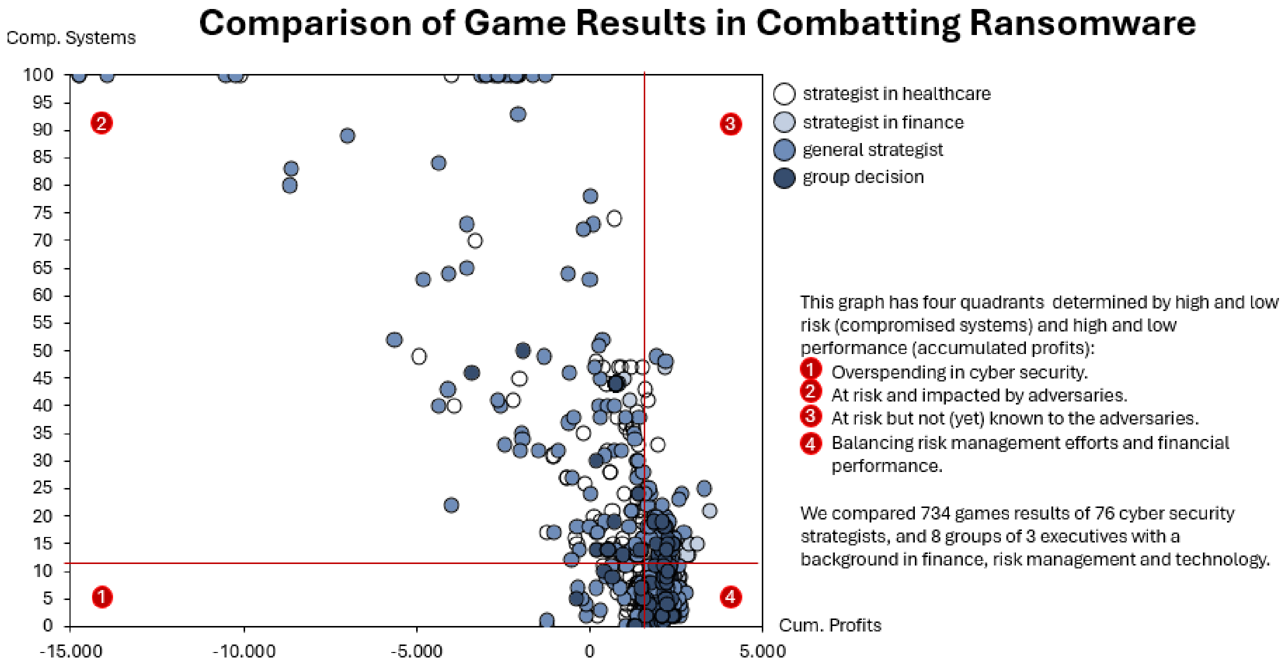
This graph has four quadrants determined by high and low risk (compromised systems) and high and low performance (accumulated profits):
1 Overspending in cyber security.
2 At risk and impacted by adversaries.
3 At risk but not (yet) known to the adversaries.
4 Balancing risk management efforts and financial performance.

We compared 734 games results of 76 cyber security strategists, and 8 groups of 3 executives with a background in finance, risk management and technology.

Figure 9. Game plot results after five years per game type.

When faced with generalized cyber threats, 60% of the games ended in the 4th quadrant. However, when adding uncertainty or complexity to the game, these results deteriorated quickly. In the case of randomly launched generalized cyber threats, this percentage lowered to 48%. The complexity of ransomware lowered this percentage to 36% (not paying ransom) or 29% (paying ransom). Our game results indicate that even experienced and knowledgeable decision-makers have difficulties appreciating complexity and uncertainty, as more games ended up in the other quadrants.

When comparing the sectors where participants work, we observe that 66% of the games played by security specialists in the financial sector ended in the 4th quadrant, followed by decision-makers with 55% of their games in this quadrant, and 44% of the games of all other participants ended up in this quadrant. Yet, in the most complex form of the game—combating ransomware and paying the ransom—the group of decision-makers outperformed all others, with 67% of their games ending in the 4th quadrant. When participants faced uncertainty, security specialists in the financial sector outperformed all others, with 58% of their games in this quadrant. When combating ransomware threats, security specialists working in the financial or healthcare sectors did well, with 45% of their games ending in this quadrant. Overall, group decision-makers showed the most stable performance, ending up with most games in or near the preferred quadrant.



This graph has four quadrants determined by high and low risk (compromised systems) and high and low performance (accumulated profits):
1 Overspending in cyber security.
2 At risk and impacted by adversaries.
3 At risk but not (yet) known to the adversaries.
4 Balancing risk management efforts and financial performance.

We compared 734 games results of 76 cyber security strategists, and 8 groups of 3 executives with a background in finance, risk management and technology.

Figure 10. Game plot results after five years per participant type.

Participants played the game several times, and once they understood how to develop a sustainable strategy to manage cyber risks, they started to use the simulation in an exploratory way to find alternative or better strategies. Consequently, participants ended up in other quadrants too. This raises a question about the learning efforts in the simulation environment.

Learning efforts in combating ransomware

In terms of learning efforts, we measured the attempts participants needed to achieve game results in the most favorable 4th quadrant for the first time when combating ransomware with or without paying the ransom. We also added the percentage of participants able to do so. Our game data allowed us to analyze these learning effects for 59 participants. These are shown in Table 2.

		Average	SD	participants / groups	% success
Pay Ransom	Health	1.7	1.10	22	50%
	Group	1.4	0.53	8	88%
	Other	2.2	1.10	16	31%
	Overall	**1.7**		**46**	**50%**
Ransomware	Health	2.4	1.46	25	80%
	Group	2.6	1.13	8	88%
	Other	2.7	2.06	26	46%
	Overall	**2.5**		**59**	**66%**

Table 2. Learning effects when combating ransomware.

When it comes to combating ransomware, only 66% of experienced security strategists can design an effective strategy. On average, they need 2.5 attempts to develop such a strategy. With experience, they require only 1.7 attempts on average to design such strategy when combating ransomware under condition of paying the ransome. Unfortunately, the additional complexity related to ransom payment dynamics lowers their success rate to 50%. We used ANOVA to analyze the differences between groups (Hair et al., 2006). There are no significant differences between the groups, except for one interesting observation: group-based decision-making significantly increases the success rate, with 88% of groups able to define successful strategies for combating ransomware, regardless of whether a ransom is paid.

Implemented Strategies for Combating Ransomware

For 55 games, we used detailed decisions of individual participants for further analysis. These 55 games fit well within the accumulated profit ranges (winning criteria) of the 734 games. These 55 games involve combating the ransomware threat with or without paying the ransom. We analyzed the accumulated investments as a percentage of the IT budget over five years in prevention, detection, response, and recovery, the total of these four combined, and investments in mature capabilities. We define a mature capability as cyber security investments exceeding 3% year on year. A defender can have up to four mature capabilities (prevention, detection, response, and recovery). Examples of mature capabilities include network segmentation (prevention) and anomaly detection (detection). These results are shown in Table 3 for high versus low-risk quadrants and Table 4 for high versus low-profit quadrants. These tables show a strong tension between risk and financial performance. Low risk requires significantly higher investment levels and many mature capabilities, while high profitability requires significantly lower investment levels and fewer mature capabilities. Table 4 shows overall less significant differences in investment strategies concerning financial performance for two reasons: (1) the low number of high-profit performance games, and (2) within this small group, different investment strategies can yield similar effective results but will affect the standard deviation significantly. We used t-statistics to compare the different datasets (Hair et al., 2006).

Risk	items	Prevention	Detection	Response	Recovery	Total	Capabilities
Low	AVG	19,90	16,76	17,57	19,67	74,39	2,93
	SD	4,31	8,38	5,02	6,83	15,24	1,19
	##	29	29	29	29	29	29
High	AVG	11,83	11,46	12,42	11,50	47,21	0,72
	SD	6,25	5,70	5,26	6,71	11,58	0,84
	##	26	26	26	26	26	26
significance		P<0.01	P<0.01	P<0.01	P<0.01	P<0.01	P<0.01

Table 3. Investment insights over five Years: high-risk versus low-risk quadrant.

Profit	items	Prevention	Detection	Response	Recovery	Total	Capabilities
High	AVG	16,20	10,60	12,70	10,00	49,50	1,80
	SD	6,35	10,76	9,35	13,69	12,26	1,10
	##	5	5	5	5	5	5
Low	AVG	16,07	14,62	15,38	16,39	62,46	1,92
	SD	6,75	7,32	5,30	7,01	19,29	1,55
	##	50	50	50	50	50	50
significance		N/a	N/a	N/a	P<0.1	N/a	P<0.1

Table 4. Investment insights over five years: High-profit versus low-profit quadrant.

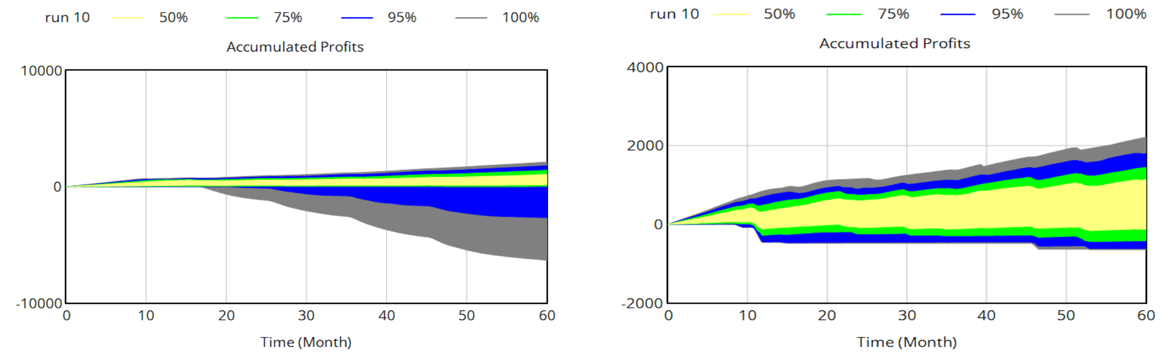
Overall, as multiple pathways to combating ransomware may yield similar results in risk and financial performance, a strong cyber vision toward an intended end state with both focus areas and small defense investment calibration toward emerging threats over time will help. The presence of more than one mature capability is essential, but most capabilities do not need to be fully matured. These not fully mature capabilities appear financially appropriate. Additionally, investment levels in the different capabilities will also differ over time.

Sensitivity Analysis and Optimization

To strengthen the robustness of our work, we used both optimization and sensitivity analysis. The optimization analysis determined the most effective investment strategy using simulation software. We aimed to maximize accumulated profits (relative weight 5) and minimize compromised systems (relative weight 1). After 235 simulations, the optimized investment strategy to combat ransomware involved low investments in prevention, high investments in detection, and maximum investments in response and recovery, yielding the best results of $2,200 accumulated profit and 1.44% of compromised systems. When paying the ransom, equivalent results were established after 135 simulated games by using the previously established optimized strategy but lowering the investments in response from maximum to high levels. This lower level of investment balances paying the ransom to the adversary. These insights align with the call to executive boards to focus on resilience (Pearlson, 2024) and are consistent with observed investment strategies in the previous section. They also show that a strong cyber risk management strategy makes ransom payments an option for consideration.

The sensitivity analysis, a random exponential distribution-drawn Monte Carlo simulation, consists of 20,000 different investment strategies under the conditions of combating ransomware with and without paying the ransom. This distribution aligns with the distribution in our dataset, emphasizing average to higher investments in security capabilities. The sensitivity analysis, presented in this research, uses the different colors of yellow, green, blue, and gray to present the distribution of possible outcomes. In this analysis, each investment strategy for a 5-year period is a separate simulation run of the model aggregated by the model software. Figure 11 shows the results of the Monte Carlo simulation.

Our sensitivity analysis shows that combating the ransomware threat has the same risk profile in terms of compromised systems, irrespective of paying the ransom. Financial performance shows that paying the ransom mainly limits the downside risk of the ransomware threat impact. This indicates that paying ransom is primarily associated with poor cyber risk management strategies. Nevertheless, the emerging nature of this risk may create situations where paying ransom is the only viable solution.



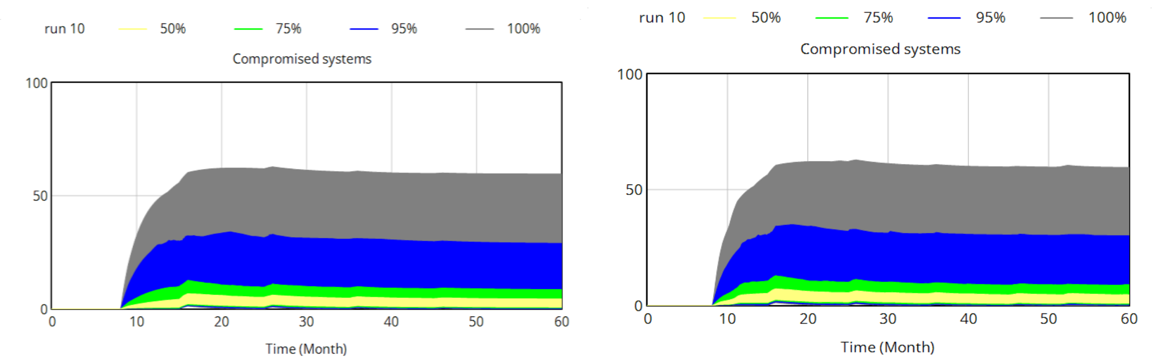


Figure 11. Sensitivity analyses: accumulated profits and compromised systems. Left side – graphs related to ransomware threat. Right side - graphs related to paying ransom.

Figure 11 also shows that this downside impact of the ransomware threat fits into the outer probability spectrum of the sensitivity analysis. Maintaining strong financial performance and low-risk levels under a ransomware threat requires a solid cyber risk management strategy, regardless of whether the ransom is paid. Ultimately, having such a strategy makes paying the ransom an option.

Conclusion and Discussion

Our work contributes to both SD literature and Information Security Management literature. In the field of SD, we integrated different systemic structures (success-to-the-successful and susceptible-infected-resolved) into a well-known cybersecurity game to combat the ransomware threat. Additionally, we combined data science efforts to leverage large data repositories to strengthen model calibration. Finally, we added to the suite of training and awareness solutions in this field.

In the field of Information Security Management, our work provides a new angle to raise awareness at the board level using simulation-aided approaches. To our knowledge, simulations have rarely been used in cyber risk management to strengthen board governance and oversight in this field.

Societal increasing exposure to ransomware threats, followed by regulatory changes, pushes cyber risk management to the boardroom level and shows a need to strengthen awareness to govern and oversee cyber risk. Our work fulfills this need because, unlike the real world, where a bad choice may materially harm organizations, simulation games allow managers to test how their cyber risk management strategy decisions evolve in real life (Armenia et al., 2018; Jalali et al., 2019). One hundred executives and business leaders from different industries provided insights into their decision-making with 734 different games. People have difficulties making decisions in the complex environment of cyber risk and tend to use simple mental rules (heuristics) to make decisions in these environments (Grossklags and Reitter, 2014; Sterman, 1989). In general, these simple mental rules usually help regarding short-term objectives (Rosoff et al., 2013; Tversky and Kahneman, 1973) but lead to biased gain and loss estimations (Kahneman and Tversky, 1979; Kahneman, 2011). Ultimately, such event-driven decisions or reactive approaches may generate future risks (Sterman, 2001).

Our simulation shows that even highly experienced and knowledgeable decision-makers have difficulties appreciating cyber risk. Approximately 50% to 66% of cybersecurity strategists need 1.7 to 2.5 attempts to devise an effective investment strategy to combat ransomware threats. When it comes to these investments, our work shows the following:

- Optimizing cyber risk management strategies is challenging in this complex environment.

- Time delays in building cybersecurity capabilities are critical, and investing more in the future does not compensate for a lack of budget in the past.
- There is an inherent risk-reward paradigm, in which equivalent budget spending creates similar rewards but very different risk profiles, and vice versa. Yet, in addition some mature capabilities are needed to combat ransomware.
- Investing wisely creates much more flexibility around ransom payment decisions.

Our work also provides insights to strengthen cyber risk governance and oversight at the board level. We advocate for strengthening current management dashboards with simulation capabilities. Simulation shows the 5-year future effects of strategic decisions and allows for exploring scenarios to maximize profit and minimize risks. Additionally, to Align Cyber Risk Management with business needs, we recommend governing and overseeing cyber risks in a committee consisting of a multidisciplinary group with backgrounds in risk management and finance, technology, and business. Our work shows that group-based decisions provide mostly long-term effective solutions when dealing with complexity, as 88% of the groups could devise effective strategies to combat ransomware.

Our work is a general cybersecurity simulation, while specific industries have unique characteristics. Examples include Operational Technology in the manufacturing sector (Prinsloo et al., 2019). Cyber risk exposure in healthcare and manufacturing may cause additional impacts such as safety risks (Buzdugan, 2020; Prinsloo et al., 2019), and critical infrastructures may cause significant societal impact (Zeijlemaker et al., 2024). Additionally, technological evolutions such as artificial intelligence, machine learning, and quantum computing may change the interaction between humans and computers (Malone and Bernstein, 2022) and, consequently, the attacker-defender interaction as TTPs and mitigation measures may also evolve (Raban and Hauptman, 2018). All this underscores the need for differentiated simulation and opportunities for future research.

Acknowledgements

Think Cell software was used to create Figures 9 and 10.

Appendix 1

Compared to the original cyber security simulation (Jalali et al., 2019) this research incorporated changes to both the model structure and the model parameters.

Model structure changes

Three model structure changes have been included. Each structure change is explained, and mathematical equations are provided. These equations include their variables with units between brackets. DMNL refers to a dimensionless unit used in SD to calculate percentages or fractions.

- The recovery capability. The recovery capability structure involves the investment in this capability as well as its decay over time over time. This capability mitigates the effects of the ransomware attack impacting revenue generating ability of the organisation. The second structure that has been included.

$$RC\ (t) = \int_0^t [\ RCi - RCd] + RC(o)\ (\mathrm{dmnl})$$

$RC\ (t)$ = is the accumulated maturity of the recovery capability over time driven by its initial maturity $RC(o)$ and its recurring investments RCi and capability decay over time RCd.

$$M\ (t) = \int_0^t [\ Mi - Md]\ (\mathrm{dmnl})$$

$M\ (t)$ = is the accumulated impact of a ransomware attack on top of a generalized cyber threat driven by the ransomware attack behavior and mitigation behavior.
Mi = 10.5 *CA - $M\ (t)$ where CA (dmnl/month) is the occurred ransomware attack and 10.5 is the model parameter bridging the difference between generalized cyber threats impact and ransomware impact following industry research (NetDiligence 2022).
Md = $RC\ (t)$ * RL + $ReC\ (t)$ * ReL which resembles the decline of the ransomware impact caused by maturity if the recovery $RC\ (t)$ and response capability $ReC\ (t)$ in place. Both are multiplied by a non-linear and non-dimensional multiplier RL and ReL respectively that translates capability maturity to mitigation efforts (Sophos (2023).

- The spreading of ransomware. This structure involves the epidemic properties of ransomware where compromised systems infect systems (not) at risk. A second element is that high mature prevention and detection limits this effect as it reflect measures of network segmentation and anomaly detection, respectively. Below the mathematical equation is specified for this structure:

S = L*CS/(CS+SNR+SR)^2^P where
S (dnml) = spreading effect as a fraction that increases systems not at-risk becoming systems at risk and system at risk becoming compromised systems.
L (dnml) = limit of the spreading caused by security measures like anomaly detection and network segmentation. This is a non-linear and non-dimensional multiplier depending on maturity of prevention and/or detection.
CS (systems) = total number compromised systems
SR (systems) = total number of system at risks
SNR (systems) = total number of systems not at risk
^2 is uses to include all possible communications between connected assets within the network topology of the defender.
^P raises a power to reflect the speed of spreading aligned with multiple ransomware cases including mentioned Maersk and Maastricht University.

- The option to pay for the ransom. This is a binary structure that affect probability driven event as paying the ransom (1) indues a risk of the adversary attacking more often and recovery is not always effective due to incomplete data restore, and (2) evokes a one-off payments that may reduce risk mitigation efforts. Relevant mathematics are:

P(At|Rp) = 0.80 meaning that when a ransom is paid (Rp) there is an 80% probability that another cyber attack (At) will be launched with 12 months. Under the condition of paying ransomware the total number of ransomware attacks in the five-year period is maximized by 180%.
P(Rcf|Rp) = 0.62 meaning that when a ransom is paid (Rp) there is an 62% probability that the received unlock code will not work properly. This will cause the defender to fail back to its original recovery procedures for a fraction between 0% and 100% (based on a random uniform probability function).

Model parameter changes

In Table 5 the parameters all parameters are visible that have been changed in the original model when repurposing the simulation model.

Model Parameter	Jalali, et al (2019)	Ransomware model	Justification
Time 1 (average time for risk propagation)	10	7	IBM (2024) it takes approx. 7 month to propagate cyber risk.

Time 2 (average time to detect system at risk)	2	2	Following our data analysis detection takes approx. 1-2 months.
Time 3 (average response time)	3	2	Recovery efforts are approx. 2-3 months Sophos (2023), IBM (2024).
Power Impact of detection	0.5	0.4	This parameter at 0.4 yields a power of detection close to 66% in the simulation. This is in line with our data analysis.
Average cyber attack duration should be approx. 10 - 11 months (Cybereason 2022, Culafi 2023, Vardham & Tonogbanua 2024, IBM 2024). Detection and response should not exceed three months combined.			

Literature

Acemoglu D, Chernozhukov V, Werning I, Whinston MD. 2020. Optimal targeted lockdowns in a multi-group SIR model. *NBER Working Paper* 27102.

Antrosio JV, Fulp EW. 2005. Malware defense using network security authentication. *Third IEEE International Workshop on Information Assurance* (IWIA'05), 43–54, doi: 10.1109/IWIA.2005.11.

Armenia S, Angelini M, Nonino F, Palombi G, Schlitzer MF. 2021. A dynamic simulation approach to support the evaluation of cyber-risks and security investments in SMEs. *Decision Support Systems* 147 (113580). https://doi.org/10.1016/j.dss.2021.113580.

Armenia S, Ferreira Franco E, Nonino F, Spagnoli E, Medaglia CM. 2018. Towards the definition of a dynamic and systemic assessment for security risks. *System Research and Behavioural Science* ISSN: 1099–1743, doi: 10.1002/sres.2556.

Bezemer PJ, Nicholson G, Pugliese A. 2014. Inside the boardroom: Exploring board member interactions. *Qualitative Research in Accounting & Management* **11**(3): 238–259.

Böhme R, Moore T. 2016. The "iterated weakest link" model of adaptive security investment. *Journal of Information Security* **7**:81–102. doi: 10.4236/jis.2016.72006.

Buzdugan A. 2020. Integration of cyber security in healthcare equipment. In Tiginyanu I, Sontea V, Railean S. (eds.) *4th International Conference on Nanotechnologies and Biomedical Engineering. ICNBME 2019. IFMBE Proceedings*, vol 77. Springer, Cham. https://doi.org/10.1007/978-3-030-31866-6_120.

Casanovas M, Nghiem A. 2023. Cybersecurity – Is the Power System Lagging Behind? https://www.iea.org/commentaries/cybersecurity-is-the-power-system-lagging-behind.

Chapman R. 2024. Ransomware Cases Increased by 73% in 2023 Showing Our Actions Have Not Been Enough to Thwart the Threat. https://www.sans.org/blog/ransomware-cases-increased-greatly-in-2023/.

CIS. 2021. CIS controls V8. Centre of Internet Security. East Greenbush, New York.

Connolly TM, Boyle EA, MacArthur E, Hainey T, Boyle JM. 2012. A systematic literature review of empirical evidence on computer games and serious games. Comput. Educ. **59**: 661–686.

Cunico G, Aivazidou E, Mollona E. 2021. System dynamics gamification: A proposal for shared principles. Syst. Res. Behav. Sci. preprint.

Culafi, A. 2023, January 8. LastPass faces mounting criticism over recent breach. Techtarget.com. https://www.techtarget.com/searchsecurity/news/252529329/LastPass-faces-mounting-criticism-over-recent-breach

Cybereason. 2022. Ransomware: The True Cost to Business 2022. Report. https://www.cybereason.com/ransomware-the-true-cost-to-business-2022.

Delvecchio T, Zeijlemaker S, De Bernardis G, Siegel M. 2024. Revolutionizing board cyber-risk management using collaborative gaming. In *Proceedings of the 10th International Conference on Information Systems Security and Privacy*, ISBN 978-989-758-683-5, ISSN 2184-4356, 112–119.

Dijkstra M, Van Dantzig M. 2020. Spoedondersteuning Project Fontana met Reactie Universiteit Maastricht, Fox-IT. https://www.vtmgroep.nl/kennisbank/bevindingen-fox-it-bij-hack-universiteit-maastricht.

ENISA. 2023. ENISA Threat Landscape 2023, European Union Agency for Cyber Security. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

European Commission. 2022. Cyber Resilience Act – Factsheet, European Commission Newsroom, https://ec.europa.eu/newsroom/dae/redirection/document/89528.

Fleischer-Black M. 2022. SEC Cyber Rules: How to Prepare for the New 8-K Incident Mandate. https://www.cslawreport.com/19356726/sec-cyber-rules-how-to-prepare-for-the-new-8k-incident-mandate.thtml.

Gale M, Bongiovanni I, Slapnicar S. 2022. Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead. *Computers & Security* 121, 102840.

Gardiner J, Cova M, Nagaraja S. 2014. Command and control, understanding, denying, and detecting. University of Birmingham, Centre for the Protection of Natural Infrastructure.

GCIO. 2020. An overview of ISO/IEC 27000 family of Information Security Management System Standards. Published by the Office of the Government Chief Information Officer in April 2015 (Updated in May 2020).

Geller E. 2023. Government Agencies Are Lagging on Key Cyber Defenses, and the White House Isn't Happy. https://themessenger.com/tech/government-agencies-are-lagging-on-key-cyber-defenses-and-the-white-house-isnt-happy.

Grossklags J, Reitter R. 2014. How task familiarity and cognitive predispositions impact behavior in a security game of timing. *IEEE 27th Computer Security Foundations Symposium*.

IBM. 2024. Cost of databreach report 2024. https://www.ibm.com/reports/data-breach-action-guide

Hair JH, Black WC, Babin BJ, Anderson RE, Tatham RL. 2006. *Multivariate Data Analysis*, 6th Edition, Pearson, Prentice Hall, Upper Saddle River, New Jersey.

Haq MYM, Abhishta A, Zeijlemaker S, Chau A, Siegel M, Nieuwenhuis LJ. 2024. Measuring malware detection capability for security decision making. In *9th International Workshop on Traffic Measurements for Cybersecurity, WTMC 2024*.

Herr T. 2014. PrEP: A framework for malware & cyber weapons. *Journal for Information Warfare* **13**(1).

Hyce. 2023. Ransomware Attacks - Never Pay the Ransom (Here's Why), ransomware protection blog, Hycu.com. https://www.hycu.com/blog/ransomware-attacks-dont-pay-the-ransom.

Jalali MS, Siegel M & Madnick S. 2019. Decision-making and Biases in Cyber-security Capability Development : Evidence from a Simulation Game Experiment. The Journal of Strategic Information Systems, Volume 28, Issue 1, March 2019, Pages 66-82. https://doi.org/10.1016/j.jsis.2018.09.003.

Kahneman D. 2011. *Thinking, Fast and Slow*. Farrar, Straus, and Giroux.

Kahneman D, Tversky A. 1979. Prospect theory: An analysis of decision under risk. *Econometrica* **47**(2).

Kerner MS. 2024. Ransomware trends, statistics and facts heading into 2024. https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts.

Kwon J, Johnson ME. 2014. Proactive versus reactive security investments in the healthcare sector. *MIS Quarterly* **38**(2): 451-A3. https://misq.umn.edu/proactive-versus-reactive-security-investments-in-the-healthcare-sector.html.

Lane DC. 1995. On a resurgence of management simulations and games. J. Oper. Res. Soc. **46**: 604–625.

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.

Malone TW, Bernstein MS. (Eds.). 2022. *Handbook of Collective Intelligence*. MIT Press.

Meadows D. 2007. A brief and incomplete history of operational gaming in system dynamics. Syst. Dyn. Rev. **23**: 199–203.

Microsoft. 2016. Volume 21, Microsoft security intelligence report January through June 2016, Regional threat assessment. Downloaded from: https://www.microsoft.com/security/sir/threat/.

Mızrak F. 2023. Integrating cybersecurity risk management into strategic management: A comprehensive literature review. *Research Journal of Business and Management* **10**(3): 98–108. https://doi.org/10.17261/Pressacademia.2023.1807.

Moore, T., Duynes, S., & Chang, F. R. (2016). Identifying how firms manage security investment. Workshop on the Economics of Information Security (WEIS), Berkeley, CA, June 13–14.

Morgan S. 2023. Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

Muneer F. 2021. Cybersecurity Capability Maturity Model, Version 2.0, July 2021, US Department of Energy.

Nagar, G. (2024). The Evolution of Ransomware: Tactics, Techniques, and Mitigation Strategies. Valley International Journal Digital Library, 1282-1298.
https://vipublisher.com/index.php/vij/article/view/387

NetDilligence. 2022. Cyber Claim Study 2022. https://netdiligence.com/cyber-claims-study-2022-report/.

Olson EG. 2005. Strategically managing risk in the information age: A holistic approach. *Journal of* Business Strategy **26**(6): 45–54. https://doi.org/10.1108/02756660510700618.

Orlando A. 2021. Cyber risk quantification: Investigating the role of cyber value at risk. *Risks* **9**(10): 184. https://doi.org/10.3390/risks9100184.

Paich M, Peck C, Valant J. 2009. *Pharmaceutical Product Branding Strategies: Simulating Patient Flow and Portfolio Dynamics*. Second edition. Informa Healthcare USA. Inc.

Papathanasiou JSS, Armenia S; Barnabè F, Carlini C, Ciobanu N, Digkoglou P, Jarzabek L, Kulakowska M, Lanzuisi A, Morfoulaki M, et al. 2019. Game based learning on urban sustainability: The "sustain" project. In *Proceedings of the 11th International Conference on Education and New Learning Technologies*, Palma, Spain, 1–3 July 2019.

Pascoe CE. 2023. Public Draft: The NIST Cybersecurity Framework 2.0.

Pearlson K, Hetner C. 2022. Is Your Board Prepared for New Cybersecurity Regulations? IT Security Management. Harvard Business Review. http://bit.ly/40Jql8v.

Pearlson K. 2024. When Cyberattacks Are Inevitable, Focus on Cyber Resilience. https://hbr.org/2024/07/when-cyberattacks-are-inevitable-focus-on-cyber-resilience.

Petrosyan A. 2024. Businesses Worldwide Affected by Ransomware 2018–2023. https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/#:~:text=In%202023%2C%20the%20healthcare%20industry,by%20the%20government%20facilities%20industry.

Prinsloo J, Sinha S, Von Solms B. 2019. A review of industry 4.0 manufacturing process security risks. *Applied Sciences* **9**(23): 5105. https://doi.org/10.3390/app9235105.

Proudfoot JG, Cram WA, Madnick S. 2024. Weathering the storm: Examining how organizations navigate the sea of cybersecurity regulations. *European Journal of Information Systems*, (1–24).

Proudfoot JG, Cram W, Madnick S, Coden M. 2023. The importance of board member actions for cybersecurity governance and risk management. *Management Information Systems Quarterly Executive* (MISQE) **22**(4): 235–250.

Qudrat-Ullah H. 2010. Perceptions of the effectiveness of system dynamics-based interactive learning environments: An empirical study. *Comput. Educ.* **55**: 1277–1286.

Raban Y, Hauptman A. 2018. Foresight of cyber security threat drivers and affecting technologies. *Foresight* **20**(4): 353–363. https://doi.org/10.1108/FS-02-2018-0020.

Rosoff H, Cui J, John RS. 2013. Heuristics and biases in cybersecurity dilemmas. *Environment Systems and Decisions* **33**: 517–529. https://doi.org/10.1007/s10669-013-9473-2.

Sganga N, Bidar M. 2021. 80% of Ransomware Victims Suffer Repeat Attacks, According to the New Report. CBS News.

Steinberg S, Stepan A, Neary K. 2021. NotPetya: A Columbia University Case Study, School of International and Public Affairs Case Consortium at Columbia. https://www.academia.edu/49546003/Case_Study_The_NotPetya_Campaign.

Sterman J. 2000. *Business Dynamics: System Thinking and Modelling for a Complex World*. Irwin McGraw-Hill.

Sterman JD. 2001. System dynamics modelling tools for learning in a complex world. *California Manage. Rev.* **43**: 8–25. https://e-tarjome.com/storage/panel/fileuploads/2019-03-09/1552121618_E11884-e-tarjome.PDF.

Sterman JD, Meadows D. 1985. STRATAGEM-2. *Simul. Games* **16**: 174–202.

Sterman J. 1992. Teaching Takes Off: Flight Simulators for Management Education “The Beer Game,” October 1992. Available online: http://web.mit.edu/jsterman/www/SDG/beergame.html (accessed on December 21, 2021).

Sterman J. 1989. Modeling managerial behavior: Misperceptions of feedback in a dynamic decision-making experiment. *Management Science* **35**(3): 321–339.

Sophos. 2023. 2023 Ransomware Report: Sophos State of Ransomware. https://www.sophos.com/en-us/content/state-of-ransomware.

Travelers. 2024. Travelers Risk Index Cyber Report 2023. https://www.travelers.com/resources/risk-index/2023-cyber-top-business-risk.

Tversky A, Kahneman D. 1973. Judgment under uncertainty: Heuristics and biases. *Oregon Institute Research Bulletin* **13**(1).

Vardham, R & Tonogbanua, L. 2024, Jan 02. How Many Cyber Attacks Happen Per Day in 2024?, Techjury.com. https://techjury.net/blog/how-many-cyber-attacks-per-day/.

Wang J. Neil M. & Fenton N. 2020. A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model, Computers & Security, Volume 89, February 2020, 101659. https://doi.org/10.1016/j.cose.2019.101659.

World Economic Forum and Partners. 2021, March 23. Principles for Board Governance of Cyber Risk, https://www.weforum.org/reports/principles-for-board-governance-of-cyber-risk/

Wolthuis R, Phillipson F, Rochat P, Ingen, B van, Zeijlemaker S & Gorter D. 2019. Quantifying Cyber security Risks. (article). TNO.

Wouters P, van Nimwegen C, van Oostendorp H, van der Spek, ED. 2013. A meta-analysis of the cognitive and motivational effects of serious games. *Journal of Educational Psychology* **105**: 249–265.

Zeijlemaker S, Pal R, Siegel M. 2024. Strengthening managerial foresight to defeat cyber threats. *AMCIS 2024 Proceedings*, August 15–17, Salt Lake City, Utah.

Zeijlemaker S, Hetner C, Siegel M. 2023. Four Areas of Cyber Risk That Boards Need to Address. https://hbr.org/2023/06/4-areas-of-cyber-risk-that-boards-need-to-address.

Zeijlemaker S, Siegel M. 2023. Capturing the dynamic nature of cyber risk: Evidence from an explorative case study [Conference session]. *Hawaii International Conference on System Sciences* (HICSS)–56, Hawaii.

Zeijlemaker S, Siegel M, Khan S, Goldsmith S. 2022. How to Align Cyber Risk Management with Business Needs. https://www.weforum.org/agenda/2022/08/how-to-align-cyber-risk-management-with-business-needs/.

Zeijlemaker S. 2022. Unraveling the dynamic complexity of cybersecurity: Towards identifying core systemic structures driving cybersecurity investment decision-making. Radboud University (342 pages) (S.l.: s.n.) Supervisor(s): Prof. Dr. EAJA Rouwette & Prof. Dr. M von Kutzschenbach. (Doctoral Thesis).

Zhang T, Antunes H, Aggarwal S. 2014. Defending connected vehicles against malware: Challenges and a solution framework. *IEEE Transactions on Industrial Technology* **1**(1): 10–21.