Capturing the Dynamic Nature of Cyber Risk: Evidence from an Explorative Case Study

S. Zeijlemaker
Cyber Security at MIT Sloan,
Sloan School of Management
szeijl@mit.edu

M. Siegel
Cyber Security at MIT Sloan,
Sloan School of Management
msiegel@mit.edu

Abstract

In this research, we developed a novel approach to enable a dynamic cyber risk management strategy as the dynamic nature of cyber risk is rarely considered in current decision support tools. Our explorative case study shows that many management challenges such as investment decisions, priority setting, and "shelf time" analyses can be continuously analyzed. Our research using system thinking and modelling provides valuable insights about these challenges to support current strategic decision-making practices and improve managerial learning. These insights enable management to identify and analyze the effectiveness of future cyber risk management strategies before implementing them.

Keywords: strategic cyber risk analysis, cyber risk management strategies, simulation, system dynamics, continuous risk management.

1. Introduction

During the last decade, multiple organizations emphasized the need for more adequate investments in cyber risk management strategies (Marks, 2021; EC, 2021). Despite this, organizations remain vulnerable to cyber threats, as evidenced by recent cyber threats that affected Kaseya (Kari, 2021), SolarWinds (Jibilian & Canales, 2021), and Colonial Pipeline (Turton & Mehrotra, 2021).

Meanwhile, cyber risk management frameworks, standards, laws and legislations, and other supportive tools have been evolving. For example, breach notification legislation, data protection acts, security directives, the ISO 27000 series, the NIST framework, MITRE Att&ck and D3fend, C2M2, OWASP, and CIS.

Although many approaches to strategic cyber risk management are available (Moore et al., 2016), as well as the knowledge about effective security management (Kwon & Johnson, 2014), defenders' security performance still lags the evolution of cyber threats and advancing skills of adversaries. This paper is about improving strategic cyber risk management by using simulation techniques.

2. Cyber risk and decision-making

Management needs to significantly improve cyber strategic and operational defense choices[1] to address the growing gap between offense and defense (SCAN, 2022; Kagubare, 2022). Executives and senior management use decision support tools for analyzing and managing cyber risks. For example, approaches for allocation and prioritization are based on adherence to frameworks (such as NIST, C2M2 etc.), positioning in comparative benchmarks, adherence to legislation and acting after suffered breaches (Moore et al., 2016).

Although some available tools and approaches can handle more complexity (Wang et al., 2020), they still have limitations (Woldhuis et al., 2019). They are static and thus do not account for the dynamic nature of cyber risk (Falco et al., 2019; Homeland Security 2018). The dynamic nature of cyber risk can be recognized in, for instance, evolving adversary tactics and skills, shifting organizational priorities, emerging security events, changing budgets, and new technology (Zeijlemaker, 2022). The complex dynamic nature of cyber risks cannot be covered by traditional risk management approaches (Lambert et al., 2013; Linkov et al., 2014).

To capture this nature of cyber risks in decision-making, we used a System Dynamics approach to develop a simulation tool that mimics the cyber risk management eco-system. The purpose of this is to explore how simulation techniques can augment the static approaches for cyber risk management decision - making. System Dynamics has rarely been used in the field of cyber risk (Jalili, 2019; Zeijlemaker, 2022).

[1] defense choices include identification, prevention, detection, response, and recovery (NIST 2018).

URI: https://hdl.handle.net/10125/103372
978-0-9981331-6-4

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 (Jalali et al., 2019; Armenia et al., 2018).

These insights can be used for feedback on the intended decisions and actions that are planned as a follow-up. A simulation shows the effectiveness of a strategy before making the necessary investments. These forward-looking simulations allow for continuous evaluation of future strategic cyber risks. So far, recent research has focused on security operations (Genge et al., 2015; Kannan, & Swamidurai, 2019), specific capabilities (Nazareth & Choi 2015) or advocate the need for quantitative strategic modelling (Xu, 2014; Medoh, & Telukdarie, 2022; Khan et al 2022).

2.1 To be in control of cyber risk

Cyber risk management frameworks conceptualize the interconnectedness of threat, risk, security measures, and consequences of impact (Graubart & Bodea, 2016; ISACA, 2015; NIST, 2018). In this context, the purpose of cyber risk management is threefold: (1) bringing the exposure of the organization to known and unknown threats to acceptable levels (Eling et al., 2021), (2) supporting the priority setting of the investments in the security program (Paté-Cornell et al., 2018), and (3) justifying resources and budgets that are allocated to the security function (Paté-Cornell et al., 2018; Moore et al., 2016). These acceptable levels are often conceptualized as being within the organization's risk appetite (Eling et al., 2021; COSO, 2004).

Risk management provides the concept of "being in control". An organization is in control if it has reasonable assurance of its capability to adjust its performance timely through its management control system when this performance is outside a predefined boundary (Paape, 2008; Strikwerda, 2005; COSO, 2004). These boundaries are often predefined by decision-makers and represent the risk the organization is willing to take, often referred to as risk appetite (Eling et al., 2021; COSO 2004).

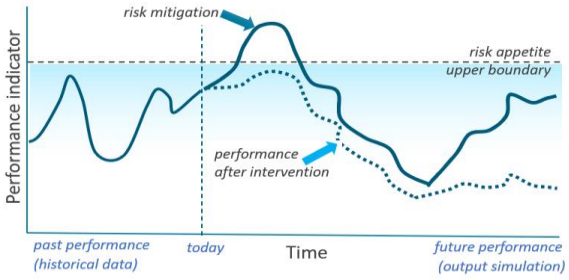

Figure 1. Dynamic risk management in terms of performance behavior over time (Zeijlemaker, 2022)

Figure 1 (Zeijlemaker, 2022) shows the past and future behavior of a performance indicator that is expected to go outside the risk appetite boundary under the current policies. Timely risk management policy interventions (risk mitigation) bring the performance within these boundaries (acceptable risk appetite). Another simulation run (performance after simulation in Figure 1) provides such assurance.

2.2 Dynamic cyber security capabilities

Organizations invest in security measures to limit the effect of cyber threats. These security measures can be seen as capabilities. A capability is the ability of the organization to prioritize and deploy its resources– people, processes, and technology– to deliver performance (Jalali et al., 2019; Teece, 2018). The dynamic nature of cyber risk requires organizations to rapidly reconfigure its resources for aligning the capabilities with the changing internal and external environment. For these dynamic capabilities speed and degree of alignment are essential (Teece, 2018).

In terms of cyber risk management investment, a decision about security capabilities involves two aspects: (1) the extent to which security capabilities can improve maturity or; (2) the extent to which security capabilities have sufficient resources to cope with current workload caused by the rapidly changing external and internal environment. Decision-makers are often biased to make decisions that yield immediate, easy-to-observe gains at the expense of long-term, hard to measure, capability maturity improvements (Sterman, 2001). What results is that organizations find themselves trapped "*in a downward spiral of eroding process capability, increasing work hours and less and less time for improvement*". (Repenning & Sterman, 2002, p. 282).

3. Model design and validation

System Dynamics is originated in the 1950s and grounded in system thinking and control theory. The method has been known for capturing and analyzing complex dynamics problems (Sterman, 2000; Duggan, 2016). Complex systems demonstrate counter-intuitive behavior that arise from the interactions between their agents and components (Sterman, 2006; Forrester, 1971).

Over the last 60 years the field had a strong methodological development (Martinez-Moyano & Richardson, 2013, Randers 2019). Besides limits to growth System Dynamics has many applications in business, social organizations, and society (Randers

2019), referred to as case studies (Randers 2019, Sterman 2003).

Our research was conducted with a European Fortune-500 organization using a System Dynamics group modelling approach. For the purpose of anonymization, this organization is called Smart Wealth Management Inc. (20,000 employees and 40,000 end-user devices and servers).

The group model process contributes to achieving consensus and shared understanding (Vennix, 1996). In this process, the modeler has a facilitating role and builds the model together with the experts. The experts with their issues and organizational focus have experience with the real eco-system (Ford & Sterman, 1998). We used three group sessions with highly experienced security consultants, business consultants, product owners, and behavioral security specialists with global domain responsibilities to construct the model. We used a phased model-building approach. The parameters for our model are based on open-source external data sources, scientific papers, and case study data. We used the Vensim software for building the model and SDM-Doc for documentation purposes.

The model structure has three important sub-model structures: (1) the lifecycle of a security capability, (2) the defense-in-depth approach, and (3) spillover effects. We explain the structures at an aggregated level because the model has over 350 variables and 7800 feedback loops. Mathematical details on model core structures can be requested from the authors.

3.1. The lifecycle of a security capability

A System Dynamics approach is well-known to analyze the aspect of a lifecycle of a capability (McAvoy et al., 2021) and is related to the capability trap (Repenning & Sterman, 2002). The systemic structure of the lifecycle of a security capability is visible in Figure 2.

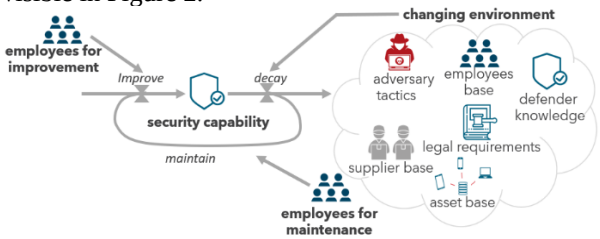

Figure 2. Security capability

Employees are needed to improve the maturity of a security capability from the present to the desired level. These employees integrate, build, and reconfigure resources –people, processes, and technology– to increase the maturity of the capability and deliver better security performance. Meanwhile, a daily workload needs to be handled, like emerging vulnerabilities that require patching, supplier onboarding, employee onboarding and training, management of changes and acting on emerging incidents. A lack of maintenance employees delays this workload and causes the maturity of the capability to decline because agreed controls and procedures are not properly executed.

Our model recognizes a four-tier maturity level structure ranging from no measures at all (Tier 1) to a highly sophisticated, strong, matured, and fully implemented capability for a large enterprise (Tier 4). This tiered maturity approach is like CIS, C2M2 or CMMC but can easily translated to other security frameworks. In our case study, we used Smart Wealth Management's internal capability assessment supplemented with their security resource assessment and IT security risk control reports. This information, complemented by interviews, was an important input to the parameters of the model and provided insights into effectiveness of security capabilities. We applied this approach to the following capabilities: asset management, vulnerability management, threat detection, identity and access management, workforce, incident response, service provider management, and network protection.

3.2 Defense-in-depth

The defense-in-depth approach has measures against the adversary across different organizational dimensions and if one measure fails, another will be in place to thwart an attack (Groat et al, 2012; NIST, 2015). The adversary launches attacks against the defender. Successful attacks evoke more attacks due to: (1) the adversary achieves his goals and continues to do this (Huang et al., 2019) and (2) conjugation effect (Baldwin et al., 2016), and (3) word-of-mouth effect mobilize more adversaries to attack (Zeijlemaker 2022). Prevented attacks contribute to adversaries' innovation (long-term effect) or attacking other targets (short-term effect) (Zeijlemaker 2022). For the defender, there is an opposite effect. The defender will improve its defenses when the attacker becomes successful (Martinez-Moyano et al., 2015) either reactively–after an observed successful attack–or proactively, based on observed emerging attack behavior (Böhme & Moore, 2016). The defender's improvement takes time due to the decision-making and implementation efforts. Our model recognizes four possible points of entry for the adversary: servers connected to the internet, compromised (user) accounts, end-users' email and web browsers, and unmanaged assets (MITRE 2018).

The adversary needs to circumvent multiple defensive measures and exploit multiple weaknesses to impact critical assets of the defender, wherein insecure behavior of unaware employees has a key role (BakerHostetler, 2016). Aware employees are essential

because they know how to protect themselves and how to react in the case of a cyberattack (Pattison et al., 2012; CIS, 2021; NIST, 2018). Although unaware employees can learn through mistakes, incidents, scheduled training, and knowledge-sharing sessions, their knowledge decays over time due to reasons such as security fatigue, knowledge decay in the workplace, or just forgetting problems and topics (Parkin et al, 2016; Cram et al, 2021). Besides, the adversary tries to fool employees by targeted phishing campaigns or sophisticated malicious emails, attachments, or websites.

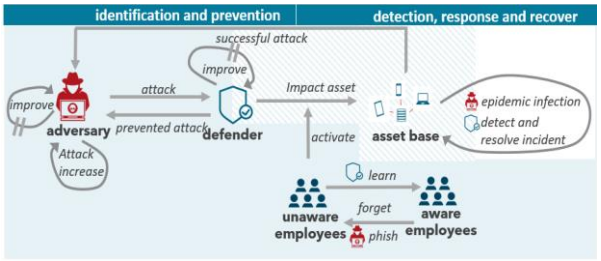

Figure 3. Defense-in-depth

Ultimately, the adversary may reach the asset base of the defender. In terms of cyber risk, assets go through four different stages (Jalili et al., 2019; Sepulveda Estay, 2021; Zeijlemaker, 2022): (1) susceptible assets that are compromised by the adversary become an unknown compromised asset, (2) after detection, unknown compromised assets become known compromised assets, (3) responsive actions by the defender mitigate the effects of the attack and become resolved assets, and (4) resolved assets are packed in production as susceptible assets. In this sequence, isolation is important for limiting adversary activities (Torres, 2014) because unknown compromised assets can compromise more susceptible assets due to lateral movement or automated epidemic malware properties (e.g., worms). The defense-in-depth approach is visualized in Figure 3.

3.3. The spillover effects

Spillover effects are related to the fundamental tension between efficiency and resilience (Hall et al., 2013). Resilience requires spare capacity, duplication of resources, loosely coupled systems, and layered defenses. Improving efficiency means eliminating them (Hall et al., 2013).

Consequently, there are limits to the effectiveness of incident response capacity (Wiik et al., 2005) and reducing this capacity may draw even more resources to this process (Van den Eede, 2006). When the limits of response and recovery capability are reached, the impact of the security incidents "spill over" to other IT teams because those teams need to contribute to solving the problems at hand as well. Initially, additional resources, including senior management, are temporarily moved from maintenance and support to incident response, but, ultimately, project delivery capacity can be drained too. A "spillover" effect has an enormous impact because staff performance is harmed by switching tasks (Hamann et al., 2013), working harder (Sterman, 2000), and working longer (Sterman, 2000) under pressure. The spillover effect is visualized in Figure 4.

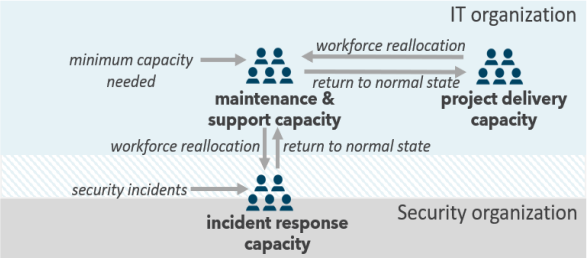

Figure 4. Spillover effects

3.4 Model validation

Over the years System Dynamics evolved in providing strong methods to model validation (Forrester & Senge, 1980; Barlas, 1996; Sterman, 2000).

First, we had two validation sessions with security architects where the boundary and structure of the model were discussed and accepted. A part of these sessions was detailed model walk-throughs based on real-world security incidents as well as model structure cross-checks with relevant enterprise architecture design documents. These documents give insights into the design and coherence between different components of the organization–people processes and technology and how there are used for strategic intent (Jonkers et al., 2006; IEEE 1471, 2000**; Sowa & Zachman, 1992).** Strong alignment (Warren, 2015) with enterprise architecture enables re-usability of the model (Sowa & Zachman, 1992). In the case of model re-usage, most adaptations of the model to different organizations should be resolved by changing parameters.

Theil statistics	Real World Data vs Model
Theil's U (<1)	0.56
Theil's inadequate statistics (add up to 1)	
Um (average)	0.39
Us (systemic error)	0.01
Uc (noise)	0.6

Figure 5. Reference mode versus model output

Second, the model can replicate the reference mode, a 12-month trend of the number of security incidents of our case study organization. Figure 5 shows the historical data of the organization, the model output, and evaluation statistics (used Theil's U and Theil

Inadequate Statistics). Theil's U is below 1 which indicates that the forecast provided by the model is accurate (Theil, 1966). Theil Inadequate Statistics shows that the difference between model and real data is mostly explained by noise (Uc = 0.6) and limitedly by errors in the model structure (Us = 0.1) or errors in model parameters (Um = 0.3) (Sterman, 2000). The high level of noise can be explained by the emerging and uncertain nature of security incidents.

4. Results

In this section, we explain the reference mode run of Smart Wealth Management Inc., which is a 60-month forecast based on the existing cyber risk management strategy. Thereafter, different subsections focus on exposing threats to the organization, priority setting in the security program, and reflection on the case study.

4.1. Reference mode run

Figure 6 shows three output graphs on the reference mode run. The "security resources required" graphs are a forecast of the number of security resources needed. After the major breach that occurred in month 40, additional security resources are needed for incident response and recovery. The "security incidents" graph shows the number of non-aggregated security incidents per month. The spikey nature of incidents is visible. The "resource state diagram" graph shows how IT, and security resources evolve over time. The spillover effects are visible where project delivery resources are reallocated to maintenance & support teams. The additional response and recovery workload are represented by the higher resource levels of maintenance and support. Each graph contains 12 months of historical data and 60 months of forecasted data. We call this run base because, in the scenario analyses, we will compare this run to the outcome of other simulated runs.

In Figure 6, the "resources state diagram" graph shows that spillover effects start around month 20 and occur more frequently and strongly with time. This suggests a limited 'shelf-time' for the current cyber risk management strategy. The "security incidents" graph indicates a major breach around month 40, impacting approximately 25% of the asset base. This suggests that Smart Wealth Management Inc. is susceptible to advanced cyberattacks with epidemic properties or significant major lateral movement. When looking at the risk appetite line, the number of incidents crossed that boundary three times. This suggests that the current cyber risk management strategy is too risky. The risk appetite line has been established based on interviews with senior management. They tolerated a small increase because of continuous digitalization and growth in adversarial activities.

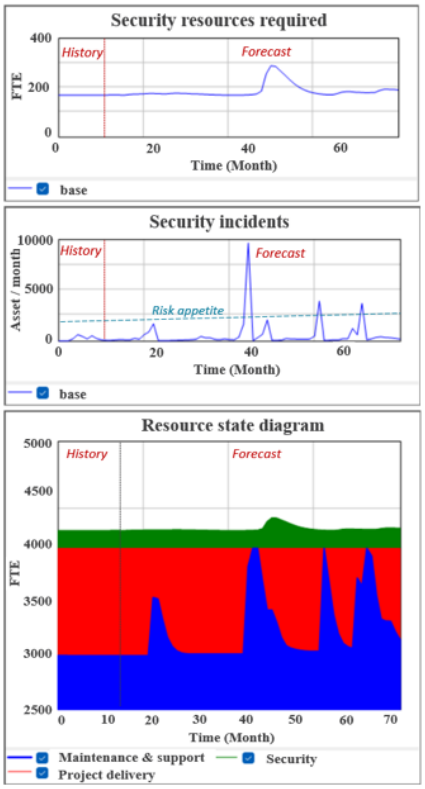

Figure 6. Evaluation graphs reference mode

The "security resources required" graph shows an oscillating pattern of staff, which suggests that capability decline takes place, and some improvement investments are made after impacting breaches. Additionally, a major increase in resources after month 40 is visible.

4.2. Supporting priority setting

Table 1 shows the decisions taken per alternative scenario for two cases, both involve setting priorities for investing in security capabilities. The following cases are described similar as strategic dialogues with senior and executive management.

4.2.1. Case 1: prioritizing investments

Following an assessment, Smart Wealth Management Inc. identified both incident response and asset management as requiring improvement which start over 12 months. In such a situation, management has three options: (1) invest in asset management (Scenario 1), (2) invest a bit in both (Scenario 2), or (3) invest in incident response (Scenario 3). Figure 7 shows the results of the simulation of Scenarios 1–3 and an explanation is provided above the figure.

Security Capability with intended maturity scores (1 to 4)	Base (section 4.2)	Case 1: Prioritizing			Case 2: Learn and segment		
		Scenario 1. (Section 5.2.1)	Scenario 2. (Section 5.2.1)	Scenario 3. (Section 5.2.1)	Scenario 4. (Section 5.2.2)	Scenario 5. (Section 5.2.2)	Scenario 6. (Section 5.2.2)
Network protection	3	3	3	3	3	3	3*
Asset management	2	3	2.5	2	3	3	3
Vulnerability management	3	3	3	3	3	4	4
Threat detection	3	3	3	3	3	3	3**
Response	2	2	2.5	3	3	4	4
3rd Party management	2	2	2	2	2	2	2
Identity and access management	2	2	2	2	2	2	2
Workforce management	3	3	3	3	3	3	3

Table 1. Cyber security maturity scores per scenario
* = additional efforts in network segmentation. ** = additional efforts in anomaly detection

Investment in incident response (Scenario 3) contributes to faster and better response processes but does not significantly lower the number of the incidents. Investment in asset management (Scenario 1) lowers the number of vulnerabilities that can be exploited by those assets. Consequently, this lowers the number of incidents because fewer unmanaged assets can be used as an entry point for the adversary. When doing a little bit of both, the effects of both scenarios are averaged. Therefore, the "security resources required" graph and the "cumulative security incidents" graph in Figure 7 show that investing in asset management yields the best results (the lowest number of incidents and resources required). The "resource state diagram" graph shows the favored situation (Scenario 1). This figure shows that spillover effects become visible from month 40. This is a delay of 20 months compared to the base run (see Figure 6).

4.2.2. Case 2: proactive learning and segmentation

Smart Wealth Management Inc. has correctly stabilized and prioritized the roadmap, which means that Scenario 1 will be implemented. Around month 40, the cyber risk management strategy is not stable anymore because security incidents go up and "spillover" effects appear around month 40, as shown in Figure 8. The next challenge is resolving this issue. Improvement will take place after 10 months in the simulation.

Management has four options to address these issues: (1) contribute to focusing on incident resolution (based on the optimal outcome of case 1), (2) invest in incident evaluation (Scenario 4), (3) focus on understanding threat environment (Scenario 5), and (4) hunt for abnormal behavior based on an understanding of the threat environment (Scenario 6).

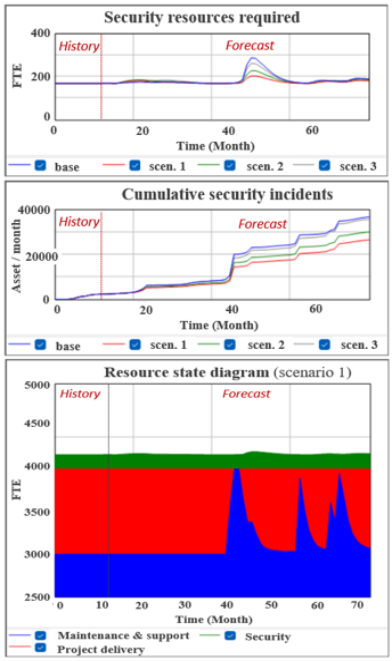

Figure 7. Evaluation graphs case 1

Figure 8 shows the results of the simulation of Scenarios 4–6.

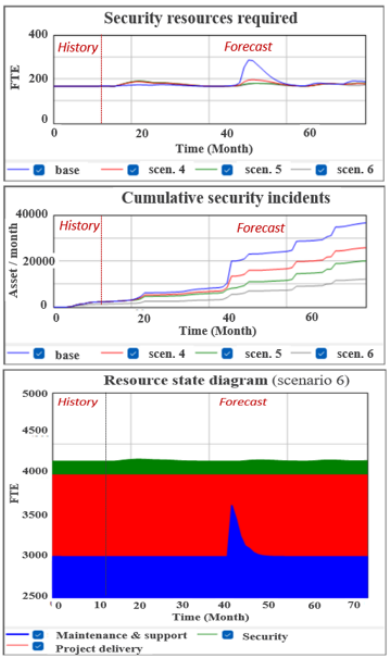

Figure 8. Evaluation graphs case 2

In Figure 8, the "security resources required" graph and the "cumulative security incidents" graph show the best results are realized by Scenario 6: "hunting for anomalies based on an understanding of the threat environment".

A focus on incident resolution implies 'working harder' and yields similar output as Scenario 1. Scenario

1 is not visible in Figure 8 (see Figure 7 for Scenario 1). Investing in incident evaluation (Scenario 4) shows some improvements. Incident evaluation means that post-mortem analysis is executed after security incidents and defense improvements are done as follow-up. This is called reactive learning, because these improvements prevent similar incidents from happening again. Reactive learning yields higher use of resources because the defender must resolve the incident, recover from its impact, and invest in defense improvements. Understanding the threat environment (Scenario 5) is proactive learning. This is done using threat intelligence, the synthesis of information detailing potential threats with a solid understanding of network structure, operations, and activities (Chismon & Ruks, 2015). Proactive learning contributes to defense improvement (Martinez-Moyano et al., 2015), near online real-time threat assessment (Riesco & Villagrá, 2019), and near online real-time event-evaluation (Riesco & Villagrá, 2019). It contributes to a higher number of prevented attacks because the defender already anticipates to the attack before it happens. Compared to Scenario 5, Scenario 6 had an additional focus on anomaly detection and segmentation. Anomaly detection involves the use of algorithms in multi models and machine learning to identify abnormal communication on the network, between devices, within devices, and with malicious domains (Sanzgiri & Dasgupta, 2016). Anomaly detection contributes to the early detection of lateral movement and attacks with epidemic properties. Segmentation provides the means to isolate devices and limits the effects of lateral movement and the epidemic properties of an attack (Johansson et al., 2020). Therefore, the magnitude of occurred security incidents in month 40 is very low. The "resource state diagram" graph in Figure 8 shows the favored situation (Scenario 6). This figure shows only one occasion of spillover effects.

4.2.3 Reflection on the case study

A part of the case study was sharing insights with stakeholders about how the systemic structure relevant to cyber risk management causes the outcome of several scenarios. Important input from our case study was based on capability assessment (static tool). The reference model run showed that the current cyber risk management strategy was not future proof. Eventually, the current strategy did not contribute to the perceived risk reduction (static tool). Our case study addressed different common managerial challenges such as priority setting in the security program through scenario analysis. We were able to simulate a wide range of strategies and showed which contributed the most to effective and efficient cyber defense and security program choices. These insights were not available from the current reporting and assessments (which were used as input for our case study).

5. Discussion and future research

Our simulation results provide insights into threats and the notion of the long-term sustainability of its current cyber risk management strategy. Although this strategy was perceived as sustainable, our analysis provides ideas for future improvements. We believe that this difference between perception and simulation results can be explained by the dynamic complex nature of cyber risk management. People have difficulties in making decisions in dynamic complex environments and tend to use heuristics (simple mental rules) to make decisions in such environments (Grossklags & Reitter, 2014; Sterman, 1989). Heuristics usually help regarding short-term objectives (Rosoff et al., 2013; Tversky & Kahneman, 1973). Heuristics often lead to biased decisions regarding gain and loss estimations (Kahneman & Tversky, 1979; Kahneman, 2011), and eventually, event-driven decisions or reactive approaches may generate problems for tomorrow (Sterman, 2001). Our simulation results contributed by challenging the perceived risk reduction effectivity and identified cyber risks that were wrongly considered as distant and far away for the case study organization.

This is why we advocate augmenting the current cyber risk management decision-support tools with system-dynamics-based simulation techniques. Especially since we used inputs from commonly used support tools for cyber risk management (Moore et al., 2016).

In addition, where Paape (2008), Strikwerda (2005), and COSO (2004) conceptualize "being-in-control," we use a System Dynamics approach and visualization techniques to operationalize this concept and incorporate risk management into the forward-looking aspect of our analysis. Our graphs show accepted behavior (risk appetite) and simulate the behavior of performance indicators. The wide range of simulated strategies shows what strategies contribute to risk mitigation by bringing the simulated behavior of these performance indicators within the boundaries of the accepted behavior.

The purpose of our case study is to demonstrate how cyber risk management functions can address the dynamic nature of cyber risk at an executive level to improve their cyber risk strategy design.

Three security capabilities should be considered more in the future. In our study, the security capabilities related to 3rd party management, security software development, and encryption are limitedly considered in our analysis.

This case study is also limited to one anonymized case. Yet, we advocate the re-usability of our simulation

model based on our approach and level of modeling. It would be interesting to validate this assumption in subsequent research.

6. Conclusion

Major security incidents drove us to the question of how the dynamic nature of cyber risk can be effectively captured in decision-making?

We used a System Dynamics approach to capture the system structure relevant to the dynamic nature of cyber risk, and we simulated a wide range of strategies. This approach reused much knowledge, data, and insights that were already present in the case study organization and used in the current static cyber risk management strategy process. Therefore, we advocate that our approach augmented the existing cyber risk management decision support tools.

We can simulate a wide range of strategies and allow managers to learn, experiment, and identify counter-intuitive strategies for maximizing the impact of cyber risk management decisions. We also provide the means for continuous evaluation of cyber risk. Our research showed how simulated strategies may be performed for the future and address relevant and common managerial challenges. Important lessons from these simulations are the following:

(1) Obvious solutions do not always yield the best and most sustainable impact.
(2) Proactive learning is critical to organizational effectiveness.
(3) It is critical to anticipate spillover (2nd order) effects.

Insights from our study are important for proactive cyber risk management, continuous cyber risk management, and making sustainable cyber risk management strategies for all organizations. In addition, simulations have been shown to provide feedback about the effectiveness of intended cyber risk management strategies before making large investments in these strategies. This has been confirmed for our case study by the received managerial feedback:

"*Dynamic modeling showed the impact of strategic decisions before making large investments. It helps me to determine what to invest, where, and when.*"

"*It sure made my job easier to explain investing in security to the managing board*"

"*Business dynamic modelling has the ability to simplify complex problems and make them easy to understand*".

Acknowledgement

This work is co-funded by "Fondo Europeo di Sviluppo Regionale Puglia POR Puglia 2014 – 2020 – Asse I – Obiettivo specifico 1a – Azione 1.1 (RS) - Titolo Progetto: Suite prodotti Cybersecurity e SOC" and BV TECH S.p.A.

This work is co-funded by Cybersecurity at MIT Sloan (MIT CAMS https://cams.mit.edu)

References

Armenia, S., Ferreira Franco, E., Nonino, F., Spagnoli, E., Medaglia, C.M., (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.

McAvoy, S., Grant, T., Smith, C., & Bontinck, P., (2021). Combining Life Cycle Assessment and System Dynamics to improve impact assessment: A systematic review, Journal of Cleaner Production 315 (2021) 128060, https://doi.org/10.1016/j.jclepro.2021.128060.

Baldwin, A., Gheyas, I., Ioannidis, C., & Williams, J. (2016). Contagion in security attacks, Journal of Operational Research Society.

BakerHostetler. (2016). Is your organization compromise ready? 2016 Data Security Incident Response Report. Retrieved from http://f.datasrvr.com/fr1/516/11618/BakerHostetler_2016_Data_Security_Incident_Response_Report.pdf

Barlas, Y. (1996). Formal aspects of model validity and validation in system dynamics, System dynamics Review, 12(3), 183–210.

Böhme, R. & Moore, T. (2016). The iterated weakest link, a model of adaptive security investment. Journal of Information Science, 7(2).

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

Chismon, D., & Ruks, M. (2015). Threat intelligence: Collecting, analysing, evaluating, MWR Security, CCERt-UK and CPNI, 2015IEE.

COSO (2004). *Enterprise Risk Management Integrated Framework*. Committee of Sponsoring Organizations of the Treadway Commission, USA.

Cram, W.A., Proudfoot, J.G. & D'Arcy, J. (2021). When enough is enough: Investigating the antecedents and consequences of information security fatigue. Inf Syst J. 2021;31:521–549, DOI: 10.1111/isj.12319.

Duggan, J. (2016). An introduction to system dynamics system dynamics modeling with R. Springer International Publishing.

Van Den Eede, G., Muhren, W., Smals, R., and Van de Walle, B., (2006). IS Capability for Incident Management and the DERMIS Design Premises. Proceedings of the 3rd International ISCRAM Conference (B. Van de Walle and M. Turoff, eds.), Newark, NJ (USA), May 2006.

Eling, M., McShane, M., & Nguyen, T., (2021). Cyber risk management: History and future research directions. Risk Manag Insur Rev.; 24: 93– 125. https://doi.org/10.1111/rmir.12169.

EC (2021). Shaping Europe's digital future, read on January 14th, 2022, retrieved from: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies .

Falco, G., Eling, M., Jablanski, D., Miller, V., Gordon, L. A., Wang, S., Schmit, J., Thomas, R., Elvedi, M., Maillart, T., Donavan, E., Dejung, S., Weber, M., Durand, E.,

Nutter, F., Scheffer, U., Arazi, G., Ohana, G., Lin, H. (2019, June 3–4). *A research Agenda for cyber risk and cyber insurance*. The 2019 Workshop on the Economics of Information Security, Boston.
Ford, D. N., & Sterman, J. D. (1998). Expert knowledge elicitation to improve formal and mental models. System Dynamics Review, 14(4), 309–340.
Forrester, J. W. (1971). Counterintuitive behaviour of social systems. Technology Review, 73, 53–68.
Forrester, J., & Senge, P. (1980). Tests for building confidence in system dynamics models. Studies in the Management Sciences, 209–228.
Genge, B., Kiss, I., & Haller, P. (2015). A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures. International Journal of Critical Infrastructure Protection, 10, 3-17.
Grossklags J, & Reitter R. (2014). How task familiarity and cognitive predispositions impact behaviour in a security game of timing. IEEE 27th Computer Security Foundations Symposium.
Graubart, R., & Bodea, D., (2016). The Risk Management Framework and Cyber Resiliency, The MITRE Corporation. Case No. 16-0776.
Groat, S., Tront, J. $ Marchany, R. (2012) Advancing the defense in depth model. 2012 7th International Conference on System of Systems Engineering (SoSE), 2012, pp. 285-290, doi: 10.1109/SYSoSE.2012.6384127.
Hamann, H., Karsai, I. & Schmickl, T, (2013). Time Delay Implies Cost on Task Switching: A Model to Investigate the Efficiency of Task Partitioning. Bull Math Biol 75, 1181–1206 (2013). https://doi.org/10.1007/s11538-013-9851-4.
Homeland Security (2018). *Cyber Risk Economics Capability Gaps Research Strategy*. DOI: 10.23721/1460960.
Huang K., Siegel M., & Madnick, S. (2019). Systematically understanding the cyber-attack business: A survey. ACM Computing Surveys, Volume 51, Issue 4,Article No.: 70, pp 1–36. https://doi.org/10.1145/3199674.
IEEE 1471 (2000). Defining architecture [online], ISO/IEC/IEEE 42010 Website. http://www.iso-architecture.org/ieee-1471/defining-architecture.html. Read in May 2016.
ISACA (2015). CISM review manual 2015. ISACA.
Jalali, M.S., 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.
Jibilian, I., & Canales, K., (2021, April 15th). The US is readying sanctions against Russia over the SolarWinds cyber-attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal, Business Insider, read on 10 January 2022, retrieved from: https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12?international=true&r=US&IR=T.
Johansson, D., Jönsson, P., Ivarsson, B. & Christiansson, M. (2020). Information Technology and Medical Technology Personnel´s Perception Regarding Segmentation of Medical Devices: A Focus Group Study, Healthcare 2020, 8, 23; doi:10.3390/healthcare8010023.
Jonkers, H., Lankhorst, M. M., Ter Doest, H. W. L., Arab, F., Bosma, H., & Wieringa, R. J., (2006). Enterprise architecture: Management tool and blueprint for the organization. *Information Systems Frontiers, 8,* 63–66.
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).
Kannan, U., & Swamidurai, R. (2019). Empirical Validation of System Dynamics Cyber Security Models. In 2019 SoutheastCon (pp. 1-6). IEEE.
Kari, P., (2021, July 23rd). Tech firm hit by giant ransomware hack gets key to unlock victims' data, the guardian, read on 10 January 2022, retrieved from https://www.theguardian.com/technology/2021/jul/22/ransomware-attack-kaseya-key-hacking.
Kagubare, I., (2022, June, 13). Top cyber official says transformation needed in cyberspace, The Hill. https://thehill.com/policy/cybersecurity/3521797-top-cyber-official-urge-for-transformation-in-cyberspace/.
Khan, S. K., Shiwakoti, N., & Stasinopoulos, P. (2022). A conceptual system dynamics model for cybersecurity assessment of connected and autonomous vehicles. Accident Analysis & Prevention, 165, 106515.
Kwon, J., & Johnson E. M. (2014). Proactive versus reactive security investments in the healthcare sector, *MIS Quarterly 2014, 38*(2).
Lambert, J.H., Keisler, J.M., Wheeler, W.E. et al., (2013). Multiscale approach to the security of hardware supply chains for energy systems. Environ Syst Decis 33, 326–334 https://doi.org/10.1007/s10669-013-9465-2.
Linkov, I., Bridges, T., Creutzig, F., Decker, J., Fox-Lent, C., Kröger, W., … Thiel-Clemen, T. (2014). Changing the resilience paradigm. Nature Climate Change, 4(6), 407–409.
Marks, J., (2021, November 2nd). Cybersecurity funding is at stake in Democrats' spending battles, The Washington Post, read on January 14th, 2022, retrieved from: https://www.washingtonpost.com/politics/2021/11/02/cybersecurity-funding-is-stake-democrats-spending-battles/)
Martinez-Moyano, I.J., Morrison, D., & Sallach, D. (2015). Modeling Adversarial dynamics. Proceedings of the 2015 Winter Simulation Conference, 2412–2423.
Martinez-Moyano IJ, Richardson IJG (2013) Best practices in system dynamics modelling. Syst Dyn Rev 29(2):102–123.
Medoh, C., & Telukdarie, A. (2022). The Future of Cybersecurity: A System Dynamics Approach. Procedia Computer Science, 200, 318-326.
MITRE (2018). MITRE ATT&CK, Initial Access, ID: TA0001, Created: 17 October 2018, Last Modified: 19 July 2019. https://attack.mitre.org/versions/v10/tactics/TA0001/
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.

Nazareth, D. L., & Choi, J. (2015). A system dynamics model for information security management. Information and Management, 52(1), 123–134.
NIST (2018, April). Cyber-security Framework Version 1.1. Framework Documents, NIST. https://www.nist.gov/cyberframework/framework.
NIST (2015, April). National Institute of Standards and Technology Special Publication 800-161, Natl. Inst. Stand. Technol. Spec. Publ. 800-161, 282 pages (April 2015), CODEN: NSPUE2 http://dx.doi.org/10.6028/NIST.SP.800-161.
Paape, L. (2008). 'In control' statements: Fried air or a phenomenon to be cherished? oration, Nyenrode Business Universiteit.
Parkin, S., Krol, K., Becker, I., & Sasse, M. A. (2016). Applying cognitive control modes to identify security fatigue hotspots. In Twelfth Symposium on Usable Privacy and Security (SOUPS 2016).
Paté-Cornell, M.E, Kuypers, M., Smith, M., Keller, P., (2018). Cyber risk management for critical infrastructure: a risk analysis model and three case studies, Risk Anal., 38 (2) (2018), pp. 226-241.
Pattison, M., Jerram, C., Parson, K., McCormac, A., & Butavicius, M. (2012). Why do some people manage phishing e-mails better than others? Information Management & Computer Security, 18–28.
Randers, J. (2019). The great challenge for system dynamics on the path forward: implementation and real impact. System Dynamics Review, 35(1), 19–24. https://doi.org/10.1002/SDR.1623.
Repenning, N. P., & Sterman, J. D. (2002). Capability traps and self-confirming attribution errors in the dynamics of process improvement. Administrative Science Quarterly, 47, 265–295.
Riesco, R., Villagrá, V. A. (2019). Leveraging cyber threat intelligence for a dynamic risk framework. *Int. J. Inf. Secur. 18*, 715–739. https://doi.org/10.1007/s10207-019-00433-2.
Rosoff, H., Cui, J., & John, R.S., (2013). Heuristics and biases in cyber security dilemmas. Environment Systems and Decisions 33, 517–529. https://doi.org/10.1007/s10669-013-9473-2.
Sanzgiri, A., & Dasgputa, D. (2016). *Classification of insider threat detection techniques.* Proceedings of the 11th Annual Cyber and Information Security Research Conference, Article No. 25, Oak Ridge TN USA April 5 – 7.
SCAN (2022), Cyber Security Assessment Netherlands 2022, National Coordinator Terrorism and Security, Ministry of Justice. https://english.nctv.nl/documents/publications/2022/07/04/cyber-security-assessment-netherlands-2022.
Sepulveda Estay, D., (2021). A system dynamics, epidemiological approach for high-level cyber-resilience to zero-day vulnerabilities, in Journal of Simulation, February 2021, DOI: 10.1080/17477778.2021.1890533.
Sowa, J. F., & Zachman, J. A. (1992). Extending and formalizing the framework for information systems architecture. IBM Systems Journal, 31(3). IBM Publication G321-5488.
Sterman, J. (2006). Learning from evidence in a complex world. Public Health Matters, 96(3).
Sterman, J. (2003). System Dynamics: Systems Thinking and Modeling for a Complex World, Working Paper, ESD Working Papers;ESD-WP-2003-01.13-ESD Internal Symposium.
Sterman, J.D., (2001). System dynamics modeling: tools for learning in a complex world. California Manage. Rev. 43, 8–25.
Sterman, J. (2000). Business Dynamics: System thinking and modelling for a complex world. Irwin MC Graw-Hill.
Sterman, J. (1989). Modeling managerial behaviour: Misperceptions of feedback in a dynamic decision-making experiment. Management Science, 35(3), 321–339.
Strikwerda, J. (2005). To be or not to be: In control. *Controllers Magazine*, *19*(4), 38–42.
Teece, D.J., (2018). Business models and dynamic capabilities. Long Range Planning 51 (2018) 40-49, http://dx.doi.org/10.1016/j.lrp.2017.06.007.
Theil, H. (1966). *Applied Economic Forecasting*. Rand McNally.
Torres, A., (2014). Incident Response: How to Fight Back, A SANS Survey. 2014 SANS™ Institute.
Turton, W., & Mehrotra, K., (2021, June 4th). Hackers Breached Colonial Pipeline Using Compromised Password. Read on January 10th, 2022. Retrieved from: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password
Tversky, A., & Kahnema, D. (1973). Judgement under uncertainty: Heuristic and biases. Oregon Institute Research bulletin, 13(1).
Vennix, J.A.M. (1996). Group Model Building, facilitating team learning using system dynamics. John Wiley & Sons ltd.
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.
Warren, K. (2015). Strategy dynamics essentials. Createspace Independent Publishing Platform, 2nd edition, 2015.
Wiik, J., & Gonzales, J.J., (2005). Limits to Effectiveness in Computer Security Incident Response Teams, 23rd International Conference of the System Dynamics Society. The System Dynamics Society, Boston, MA.
Wolthuis, R., Phillipson, F., Rochat, P., Ingen, B. van, Zeijlemaker, S. & Gorter, D. (2019). Quantifying Cyber security Risks. (article). TNO.
Xu, S. (2014). Cybersecurity dynamics. In Proceedings of the 2014 Symposium and Bootcamp on the Science of Security (pp. 1-2).
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 pag.) (S.l.: s.n.) Supervisor(s): prof. dr. E.A.J.A. Rouwette & prof. dr. M. von Kutzschenbach.