AGENT BASED MODELING

OF THIRD-PARTY ENTERPRISE CYBERSECURITY

MUHAMMED YUSUF AKÇAKAYA

BOĞAZİÇİ UNIVERSITY

2024

AGENT BASED MODELING

OF THIRD-PARTY ENTERPRISE CYBERSECURITY

Thesis submitted to the

Institute for Graduate Studies in Social Sciences

in partial fulfillment of the requirements for the degree of

Master of Arts

in

Management Information Systems

by

Muhammed Yusuf Akçakaya

Boğaziçi University

2024

Agent Based Modeling of Third-Party Enterprise Cybersecurity

The thesis of Muhammed Yusuf Akçakaya

has been approved by:

Prof. Bilgin Metin
(Thesis Advisor) _____

Prof. Bertan Yılmaz Badur _____

Assoc. Prof. Mehmet Nafiz Aydın
(External Member) _____

September 2024

DECLARATION OF ORIGINALITY

I, Muhammed Yusuf Akçakaya, certify that

- I am the sole author of this thesis and that I have fully acknowledged and documented in my thesis all sources of ideas and words, including digital resources, which have been produced or published by another person or institution;
- this thesis contains no material that has been submitted or accepted for a degree or diploma in any other educational institution;
- this is a true copy of the thesis approved by my advisor and thesis committee at Boğaziçi University, including final revisions required by them.

Signature.....

Date.....

ABSTRACT

Agent Based Modeling of Third-Party Enterprise Cybersecurity

This thesis explores the use of Agent-Based Models (ABMs) to simulate cybersecurity risks within third-party relationships, an increasingly critical area in modern enterprise environments. As businesses rely more on external vendors for essential functions, their cybersecurity exposure grows, often introducing complex and unpredictable risks. The study first provides a comprehensive review of Third-Party Cyber Risk Management (TPCRM), identifying key challenges organizations face in mitigating cybersecurity threats originating from third parties. These challenges include high complexity, lack of visibility and control, and resource constraints. The study also identifies recommendations and best practices for TPCRM programs including conducting due diligence, continuous monitoring, and having strong contracts. Using the findings from this review, the thesis develops an ABM to simulate real-world scenarios involving third-party cyber risks. The model, designed in the NetLogo platform, is created using the challenges and best practices identified in the literature. By representing third-party companies, cyber attackers, and the primary organization as agents, the model explores how these entities interact and how effective risk management strategies can prevent breaches or minimize their impact. The study highlights how organizations can balance prevention and recovery costs in TPCRM. The results provide practical insights into optimizing cybersecurity measures for organizations of varying sizes and complexities, offering a tool to enhance the management of protection measures against growing cyber threats.

ÖZET

Üçüncü Taraf Kurumsal Siber Güvenliğin Ajan Bazlı Modellemesi

Bu tez, üçüncü taraf ilişkilerinde siber güvenlik risklerini simüle etmek için Ajan Tabanlı Modellerin (ABM) kullanımını incelemektedir. Modern organizasyonlarda giderek kritik hale gelmekte olan üçüncü taraf siber risk yönetimi, organizasyonların temel işlevler için dış tedarikçilerle çalışmasından doğan siber güvenlik riskleri ile ilgilenmektedir. Çalışma, ilk olarak Üçüncü Taraf Siber Risk Yönetimi'ni (TPCRM) kapsamlı bir şekilde gözden geçirerek, organizasyonların üçüncü taraflardan kaynaklanan siber güvenlik tehditlerini yönetmede karşılaştıkları zorlukları belirlemektedir. Bu zorluklar, yüksek karmaşıklık, görünürlük ve kontrol eksikliği ile kaynak kısıtları gibi unsurları içermektedir. Bu zorlukların yanında, literatürde organizasyonların alabileceği önlemler ve en iyi uygulamalar taranmış ve en sık önerilen pratikler durum tespiti yapılması, etkileşimlerin izlenmesi, ve güçlü sözleşmeler kurulması olarak tespit edilmiştir. Bu incelemeden elde edilen bulgular kullanılarak, üçüncü taraf siber risk senaryolarını simüle etmek amacıyla bir ABM geliştirilmiştir. NetLogo platformunda tasarlanan model, literatürde tespit edilen zorlukları ve en iyi uygulamaları test etmektedir. Bu çalışma, işletmelerin TPCRM'de önleme ve iyileştirme maliyetleri arasında nasıl bir denge kurabileceğini vurgulamaktadır. Sonuçlar, çeşitli büyüklük ve karmaşıklığa sahip organizasyonlar için siber güvenlik önlemlerinin optimize edilmesine yönelik pratik bilgiler sunmakta ve artan siber tehditlere karşı alınacak önlemlerin yönetimi konusunda bir araç sağlamaktadır.

ACKNOWLEDGMENTS

First and foremost, I would like to express my deepest gratitude to my thesis advisor, Prof. Bilgin Metin, for his invaluable guidance, support, and patience throughout this research. This thesis would not have been possible without him.

Special thanks to Prof. Bertan Yılmaz Badur and Assoc. Prof. Mehmet Aydın for their constructive criticism, which was incredibly helpful in improving the quality of this thesis.

I would also like to thank Dr. Meltem Mutlutürk for her support and valuable feedback, particularly regarding the agent-based model.

I am grateful to the Management Information Systems department for creating an environment conducive to research and for giving me the resources necessary for this work, and to The Institute for Graduate Studies in Social Sciences, for their support and guidance for the whole process.

I want to mention my dear friend and roommate, Mustafa Küçük, for without his presence, this thesis might have been completed much sooner.

Finally, I thank my family. Their countless unspoken contributions have shaped who I am today.

Thank you all for making this possible.

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION 1

1.1 Third-party cyber risk management and cyber supply chain risk management 4

1.2 Third-party caused breach cases 8

1.3 Agent-based modeling 11

CHAPTER 2 SYSTEMATIC LITERATURE REVIEW METHODOLOGY 13

2.1 Research method 13

2.2 Review protocol 13

2.3 Inclusion and exclusion criteria 15

2.4 Search strategy 15

2.5 Study selection process 16

2.6 Data extraction and synthesis 16

2.7 An overview of the publication sources 17

2.8 Temporal view of the sources 17

CHAPTER 3 FINDINGS FROM THE LITERATURE REVIEW 19

3.1 RQ 1: What are the primary studies on third-party cybersecurity risk management, and which research themes have been addressed in the literature? . 19

3.2 RQ 2: What are the critical challenges to address for effective third-party cybersecurity risk management in enterprise environments? 22

3.3 RQ 3: What are the best practices for an organization to manage third-party cybersecurity risks? 25

3.4 RQ 4. How can agent-based models be used to simulate third-party cyber risks? 29

CHAPTER 4 ANALYSIS OF LITERATURE REVIEW FINDINGS 31
CHAPTER 5 DEVELOPMENT OF AN AGENT-BASED MODEL FOR THIRD-PARTY CYBERSECURITY 42
5.1 Agent-based modeling tool: NetLogo 43
5.2 Proposed model 44
5.3 Agent-based model parameters and controls 49
5.4 Case study test scenarios 63
5.4.1 Scenario 1, complexity impact on cyber risk exposure 64
5.4.2 Scenario 2, risk appetite and security posture 65
5.4.3 Scenario 3, control level effectiveness and cost-benefit analysis 66
5.4.4 Scenario 4, the effectiveness of integrated control strategies 66
CHAPTER 6 SIMULATION RESULTS AND ANALYSIS 68
6.1 Scenario 1, complexity impact on cyber risk exposure 68
6.2 Scenario 2, risk appetite and security posture 70
6.3 Scenario 3, control level effectiveness and cost-benefit analysis 71
6.4 Scenario 4, the effectiveness of integrated control strategies 73
CHAPTER 7 DISCUSSION OF ABM SIMULATION FINDINGS 76
CHAPTER 8 CONCLUSION AND FUTURE WORK 79
APPENDIX MODEL CODE 84
REFERENCES 97

LIST OF TABLES

Table 1. Definitions 6

Table 2. Inclusion/Exclusion Criteria 15

Table 3. Search Results 16

Table 4. TPCRM Research Themes and Descriptions 20

Table 5. Factors of Importance for TPCRM 21

Table 6. Challenges for Third-Party Cyber Risk Management 25

Table 7. Best Practices for an Effective TPCRM Program 28

Table 8. Challenges and Best Practices Matrix 33

Table 9. Reviewed Standards and Regulations 35

Table 10. Mapping of Recommendations from Popular Cybersecurity Standards 37

Table 11. Turtles and Their Actions 46

Table 12. Model Parameters, Scenario 1 69

Table 13. Model Parameters, Scenario 2 70

Table 14. Model Parameters, Scenario 3 72

Table 15. Model Parameters, Scenario 4 74

LIST OF FIGURES

Figure 1. Publication sources 17

Figure 2. Number of publications for each year 18

Figure 3. Themes of TPCRM research 20

Figure 4. Factors of importance 22

Figure 5. Challenges to an effective TPCRM program 23

Figure 6. Best practices of TPCRM 27

Figure 7. TPCRM importance, challenges, and best practices 32

Figure 8. The tiered design of the model 47

Figure 9. Controls and parameters on the model interface 49

Figure 10. Decisions and actions simulated in the model 62

Figure 11. Breach cost for various complexities 69

Figure 12. Risk appetite effect 71

Figure 13. Control level effect on costs 72

Figure 14. Monitoring and due diligence effects on costs 75

CHAPTER 1

INTRODUCTION

The growing complexity of global business ecosystems in recent years has greatly increased organizations' reliance on third-party services. Collaborating with external vendors and partners is essential as companies grow out of traditional boundaries. These third parties provide a wide range of services, from IT and cloud support to managing supply chains and customer service, allowing companies to focus on what they do best while benefiting from the specialized skills and resources of others. These third-party providers play a critical role in enabling organizations to access advanced technologies, specialized expertise, and cost-effective services without the need to build and maintain these capabilities in-house.

In a general context, a third party refers to an individual or entity that is involved in a transaction, agreement, or relationship but is not one of the main actors. Typically, the first party is the individual or organization initiating the transaction, and the second party is the recipient or counterpart. The third party is an external participant who might offer services, mediate, or be affected by the outcome. For example, in a contract between a buyer and a seller, a third party could be a logistics company that delivers the goods.

In a business context, a third party refers to companies or individuals that provide services or products to the main business. For example, a business may hire a third-party supplier to provide raw materials or a third-party consultant to offer expertise. In an information systems context, these third-party relationships can take many forms, from cloud computing and data center hosting to software development and cybersecurity services. For example, organizations may rely on cloud service

providers like Amazon Web Services or Microsoft Azure to deliver scalable computing power, storage, and software-as-a-service solutions, allowing them to focus on their core business functions. Managed service providers (MSPs) can assume responsibility for monitoring, maintaining, and securing the organization's IT infrastructure, including networks, servers, and endpoints. Software vendors supply essential applications, such as enterprise resource planning (ERP) systems, customer relationship management (CRM) tools, or business intelligence platforms, that are integrated into the organization's information systems. Cybersecurity service providers offer specialized expertise in areas like penetration testing, vulnerability assessments, and incident response, helping to strengthen an organization's overall security posture.

Recent reports show that around 60% of organizations now work with more than 1,000 third parties (Deloitte, 2023). This number illustrates just how dependent modern businesses have become on external providers to keep their operations running smoothly. Of course, working with third parties can offer numerous advantages, such as access to specialized expertise and advanced technologies, which allows businesses to tap into skills and tools they may not have in-house. It can lead to significant cost savings, as outsourcing certain functions is often more economical than building those capabilities internally. Additionally, third-party partnerships allow companies to focus on their core competencies while gaining flexibility and scalability.

Increased reliance on third parties brings new challenges, especially in cybersecurity. Each third-party relationship enlarges the attack surface and creates potential weak points where a security breach could affect the entire organization. In today's interconnected business environment, risks extend beyond a company's

internal operations and include the external partners they rely on. Growing dependence on third parties means that companies must proactively manage these risks, particularly as cyber threats become more advanced and widespread.

To navigate this complex environment, organizations must balance taking advantage of third-party partnerships and protecting themselves from the risks they bring. This calls for a robust Third-Party Risk Management (TPRM) strategy that looks at third parties' financial and operational stability and examines their cybersecurity measures. This focus area, known as Third-Party Cyber Risk Management (TPCRM) (Keskin et al., 2021), involves the proactive identification, assessment, and mitigation of the cybersecurity risks emerging from third-party relationships.

The importance of such strategies becomes evident when looking at the data: nearly 19% of data breaches in 2022 were linked to weaknesses in third-party networks (Deloitte, 2023). These incidents demonstrate the severe financial, operational, and reputational damage that can result from vulnerabilities in external entities. A single breach can disrupt operations, lead to regulatory fines, and severely tarnish a company’s reputation, making strong TPRM practices not just a matter of caution but a critical business requirement. As a result, many companies are shifting their focus toward developing more robust TPRM frameworks that address both the traditional risks, such as financial instability or operational failures, and newer risks, particularly those related to cybersecurity (Gartner, 2023).

Managing the digital and cybersecurity risks associated with third parties is one of the greatest challenges businesses face today (EY, 2023; Deloitte, 2021). Each third-party connection increases the possibility of cyber threats such as data breaches, ransomware attacks, and phishing schemes targeting both the company and

its third-party partners. Consequently, cybersecurity has become one of the most significant aspects of TPRM.

This study focuses on TPCRM intending to answer the following research questions:

- RQ1. What are the primary studies on third-party cybersecurity, and which research themes have been addressed in the literature?
- RQ2. What are the critical challenges for effective third-party cybersecurity risk management in enterprise environments?
- RQ3. What are the best practices for an organization to manage third-party cybersecurity risks?
- RQ4. How can agent-based models be used to simulate third-party cyber risks?

1.1 Third-party cyber risk management and cyber supply chain risk management

TPCRM has various definitions in the literature, mainly because the term third-party changes meanings based on factors like industry and the size of the company in question. There is also a close but slightly different research area: Cyber Supply Chain Risk Management (C-SCRM). The area of C-SCRM is closely related to TPCRM, and there is a considerable overlap between the two. However, while C-SCRM focuses on the entire supply chain and works on the risks associated with the flow of data and information in the supply chain (Ghadge et al., 2019), TPCRM focuses on the flow of data and information between the main company and third-party entities, which the main company is in relationship with (Chingombe, 2023). Because suppliers and vendors in the supply chain are also third parties for the main company, most C-SCRM areas overlap with TPCRM areas. Thus, it is safe to say

that all supply-chain cyber risks are third-party cyber risks, but not all third-party cyber risks are supply-chain cyber risks (European Union Agency for Cybersecurity., 2021).

Table 1 lists the definitions for third-party risk and third-party risk management. Definitions of C-SCRM are also used in the study when the researcher deems the source in question to be TPCRM relative. Although none are incorrect, most researchers agree that TPCRM can be defined as a collection of business and cybersecurity processes that aim to effectively and continuously assess and manage cyber risks emerging from third-party interactions (Mohamed, 2024, Keskin et al., 2021, Chingombe, 2023).

The literature on the topic is not yet decisive. The lack of accepted and generally applicable definitions, standards, and processes is a recognized problem among researchers (Haller & Wallen, 2016; Monev, 2021). This situation challenges organizations, meaning that current TPCRM practices and standards are not mature enough.

The literature addresses the idea that an effective TPCRM should be integrated with other organizational programs and processes (Boyens et al., 2020; Cinar, 2023). Additionally, having a matured Enterprise Risk Management (ERM) program before creating a TPCRM program is also recommended (Boyson, 2014). Moreover, Abrahams et al. (2024) highlighted the importance of TPCRM, as organizations increasingly rely on third parties for key functions, managing the associated risks becomes critical to maintaining operational resilience, regulatory compliance, and member trust. Giacchero & Moretti (2021) also emphasized the need for a TPCRM to manage risks associated with third parties, including potential data breaches, loss of control over critical services, and compliance issues.

Table 1. Definitions

Perspective	Definition	Reference
Third party risk	"These risks encompass a range of potential threats, including data breaches, supply chain attacks, and compliance failures, each with its own set of implications for organizational security and operational integrity."	Ilori et al., 2024
	Risks coming from engaging third-party vendors.	Abrahams et al., 2024
	"When a third party stores, accesses, transmits or performs business activities for and with an enterprise, it represents a probable risk for the enterprise."	Putrus, 2017
	"Cybersecurity risks associated with this loss of control (and visibility) can be significant. They range from unknown provenance of hardware or software that supports an organization's digital functions to subcontractors and consultants having access to its critical data."	Boyens et al., 2020
Third-party risk management	"Third-Party Risk Management is the process used by companies to monitor and manage interactions with all external parties, particularly their vendors."	Keskin et al., 2021
	"Third-party risk management is a critical component of organizational governance and risk mitigation. It involves the identification, assessment, and management of risks associated with the engagement of external parties, such as vendors, suppliers, service providers, and contractors."	Abrahams et al., 2024
	"The practice of third-party risk management (TPRM) is an approach used by enterprises to assess, evaluate, onboard, and monitor external service providers, particularly those who supply technology or information services prior to onboarding them."	Chingombe, 2023
	"Third-party risk management is a crucial aspect of cyber security that organizations need to prioritize. It involves assessing and mitigating the risks associated with the use of external vendors, suppliers, and partners who have access to an organization's sensitive data and systems."	Mohamed, 2024
Cyber supply chain risk management	"The discipline which addresses cybersecurity risks that are related to the extended supply chains and supply ecosystems."	Hammi et al., 2023
	"Cyber supply chain risk management (C-SCRM) is an emerging management construct resulting from the fusion of approaches, methods, and practices from the fields of cybersecurity, enterprise risk management, and supply chain management."	Boyson, 2014

The TPCRM process has a lifecycle that includes planning, due diligence, contract negotiations, ongoing monitoring, and termination. Each phase has specific activities and goals, such as assessing risk appetite, performing security assessments,

establishing contracts with security standards, continuously monitoring third-party compliance, and securing offboarding processes.

The evolution of TPCRM has been significantly influenced by various cybersecurity standards and frameworks. Notable among these are ISO/IEC 27001:2022, which provides requirements for information security management systems, and NIST SP 800-161, which specifically addresses supply chain cybersecurity risk management. These standards have helped shape how organizations approach third-party cyber risks by providing structured frameworks for risk assessment and management.

The ISO/IEC 27036 series, particularly focused on supplier relationship security, offers comprehensive guidance for managing third-party cybersecurity risks. Similarly, the NIST Cybersecurity Framework includes specific components addressing third-party risk management, emphasizing the importance of supply chain risk management in overall cybersecurity strategy. These frameworks not only guide organizations in developing their TPCRM programs but also help establish common ground for security expectations between organizations and their third-party partners.

There is a strong focus on the need for compliance with various data protection and privacy laws, such as GDPR, CCPA, and others, which have begun to include more explicit requirements for third-party risk management. This is in response to the increasing number of data breaches involving third-party vendors, emphasizing the financial and reputational risks associated with inadequate third-party risk management. Next is a discussion on recent cyber events primarily caused by third-party relationships.

1.2 Third-party caused breach cases

While definitions and guidelines help build a basic understanding, real-world examples show the true impact of third-party cyberattacks. In this section, we will examine specific cases where vulnerabilities in third parties have led to major security breaches for companies.

The SolarWinds breach of 2020 represents a significant milestone in cybersecurity incidents. The attack compromised SolarWinds' Orion platform, a software tool that organizations use to manage their computer network and servers. Through a sophisticated attack method, malicious actors inserted harmful code into Orion's routine software updates. As these corrupted updates were distributed, approximately 18,000 organizations unknowingly installed the compromised software, including U.S. government agencies and major corporations. The attackers, believed to be state-sponsored, maintained undetected access to these networks for several months, extracting sensitive data throughout this period. This incident highlighted critical weaknesses in software supply chain security and led organizations to strengthen their third-party risk management practices (Oladimeji & Kerner, 2023). The impact of the SolarWinds breach continues to influence how organizations evaluate and secure their relationships with software vendors.

The Kaseya incident of July 2021 demonstrates another critical example of supply chain vulnerability in cybersecurity. The attack targeted Kaseya's VSA software, which IT service providers use to manage their clients' computer systems. Exploiting a previously unknown security flaw, the REvil ransomware group launched an attack that affected approximately 1,500 organizations. The incident was particularly significant because it created a chain reaction: the attackers first compromised IT service providers, who unknowingly spread the ransomware to their

business clients, including grocery stores, dental offices, and accounting firms (Kaseya, 2021). This breach highlighted a unique aspect of third-party risk: the potential for attacks to spread through multiple layers of business relationships. When IT service providers were compromised, their entire customer base became vulnerable. The incident resulted in widespread business disruptions and financial damage, emphasizing the need for stronger security practices in managed service relationships. Organizations learned that they must carefully evaluate not only their direct service providers but also understand how these providers protect their systems and data (Krehel, 2022).

The Okta breach in March 2022 illustrates how attackers can exploit third-party service providers to target major security companies. Okta, which provides identity management services to organizations worldwide, suffered a breach when the hacking group Lapsus$ compromised an account belonging to a customer support engineer from one of their external service providers. This incident revealed how vulnerabilities in support services can create security risks for the broader organization. The attack gave Lapsus$ access to view and potentially modify data for approximately 366 Okta customers. While this represented only a small portion of Okta's total customer base, the breach was particularly concerning because Okta's services are fundamental to many organizations' security infrastructure. However, Okta reported that their core authentication systems remained secure, preventing the attackers from directly accessing user accounts (Bradbury, 2022; Faife, 2022).

A significant supply chain vulnerability emerged in April 2024 when Microsoft developer Andres Freund discovered unusual performance patterns during SSH logins on Debian systems. His investigation revealed a deliberately planted backdoor in XZ Utils, a widely used compression software in Linux systems. Freund

reported these findings to the Open Source Security List, drawing immediate attention from the cybersecurity community (Goodin, 2024). Microsoft researcher Thomas Roccia's subsequent analysis demonstrated the potential scale of this threat, drawing parallels to the SolarWinds incident of 2020. The malicious code in XZ Utils versions 5.6.0 and 5.6.1 modified SSH daemon operations to allow unauthorized code execution through specially constructed SSH login certificates. While no actual exploitation of this backdoor was detected, its presence in such fundamental software posed a theoretical risk to millions of Linux systems worldwide. The backdoor could have enabled attackers to access sensitive data or deploy malware across affected systems had it been successfully deployed. This incident highlights two key vulnerabilities in software supply chains: the potential for malicious code to be inserted into widely used software components and the difficulty of detecting such modifications in complex open-source systems. It serves as a recent example of how threat actors continue to target fundamental software infrastructure that organizations rely upon.

These four incidents—SolarWinds, Kaseya, Okta, and XZ Utils—show how third-party security risks have become more complex and dangerous in today's connected business environment. Each case reveals a different aspect of third-party risk: SolarWinds demonstrated the danger of compromised software updates; Kaseya showed how attacks could spread through IT service providers; Okta illustrated the risks of external support services; and XZ Utils revealed how basic software tools that organizations trust can be compromised.

These cases share an important pattern: instead of attacking organizations directly, threat actors target trusted third parties to gain access to many victims at once. This strategy allows attackers to affect more targets while using legitimate

access paths to bypass security measures. The incidents also show that organizations often cannot fully monitor or control the security of their third-party providers, even though they rely heavily on them for important services and software. The long periods between the initial attacks and their discovery—especially in the SolarWinds case—highlight how difficult it is for organizations to detect security problems in their third-party relationships.

These significant security incidents demonstrate the complex, interconnected nature of modern organizational relationships and their associated cybersecurity risks. Traditional risk assessment methods ignoring third-party risks often struggle to capture the dynamic and cascading effects illustrated by these cases, where a single compromise can spread through multiple organizations and affect various systems over time. This insufficiency calls for more sophisticated approaches to understanding and analyzing third-party security risks. Agent-based modeling (ABM) offers a promising methodology to study these complex interactions and their potential outcomes. Unlike conventional risk assessment tools, ABM can simulate the behavior of multiple independent actors—such as organizations, threat actors, and third-party providers—and their interactions within the security ecosystem. The next section is a discussion on ABMs and their uses in modeling cybersecurity environments.

1.3 Agent-based modeling

Agent-based modeling (ABM) is a computational approach used to simulate the interactions of individual agents within a specific environment to observe their collective behavior and emergent patterns. In an ABM, each agent follows a set of predefined rules and possesses unique attributes, such as decision-making abilities,

mobility, and the capacity to learn or adapt. These agents interact both with one another and with their environment, enabling us to explore how complex systems evolve where it's hard to predict what will happen (Macal & North, 2009).

ABM is widely used across various fields, including public health studies, social sciences, economics, and environmental studies, due to its ability to model systems with highly diverse and interconnected components. In economics, for instance, ABM is used to simulate market dynamics by modeling individual consumers and firms (Macal & North, 2009). In public health studies, ABM is used to model the spread of infectious diseases, explore the factors contributing to obesity, and understand the dynamics of tobacco use (Ornstein & Hammond, 2021).

In cybersecurity, ABMs can model how different threats and defenses act within a network. Cybersecurity is a complex problem, and ABMs allow us to see how cyberattacks spread, how defenses can stop them, and where the weak points are in a system. Traditional models often fail to capture this complexity, but ABMs can show us how small changes—like a new virus or a weak third-party vendor—can lead to big problems for a company. ABMs are also useful because they can include a lot of real-world data, like information from sensors or security systems, to make the simulations more realistic (Vestad & Yang, 2024).

This thesis uses an ABM to model third-party interactions in a company and observes the impact of third-party cyber risk management practices; by doing so, it provides an example of using ABMs for risk analysis. As the risk emerges from the interactions between companies in the context of TPCRM, it can be observed in an ABM based on real-world data. The following section is a systematic literature review on TPCRM, followed by an ABM using the findings of the review.

CHAPTER 2

SYSTEMATIC LITERATURE REVIEW METHODOLOGY

2.1 Research method

A systematic literature review (SLR) is a methodical and comprehensive approach to identifying, evaluating, and synthesizing existing research on a particular topic. This study uses SLR methods and follows a structured process to ensure the review is thorough and unbiased. This study employs the approach outlined by Hanafizadeh et al. (2014) and used by Niknejad et al. (2020). This involves defining specific research questions, using explicit methods to search for relevant literature, and setting inclusion and exclusion criteria for selecting studies. The goal is to provide a complete, reproducible summary of the current state of knowledge on the topic, highlighting gaps in the research and suggesting areas for future study.

2.2 Review protocol

The review protocol of this study involves defining the research questions, creating a reproducible search strategy, finding and filtering the literature according to the inclusion and exclusion criteria, extracting data, reporting, and discussing the results. This study utilizes a similar approach used by Niknejad et al. (2020) with the research phases defined below. One note is that the fourth research question is addressed individually, as its focus area differs from the other research questions. The following sections of the literature review focus on the first three research questions unless stated otherwise.

- Phase 1, Identifying Research Questions
  - RQ1. What are the primary studies on third-party cybersecurity and which research themes have been addressed in the literature?
  - RQ2. What are the critical challenges for effective third-party cybersecurity risk management in enterprise environments?
  - RQ3. What are the best practices for an organization to manage third-party cybersecurity risks?
  - RQ4. How can agent-based models be used to simulate third-party cyber risks?
- Phase 2, Search Strategy & Article Selection
  - Automatic Search String (Google, Google Scholar, Scopus, ProQuest, IEEE Xplore)
  - Inclusion/Exclusion Criteria in Full Text
  - Manual Backwards Search
  - Remove Duplicate Studies
- Phase 3, Data Extraction
  - Extracting Research Objectives, Proposed Ideas, and Systems, TPCRM Theme
- Phase 4, Synthesis, Comparison, Results
  - Analyzing manually through the selected papers and comparing the findings
- Phase 5, Reporting
  - Writing the report

2.3 Inclusion and exclusion criteria

This study aims to find the relevant research and discussion about TPCRM. This research focuses on the sources published in English from 2013 to July 2024. The year 2013 was selected since the second version of the information security management standard, ISO/IEC 27001:2013, was published in 2013, with an emphasis on the importance of TPCRM. The inclusion and exclusion criteria are presented in Table 2. The time interval for the RQ4 review is chosen to be closer to the current date to limit results to newer resources.

Table 2. Inclusion/Exclusion Criteria

Criteria	Principle
Inclusion	Papers published between 2013 and July 2024 Full text accessible Papers with focus on TPCRM Papers that answer the defined research questions Papers published between 2020 and July 2024 (for RQ4 only) Papers with focus on agent-based modeling of cybersecurity systems (for RQ4 only)
Exclusion	Papers not in English language Papers out of the cybersecurity scope

2.4 Search strategy

Different search strings are tested to identify relevant literature on the topic, guided by the predefined research questions. The initial search using the full search string in the Scopus and IEEE Xplore databases returned few results. Consequently, the search strings used in these databases were refined and expanded. Please note that the results are manually filtered by date, specifically from 2013 to July 2024. Table 3 presents full search strings used in their respective databases:

Table 3. Search Results

Database	Search String	Results
Google Scholar	"third party risk management" AND ("cyber" OR "cybersecurity") AND "enterprise" AND ("best practices" OR "critical factors" OR "influencing factors")	294
Scopus	cyber AND third AND party AND risk AND management	68
ProQuest	"third party risk management" AND ("cyber" OR "cybersecurity") AND "enterprise" AND ("best practices" OR "critical factors" OR "influencing factors")	61
IEEE Xplore	("All Metadata":third party risk management) AND (("All Metadata":cyber) OR ("All Metadata":cybersecurity))	86
Google Scholar (for RQ4)	“agent based model” AND “cybersecurity” AND “third party”	215

2.5 Study selection process

Titles and abstracts of the search results are analyzed, and 49 items are selected from Google Scholar. Repeating the same procedure, four items were selected from the Scopus database. ProQuest database resulted in five items relevant to the research questions, and finally, two items selected from IEEE Xplore. After a full-text review of the papers and removing the duplicates using Zotero software, 26 items are left. A backward search is applied while doing the full-text analysis on selected papers. However, no new sources were found, as it is observed that the papers mainly cite each other.

As for the RQ4, Google Scholar returned 215 results. The first two pages are examined to find the most relevant and important research on the topic. Eight studies were reviewed manually, and three of them were selected.

2.6 Data extraction and synthesis

In this step, each primary study was read carefully, and the relevant data was extracted using Zotero Software and Microsoft Excel. The extracted data for this systematic review were put into an Excel spreadsheet based on the following columns: Study ID, Author(s), Publication Year, Title of Study, Source Type,

Methodology, Objective, TPCRM Theme, and Relevancy to the Research Questions. These items were included based on the defined research questions and the objectives of the study.

2.7 An overview of the publication sources

The literature depth on TPCRM is shallow. Thus, while selecting the primary sources, the inclusion criteria were created broadly, as explained in Section 3 of this chapter. Generally chosen criteria for primary studies, such as being published in high-impact journals, peer review processes, and non-thesis journal articles, are not implemented in this study because the number of studies providing these conditions is low. Figure 1 presents the publication sources of the primary studies.

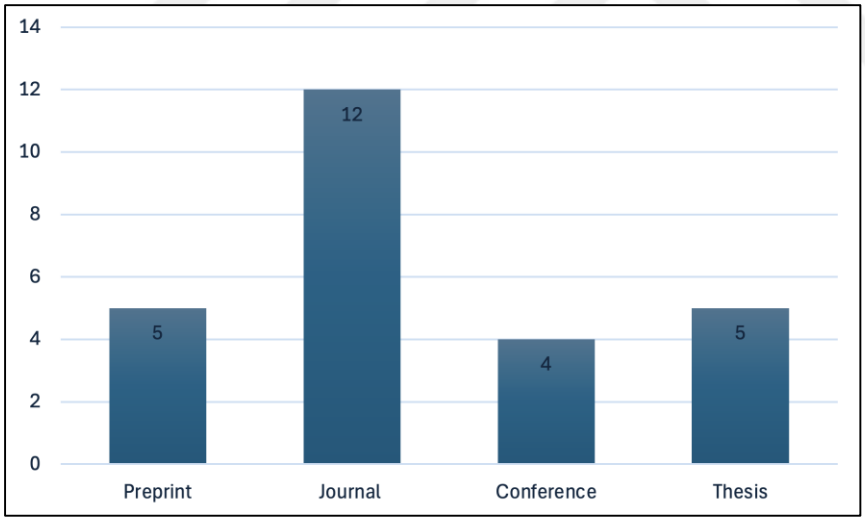

Figure 1. Publication sources

2.8 Temporal view of the sources

As stated before, using a systematic literature review, sources published between 2013 and 2024 are selected. Figure 2 presents the distribution of the sources during this period, which shows increased research interest in the subject matter. It is

observed that 2023 is the year with the most sources published (7 sources), followed by 2024 with five publications. In the year 2021, four sources are published about the topic, with 2019 and 2022 having three publications coming just behind. It is observed that 2020 has two publications, while there are no sources published in the years 2017, 2018, 2015, and 2013. Lastly, one source was published in 2014 and 2016.

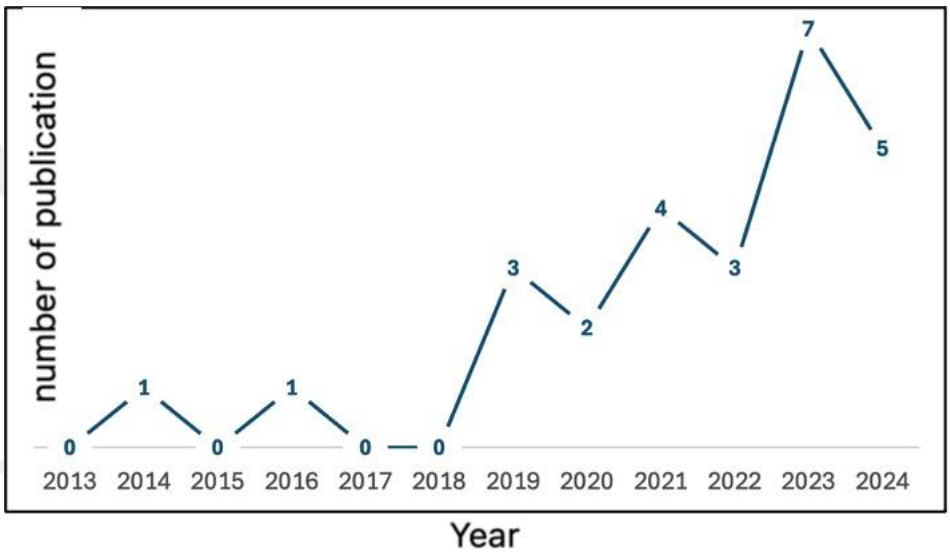

Figure 2. Number of publications for each year

CHAPTER 3

FINDINGS FROM THE LITERATURE REVIEW

As highlighted in the previous sections, this systematic review was designed to address specific research questions on TPCRM. This section presents the findings for each research question.

3.1 RQ 1: What are the primary studies on third-party cybersecurity risk management, and which research themes have been addressed in the literature?

Literature was not fully conclusive about the aspects of third-party cybersecurity management; it is observed that there are areas that all studies revolve around. These "themes" are not a comprehensive organization of TPCRM research, as the current state of literature is not yet mature enough to allow complete categorization. However, they are observed as the main topics of discussion among the researchers. The themes are created from studies emphasizing the role and importance of TPCRM, studies discussing the challenges of creating and maintaining an effective TPCRM, and studies providing recommendations and best practices for TPCRM. Of the 25 studies found, six of them focus on the importance of TPCRM in organizations. 13 articles discuss TPCRM Challenges, and 17 include sections on TPCRM Best Practices. Table 4 and Figure 3 present the themes of research for TPCRM.

Table 4. TPCRM Research Themes and Descriptions

TPCRM Theme	Description
Importance	The role and importance of TPCRM in protecting an organization from third-party cybersecurity risks, as well as the need for it.
Challenges	The difficulties and obstacles organizations face when trying to identify, assess, and mitigate cyber risks associated with third parties.
Best practices	The strategies, methodologies, and actions that have been identified as the most effective in managing and mitigating cyber risks associated with third-parties.

The first one of the themes is the importance and need for a third-party cyber risk management program. The studies with this theme highlight the compliance needs and the potential impact of the risks. Abrahams et al. (2024) and Giacchero & Moretti (2021) identify the increasing regulatory requirements related to third-party risks. Abrahams et al. (2024) build on this, noting an important connection between third-party engagements and compliance, particularly regarding data and asset protection. The literature also recognizes a potential upside of third-party risks, as they come with certain business opportunities. Because an effective TPCRM allows organizations to have more resilient third-party operations, it gives organizations a potential competitive advantage (Keizer, 2022; Sen et al., 2020).

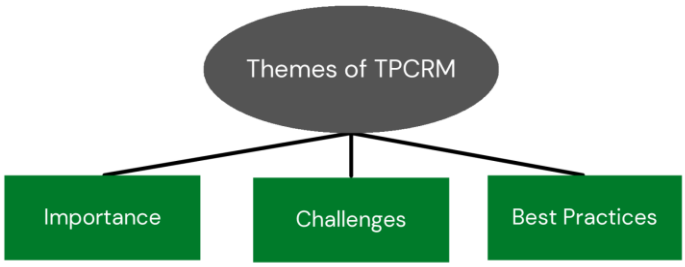

Figure 3. Themes of TPCRM research

The need for TPCRM shows itself mostly in the number and impact of breaches as well as multiple risk factors associated with third parties (Takefuji, 2022). For example, a data breach can cause both financial and reputational damage,

result in regulatory fines, and cause loss of customer trust. These risks are hard to identify, and their long-term effects are unpredictable (Keizer, 2022). Thus, having a comprehensive understanding of third-party relationships is crucial for managing the risks (Mohamed, 2024). Table 5 presents the findings on the importance of TPCRM. Figure 4 shows the factors of importance.

Table 5. Factors of Importance for TPCRM

Factor	Reference
Ensuring compliance	The connection between third-party engagements and compliance is important for protecting data and assets (Abrahams et al., 2024); Having a TPCRM is important for following tightening regulatory requirements (Giacchero & Moretti, 2021),
High risks	The risks associated with third parties are high, and the potential impact they possess is hard to identify. To effectively manage these risks, a comprehensive TPCRM is needed. (Giacchero & Moretti, 2021), (Mohamed, 2024), (Keizer, 2022), (Abrahams et al., 2024); The number and scale of attacks are rising, increasing the importance of TPCRM. (Takefuji, 2022);
Opportunity	With an effective TPCRM, possible risks and threats can become a business opportunity. (Keizer, 2022), (Sen et al., 2020).

The second one of the themes is the challenges that organizations face in managing third-party cyber risks. This theme comprises studies that discuss the difficulties and obstacles organizations face when trying to identify, assess, and mitigate cyber risks associated with third parties. The details of this theme and the complete list of challenges are discussed in the next part, the second research question.

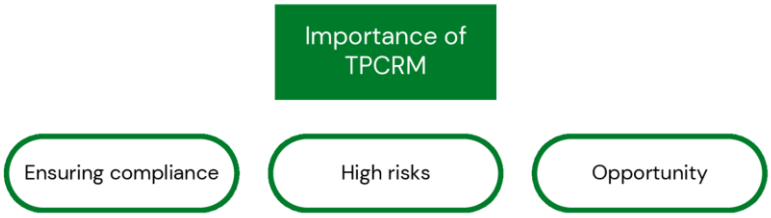

Figure 4. Factors of importance

The third and final theme centers on best practices for developing an effective TPCRM program. This theme encompasses studies that suggest a range of policies, processes, and practices for managing third-party cyber risks. Similar to the second theme, the TPCRM Best Practices theme directly addresses the third research question and is further elaborated in the section covering the said question.

3.2 RQ 2: What are the critical challenges to address for effective third-party cybersecurity risk management in enterprise environments?

The complexity of these risks is highlighted as a major challenge by multiple researchers. A large number of third-party relationships, each with its own set of risk factors, creates a challenging and complex environment for organizations (Chingombe, 2023; Roberts, 2023; Bronson, 2022). The integration of multiple systems further compounds this complexity (Cinar, 2023). To manage risks in such a complex environment, organizations are advised to engage in collaborative efforts, continuous information sharing, and coordinated planning. However, successfully implementing these practices poses an additional challenge, as there are often no universally applicable standards, particularly for organizations operating across different regions and industries (Keskin et al., 2021). As noted by Haller & Wallen (2016) and Ghadge et al. (2019), general third-party cybersecurity practices often do

not align with the needs of different organizations. This misalignment, combined with the challenges of collaboration, hampers information visibility, both due to the reasons mentioned earlier and the loss of control over assets and processes when working with third parties (Greenfield et al., 2023; Hammi et al., 2023). Figure 5 shows the challenges of creating and maintaining a TPCRM program.

Compliance requirements are highlighted as a key reason for the importance of TPCRM, but they are also viewed as a challenge, particularly for companies operating across multiple regions and industries (Hammi et al., 2023). Different regions have their own regulations and standards, making it difficult for organizations to achieve full compliance. However, adhering to these requirements is often recommended as a best practice, as it helps to ensure that all partners maintain the same high standards of cybersecurity (Zawaideh et al., 2023). Adhering to the requirements is especially hard for small and medium-sized enterprises (SMEs), mainly because it is an expensive and complex process (Kwong & Pearlson, 2024).

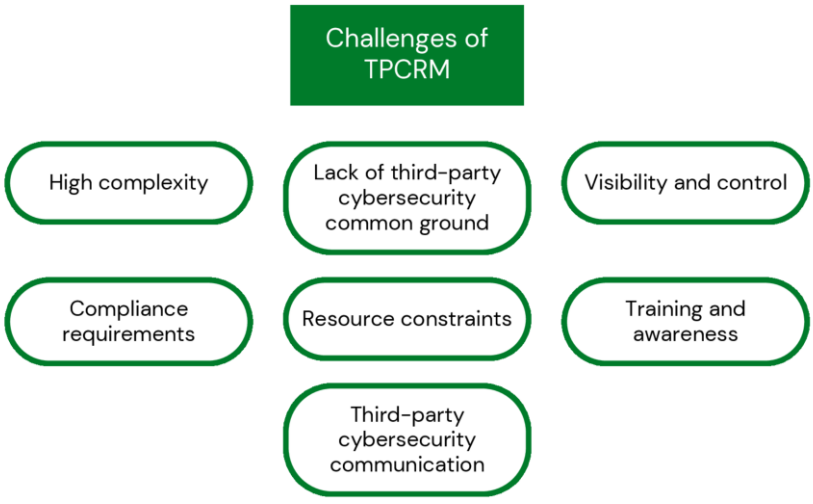

Figure 5. Challenges to an effective TPCRM program

TPCRM is a complex problem, and it requires extensive resources both in finances and knowledge/experience (Chingombe, 2023). This creates a challenge for all companies, affecting SMEs the most. As also stated by Mohamed (2024), companies need training and awareness to overcome this challenge, which is a challenge in itself. Leadership often lacks a deep understanding of third-party risks (Kwong & Pearlson, 2024), requiring special training for them as well. Finally, having effective communication with third-party entities is found to be a challenge, the reason being the long turnaround times of third parties and general communication issues between various-sized companies (Haller & Wallen, 2016; Mohamed, 2024). Table 6 presents the list of challenges ordered according to the number of sources it has been discussed.

Table 6. Challenges for Third-Party Cyber Risk Management

Challenge	Reference
High complexity	Aggregation of various risk factors (Bronson, 2022), (Chingombe, 2023); High number of third-party relationships (Roberts, 2023), (Haller & Wallen, 2016); Integration of multiple systems (Cinar, 2023), (Hammi et al., 2023); Excessive cyber threats and advanced attackers for organizations with varying vulnerabilities (Greenfield et al., 2023); Complexity too high for organizations, government should step in (Ghadge et al., 2019).
Lack of third-party cybersecurity common ground	General third-party cybersecurity practices does not align with different organizations (Haller & Wallen, 2016), (Monev, 2021), (Ghadge et al., 2019), (Keskin et al., 2021), (Roberts, 2023)
Visibility and control	Loss of control over assets, people, and processes when working with a third-party, combined with low visibility and difficulty in detection increase the challenge of managing cyber risks (Greenfield et al., 2023), (Haller & Wallen, 2016), (Hammi et al., 2023), (Roberts, 2023), (Mohamed, 2024)
Compliance requirements	Complex and evolving regulatory requirements (Haller & Wallen, 2016); Diverse regulatory requirements across different regions and industries (Hammi et al., 2023); Expensive and complex compliance requirements for SMEs (Kwong & Pearlson, 2024); Need for comprehensive knowledge regarding the regulations and standards for third-party entities (Cinar, 2023).
Resource constraints	Lack of resources and executive support (Chingombe, 2023), (Bronson, 2022); Limited resources and expertise in small and medium-sized enterprises (Hammi et al., 2023).
Training and awareness	Insufficient cybersecurity training among employees (Ghadge et al., 2019); Leadership often lacks deep understanding of third-party risks (Kwong & Pearlson, 2024), (Mohamed, 2024).
Third-party cybersecurity communication	Long turnaround times of third-parties (Mohamed, 2024); Person or persons needed to achieve reliable communication (Greenfield et al., 2023); Companies with various sizes have a hard time communicating with each other (Haller & Wallen, 2016).

3.3 RQ 3: What are the best practices for an organization to manage third-party cybersecurity risks?

One of the most frequently suggested practices is continuous monitoring and evaluation, as discussed by Abrahams et al. (2024), Boyens et al. (2020), and Ilori et al. (2024), among others. This approach primarily involves implementing mechanisms such as real-time alerts and performance tracking, directly addressing the challenges of visibility and control in TPCRM (Monev, 2021). Another best practice that directly addresses both visibility/control and high complexity challenges

is creating a collaborative information-sharing environment (Chingombe, 2023). Aliane & Zakariya (2023) describe this practice as the development and maintenance of processes, protocols, and systems that enable collaboration both internally and with external partners. This includes sharing critical information, such as threat intelligence, and fostering cooperative security efforts (Hammi et al., 2023).

Sen et al. (2020) and Boyson (2014) suggest aligning and integrating cybersecurity policies, protocols, and standards with other organizational programs, such as Enterprise Risk Management. This approach can help organizations address the challenge of lacking a common ground. Additionally, part of this alignment should involve conducting due diligence before entering third-party relationships (Kwong & Pearlson, 2024; Haller & Wallen, 2016). Companies should have standardized processes prioritizing resources based on risk attributes of a third party and customize those processes based on the specific business engagements using context or scenario-based surveys and questionnaires (Monev, 2021; Chingombe, 2023; Venugopal et al., 2024). Establishing strong contracts, alongside due diligence, that specify security requirements, data protection measures, incident response procedures, and breach notification protocols is recognized as a best practice for TPCRM (Mohamed, 2024; Ilori et al., 2024). These contracts should clearly define the roles and responsibilities of both parties and be reinforced by access control measures and robust encryption protocols (Mohamed, 2024; Zawaideh et al., 2023). Additionally, maintaining an inventory of third-party relationships and documenting their rights and permissions is another recommended practice (Giacchero & Moretti, 2021).

Employee knowledge is a critical factor for achieving high cybersecurity maturity, and raising awareness of the latest security threats and best practices is

recommended by Cinar (2023), Takefuji (2022), and Zawaideh et al. (2023). Lastly, ensuring compliance is listed as a best practice as it helps organizations in ensuring the same standards of cybersecurity. As it is discussed above, the same principle is seen in all themes of TPCRM research. Figure 6 shows the best practices of TPCRM.



Figure 6. Best practices of TPCRM

Table 7 summarizes the identified findings in descending order based on their frequency of occurrence across the analyzed literature.

Table 7. Best Practices for an Effective TPCRM Program

Best practice	Reference
Continuous monitoring and evaluation	Implement mechanisms such as site visits, formal certifications, audits, penetration testing, vulnerability scanning, e.g. for ongoing assessment of third-party vendors' performance, cybersecurity measures, and compliance with regulatory standards. Update risk assessments based on changes in their security posture and business context. (Abrahams et al., 2024). (Boyens et al., 2020), (Ilori et al., 2024), (Mohamed, 2024), (Monev, 2021), (Giacchero & Moretti, 2021), (Chingombe, 2023), (Hammi et al., 2023), (Boyson, 2014); Establish continuous monitoring systems such as real-time alerts and performance tracking to maintain visibility and transparency, detect anomalies and potential security threats in real-time (Aliane & Zakariya, 2023), (Boyens et al., 2020), (Venugopal et al., 2024), (Zawaideh et al., 2023), (Giacchero & Moretti, 2021), (Takefuji, 2022), (Sen et al., 2020).
Collaborative information sharing and incident response	Develop and maintain processes, protocols, and systems to collaborate both internally and with external partners, share information such as threat intelligence, conduct joint assessments, build cooperative security activities. (Aliane & Zakariya, 2023), (Haller & Wallen, 2016), (Chingombe, 2023), (Hammi et al., 2023), (Boyson, 2014); Develop and test incident response and disaster recovery plans with third-parties and regularly update the plans. (J. M. Boyens et al., 2020), (Ilori et al., 2024), (Zawaideh et al., 2023), (Cinar, 2023), (Takefuji, 2022).
Alignment and integration of cybersecurity policies, protocols and standards with other organizational programs	Integrate TPCRM with existing organizational systems, which is preferable with a comprehensive enterprise risk management program. Include executives from various departments. Create clear accountability and ownership mechanisms. (Sen et al., 2020), (Boyson, 2014), (Boyens et al., 2020), (Abrahams et al., 2024); Develop consistent and repeatable processes with a strong organizational cybersecurity culture, ensure that processes are aligned with widely recognized cybersecurity standards. (Kwong & Pearlson, 2024), (Haller & Wallen, 2016), (Aliane & Zakariya, 2023); Use tools such as Governance, Risk Management, and Compliance (GRC) software, that can integrate with existing systems and scale according to the evolving risk management needs. (Cinar, 2023), (Venugopal et al., 2024).
Thorough due diligence and assessment	Perform risk assessment of a third-party before engaging with the third-party, evaluate financial stability, reputation, and overall risk profile. Ensure regulatory compliance of the third-party. Check for cybersecurity standards and certifications. (Abrahams et al., 2024), (Ilori et al., 2024), (Mohamed, 2024), Have standardized processes prioritizing resources based on risk attributes of a third-party, customize those processes based on the specific business engagement using context or scenario based surveys and questionnaires. (Aliane & Zakariya, 2023), (Monev, 2021), (Venugopal et al., 2024), (Giacchero & Moretti, 2021), (Chingombe, 2023).
Training and awareness	Regularly provide cybersecurity training to both employees and third-party entities to raise awareness of the latest security threats and best practices. (Abrahams et al., 2024), (Ilori et al., 2024), (Mohamed, 2024), (Zawaideh et al., 2023), (Cinar, 2023), (Hammi et al., 2023), (Takefuji, 2022).
Strong contracts	Develop a master list of security requirements and include them in contracts. (J. M. Boyens et al., 2020); Have clear contractual agreements that outline the roles, responsibilities, performance expectations, and compliance standards of both parties. Include security requirements, data protection measures, incident response procedures, and breach notification protocols in the contracts. (Abrahams et al., 2024), (Mohamed, 2024), (Ilori et al., 2024); Track and monitor the contracts to ensure third-party accountability and compliance (Giacchero & Moretti, 2021), (Venugopal et al., 2024),
Access control and user roles	Have distinct and clear roles and responsibilities for managing cybersecurity aspects of third-party relationships. (J. M. Boyens et al., 2020), (Giacchero & Moretti, 2021); Establish strict access control measures using the principle of least privilege to regulate and limit third-party access to sensitive data and systems. (Mohamed, 2024), (Cinar, 2023); Use robust encryption protocols for data both in transit and at rest. (Zawaideh et al., 2023),
Ensuring compliance	Control that third-parties have adequate compliance with relevant regulations and standards to ensure that all partners adhere to the same high standards of cybersecurity (Abrahams et al., 2024), (Mohamed, 2024), (Zawaideh et al., 2023), (Cinar, 2023);
Inventory and documentation of third-party relationships	Have an inventory of all third-party relationships (Abrahams et al., 2024); Document and report data ownership, rights, and permissions of third-parties (Giacchero & Moretti, 2021), (Cinar, 2023);

3.4 RQ 4. How can agent-based models be used to simulate third-party cyber risks?

A comprehensive literature survey conducted by Vestad & Yang (2024) identified 39 papers examining ABM applications in cybersecurity. The analysis revealed seven distinct domains of ABM implementation in cybersecurity: the spread of malware, social networks, human and organizational issues, risk analysis and risk propagation, technological attack and defense strategies, policy evaluation, and strategic outcomes. Given this study's objective of developing a model for third-party cyber risks, it aligns primarily with the risk analysis and propagation domain.

Ashiku and Dagli (2020) demonstrated how ABMs effectively capture emergent behaviors through the modeling of interactions between third-party users, system administrators, and internal users within business systems. Their risk-based model quantifies cyberattack frequencies and evaluates defense mechanism efficacy using empirical data. While third-party users are incorporated as an agent class, the model lacks explicit controls for relationship management. Instead, it simulates organizational agents as attack and defense vectors, emphasizing internal control measures such as firewall implementation, encryption protocols, and software patch management.

Guillermo et al. (2021) developed an innovative model adapting zombie apocalypse simulation paradigms to analyze cyber-attack propagation velocities. Their research examined the impact of various parameters, including adversary sophistication, personnel training levels, and cyber defense robustness. The findings provide valuable insights into optimizing organizational behavior for more efficient cybersecurity resource allocation.

The current literature reveals a notable absence of ABMs specifically addressing third-party relationship dynamics. Existing models predominantly focus

on internal organizational controls, thereby providing insufficient insight into third-party interactions and their cascading effects. Nevertheless, these studies demonstrate the significant utility of ABMs in optimizing cybersecurity resource allocation strategies.

CHAPTER 4

ANALYSIS OF LITERATURE REVIEW FINDINGS

This thesis aims to explore the state of TPCRM as it identifies three primary research themes: TPCRM best practices, challenges in implementation, and the importance of TPCRM. A systematic review of the literature revealed significant challenges in the current practices, particularly in the standardization of processes and the alignment of TPCRM with broader organizational goals. Unsurprisingly, many of the best practices highlighted in the literature directly address these challenges. Table 8 offers an overview of the challenges and the corresponding best practices.

High complexity has been identified as the most significant challenge organizations face in implementing an effective TPCRM program. Creating an inventory of all third-party relationships and documenting their rights and permissions can help address this issue. Additionally, implementing continuous monitoring systems can be highly effective, as these systems offer visibility into the complex network of third-party interactions. The challenge of visibility and control is closely linked to high complexity, as the integration of multiple systems and the sheer number of third-party relationships can lead to a loss of control. Collaborative information sharing is crucial for overcoming this challenge, as it provides the necessary insight into the flow and status of data between the organization and its third-party entities.

It has been observed that, despite widely accepted cybersecurity standards and regulations, achieving common ground with third parties remains challenging due to organizations operating in different industries and regions. While keeping an inventory of third parties, having clear and strong contractual terms, and conducting

thorough due diligence and assessments should give organizations a better understanding of third-party practices and processes, the variation in regional laws and regulations still creates difficulties for companies aiming to ensure full regulatory compliance from their third-party partners. Figure 7 presents the full list of the findings.



Figure 7. TPCRM importance, challenges, and best practices

A lack of expertise and cybersecurity awareness is a significant issue, particularly for SMEs. While resource constraints can only be addressed by increasing resources or improving efficiency, offering training programs and hosting awareness events can effectively combat common social engineering attacks like phishing and vishing. Additionally, using free resources provided by government bodies and industry organizations can be a valuable support for strengthening cybersecurity practices.

Table 8. Challenges and Best Practices Matrix

	Continuous monitoring and evaluation	Collaborative information sharing and incident response	Alignment and integration of cybersecurity policies, protocols and standards with other organizational programs	Thorough due diligence and assessment	Training and awareness	Strong contracts	Access control and user roles	Ensuring compliance	Inventory and documentation of third-party relationships
High complexity		O		O			O		O
Lack of third-party cybersecurity common ground	O	O		O	O	O		O	O
Visibility and control	O	O				O	O		O
Compliance requirements	O		O	O		O		O	
Resource constraints			O		O			O	O
Training and awareness			O		O		O		
Third-party cybersecurity communication	O	O			O	O			

An effective Third-Party Cyber Risk Management (TPCRM) program is essential for organizations. However, they face several major challenges in implementing strong TPCRM practices, such as high complexity, limited visibility and control, difficulties in standardizing processes across various industries and

regions, and a lack of expertise and cybersecurity awareness, particularly within small and medium-sized enterprises (SMEs). These challenges can expose organizations to cyber threats that stem from their third-party relationships.

Several best practices have been identified to help organizations effectively address these challenges. Keeping a detailed inventory of all third-party relationships and documenting their rights and permissions can help reduce complexity and improve control. Implementing continuous monitoring systems and fostering collaborative information sharing can increase visibility into the activities and security posture of third parties. Establishing strong, clear contracts, conducting thorough due diligence, and performing regular assessments can ensure alignment with cybersecurity standards and regulatory requirements, even across various regions and industries. Additionally, investing in training programs and awareness initiatives can enhance cybersecurity expertise and help prevent common attacks like phishing and vishing. For SMEs, utilizing free resources provided by government and industry organizations can help strengthen their cybersecurity practices despite limited resources.

To accurately simulate a real-world network of third-party relationships in an agent-based model, it is essential to select parameters and actions that closely mirror actual conditions. The challenges and best practices identified in the literature provide a solid foundation for defining agent behaviors and model parameters. Since ABMs rely on individual agents interacting with one another based on predefined rules, these challenges and best practices can inform the creation of those rules, ensuring the model realistically reflects third-party dynamics. Incorporating factors such as complexity, lack of visibility, compliance issues, and collaborative information sharing into the agent rules will result in a more robust simulation. This

approach will not only enhance the realism of the model but also provide insights into how organizations can better manage third-party cyber risks by testing potential strategies within the simulation.

This chapter discusses research findings as theoretical approaches to third-party cybersecurity risk management. To understand how these findings translate into practice, the most popular industry standards (Cisternelli, 2024; Kosling, 2024; Ryerse, 2024) and frameworks are compared with the findings. This analysis connects academic research with real-world implementation, showing how organizations apply theoretical concepts in their daily operations. Table 9 shows the selected standards and regulations.

Table 9. Reviewed Standards and Regulations

Name	Organization	Type
ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements	ISO	Standard
ISO/IEC 27036 Cybersecurity – Supplier relationships	ISO	Standard
NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations	NIST	Standard
NIST SP 800-161 Rev. 1 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations	NIST	Standard
NIST Cybersecurity Framework v2	NIST	Framework

ISO/IEC 27001:2022 is a standard describing requirements for "establishing, implementing, maintaining and continually improving an information security management system (ISMS) within the context of the organization." There are five controls especially relevant to third-party security:

- Control 5.19. Information security in supplier relationships
- Control 5.20. Addressing information security within supplier agreements

- Control 5.21. Managing information security in the ICT supply chain
- Control 5.22. Monitoring, review and change management of supplier services
- Control 5.23. Information security for use of cloud services

Besides these controls, the standard extensively documents ISMS policies and procedures for an organization to create and manage. ISO/IEC 27001:2022 is not focused on third-party risk management as it is a standard on ISMS. However, most of its controls overlap with what the literature recommends for TPCRM programs. Table 10 maps the controls of the standards to the literature findings.

The standard deems organizations to define and implement processes to address risks associated with using suppliers' products or services. Information security requirements need to be established and agreed upon with each supplier, tailored to the specific type of supplier relationship. For an Information and Communication Technologies (ICT) supply chain, specific processes and procedures must be in place to handle associated security risks effectively. These controls are in parallel with literature best practices “Inventory and documentation of third-party relationships” and “Alignment and integration of cybersecurity policies, protocols and standards with other organizational programs”.

Additionally, the standard requires organizations to regularly monitor, review, evaluate, and manage changes in supplier information security practices and service delivery. For cloud services, processes must be established to acquire, use, manage, and exit these services in line with the organization's information security requirements. These controls can be categorized with the literature findings “Thorough due diligence and assessment” and “Continuous monitoring and evaluation”.

Table 10. Mapping of Recommendations from Popular Cybersecurity Standards

Best practice	ISO27001	ISO27036	NIST SP 800-53	NIST SP 800-161	NIST CSF
Continuous monitoring and evaluation	5.22	6.1 6.3 6.4	RA-5 CA-7 SI-4 PM-31 AC-20	RA-5 CA-7 SI-4 PM-31 AC-20	GV.SC-05 GV.SC-07 GV.SC-09 DE.CM-06
Collaborative information sharing and incident response	5.24	5.4 6.1 6.2.2 6.4	IR-4,6,7,8 SI-5 SR-8 RA-7	IR-4,6,7,8 SI-5 SR-8 RA-7	GV.RM-05 GV.SC-08 ID.RA-02 ID.RA-08 DE.AE-07 RS.CO-03 RC.C0-03
Alignment and integration of cybersecurity policies, protocols and standards with other organizational programs	5.36 5.21 5.23	6.1 6.3 7.1	PM-1,2,9,14,30 SR-1,2,3 CA-1	PM-2,9,14,30 SR-1,2,3 CA-1	GV.OC-01 GV.RM-01 GV.SC-01 GV.SC-02 GV.SC-03 GV.SC-09 GV.RR-01
Thorough due diligence and assessment	5.19 5.23	6.1 7.2	SA-9 RA-3 SR-6	SA-9 RA-3 SR-6	GV.OC-02 ID.RA-10 GV.SC-04 GV.SC-06
Training and awareness	6.3	6.2.4 6.2.6 7.2	AT-1,2,3	AT-1,2,3	PR.AT-01 PR.AT-02
Strong contracts	5.20	6.1 7.3	SA-4 SA-9 SR-8	SA-4 SA-9 SR-8	GV.OC-03 GV.SC-05 GV.SC-07
Access control and user roles	5.15	6.2.4 7.3	AC-1,2,3,4,5,6,20 SA-9	AC-1,2,3,4,5,6,20	GV.SC-02 GV.SC-05 PR.AA
Ensuring compliance	5.36	6.1 7.3	CA-1		GV.SC-07 GV.OC-03 GV.OC-04 GV.OC-05
Inventory and documentation of third-party relationships	5.9	6.2	PM-5 CM-8	SR-13	GV.SC-04 GV.SC-07 ID.AM-04 GV.OC-05

ISO/IEC 27036, particularly focused on supplier relationship security, provides comprehensive guidance that aligns significantly with the literature findings. The standard's key principles can be mapped to several best practices identified in the systematic review.

Part 1 of ISO/IEC 27036 (ISO/IEC 27036-1:2021) establishes the foundational concepts that organizations need for securing supplier relationships. It emphasizes the importance of risk-based approaches and continuous monitoring,

directly supporting the literature's recommendations for thorough due diligence and continuous monitoring/evaluation. The standard's emphasis on establishing clear security objectives and requirements aligns with the best practice of strong contracts and clear documentation of third-party relationships.

Part 2 (ISO/IEC 27036-2:2022) outlines requirements for implementing, operating, and improving supplier relationship security. Its focus on establishing clear governance structures and processes aligns with the literature's emphasis on the alignment and integration of cybersecurity policies. The standard recommends creating detailed supplier security requirements (Section 6.1), which supports the best practice of having strong contracts. The standard's emphasis on systematic supplier assessment (Section 6.1.1) aligns with the literature's recommendation for thorough due diligence and assessment.

Information sharing and incident management requirements in ISO/IEC 27036 Part 2 (Sections 6.1.1.2) directly support the literature's emphasis on collaborative information sharing and incident response. The standard's requirements for ongoing monitoring and review (Section 6.3) align with the continuous monitoring and evaluation practices identified in the literature. Furthermore, its focus on access control and user management (Section 6.2) supports the best practice of implementing strong access control measures.

Part 3 (ISO/IEC 27036-3:2023) of the standard specifically addresses ICT supply chain security, providing detailed guidelines for managing risks in complex, multi-tiered supply chains. This aligns with the literature's emphasis on visibility and control in third-party relationships. The standard's recommendations for supply chain mapping and risk assessment support the best practice of maintaining comprehensive inventory and documentation of third-party relationships.

Part 4 (ISO/IEC 27036-4:2016) focuses on cloud services security and provides specific guidance for an increasingly important aspect of third-party relationships. Its recommendations for cloud service provider assessment and monitoring align with the literature's emphasis on continuous monitoring and thorough due diligence. The standard's requirements for clear service level agreements and security requirements in cloud contracts support the best practice of establishing strong contracts.

The comprehensive nature of ISO/IEC 27036 and its alignment with the literature findings suggests that organizations following this standard would implement many of the best practices identified in the systematic review. However, the standard's requirements can be complex and resource-intensive to implement, particularly for smaller organizations. This aligns with the challenge of resource constraints identified in the literature.

Titled "Security and Privacy Controls for Federal Information Systems and Organizations", NIST SP 800-53 provides a set of controls to enhance the security and privacy of information systems. Although there are other controls that are relevant to third-party security, section 3.20 Supply Chain Risk Management focuses on supply chains and third-party security.

NIST SP 800-53 (J. Boyens et al., 2022) recommends that organizations should implement a structured approach to C-SCRM by conducting comprehensive risk assessments of their supply chains. This involves evaluating the security practices of all suppliers, understanding the potential vulnerabilities introduced by third-party components, and assessing the overall security posture of the supply chain. These assessments should be continuous, adapting to emerging threats and

ensuring that suppliers maintain high-security standards throughout the procurement and product lifecycle.

In addition to risk assessments, organizations should establish and maintain robust security controls within their supply chains. This includes integrating security requirements into procurement processes, ensuring that suppliers comply with these requirements, and developing Interconnection Security Agreements (ISAs) for interconnected systems. Continuous monitoring and improvement of these controls are essential to adapting to new threats and maintaining compliance.

NIST SP 800-161 and NIST SP 800-53 both address supply chain risk management but differ in their scope and focus. NIST SP 800-53 provides a broad set of controls for information system security, with Section 3.20 specifically addressing supply chain risk management. In contrast, NIST SP 800-161 is dedicated entirely to supply chain risk management, offering guidelines and practices tailored specifically for identifying, assessing, and mitigating risks in the supply chain (Joint Task Force Interagency Working Group, 2020). While SP 800-53 integrates supply chain considerations into a wider security framework, SP 800-161 focuses solely on supply chain security. The controls in the publication do not add new recommendations that are not given in NIST SP 800-53. However, it provides comprehensive implementation guidance for those recommendations.

The NIST Cybersecurity Framework (National Institute of Standards and Technology, 2024) is a guideline structured around five core functions: Identify, Protect, Detect, Respond, and Recover. These functions provide a high-level taxonomy of cybersecurity outcomes that any organization, regardless of size, sector, or maturity, can use to enhance its cybersecurity posture. The framework outlines specific outcomes but does not prescribe how to achieve them.

The analysis of industry standards and academic literature reveals a comprehensive framework for understanding and implementing effective TPCRM practices. While the standards provide structured guidance for implementation, the literature highlights practical challenges and emerging best practices. Together, these sources emphasize the need for a balanced approach that combines various control elements. The complexity of managing third-party cyber risks, coupled with the need to maintain business efficiency, suggests that organizations would benefit from tools that can simulate different control strategies and their outcomes. This understanding forms the foundation for developing an agent-based model that can explore these dynamics in a controlled environment. The following chapter presents such a model, incorporating the key challenges, controls, and relationships identified through this analysis to create a practical simulation tool for TPCRM decision-making.

CHAPTER 5

DEVELOPMENT OF AN AGENT-BASED MODEL FOR THIRD-PARTY CYBERSECURITY

Agent-based modeling (ABM) is a computational approach used to simulate the interactions of individual agents within a specific environment to observe their collective behavior and emergent patterns. In an ABM, each agent follows a set of predefined rules and possesses unique attributes, such as decision-making abilities, mobility, and the capacity to learn or adapt. These agents interact with one another and their environment, enabling researchers to explore how complex systems evolve. ABM is especially valuable for modeling dynamic systems where the actions and interactions of individuals can produce unpredictable or non-linear results.

ABM is widely used across various fields, including economics, social sciences, biology, and environmental studies, due to its ability to model systems with a high degree of heterogeneity and interdependence among components (Heath et al., 2009). In economics, for instance, ABM simulates market dynamics by modeling individual consumers and firms. In social sciences, it helps to understand the spread of social phenomena like rumors or behaviors. The flexibility and granularity of ABM make it a powerful tool for exploring challenging scenarios to study through traditional analytical methods or experiments.

One of the critical applications of ABM in cybersecurity is in simulating cyber-attacks and defense mechanisms. For example, agents can be programmed to simulate different types of attackers, such as hackers or malicious insiders, who attempt to breach a network. Other agents might represent defensive measures, such as firewalls, intrusion detection systems, or human operators (Ashiku & Dagli,

2020). By running simulations, researchers can observe how attacks propagate through a network, how defenders respond, and under what conditions the network remains secure or becomes compromised.

ABMs also allow for the exploration of "what-if" scenarios, where different security strategies or policies are tested in a simulated environment before being implemented in the real world. This can help organizations identify potential vulnerabilities and optimize their cybersecurity strategies. For instance, an ABM might simulate the spread of a malware infection across an organization's network, allowing IT security teams to evaluate the effectiveness of various containment and eradication strategies (Vestad & Yang, 2024). The next section gives details on the proposed model.

5.1 Agent-based modeling tool: NetLogo

The model is built using NetLogo software. NetLogo is a versatile agent-based modeling platform designed for simulating and analyzing complex systems through the interactions of individual agents. It offers a structured environment where users can define specific rules and behaviors for agents, known as "turtles," which operate within a grid of "patches" representing the environment. The system is overseen by an "observer," who controls and monitors the execution of the model (Wilensky, 1999).

NetLogo uses a simple way to handle time and movement. The environment is like a game board where turtles move around and do things. These turtles can look at their own properties - like checking their own speed or color - and they can also learn new things by interacting with other turtles or looking at the ground (patches) beneath them (Wilensky, 1999).

The whole system moves forward using "ticks". Each tick gives every turtle a chance to do something. It's similar to how in a turn-based game, each player gets to make their move before the next round starts. This tick system keeps everything organized and makes sure all turtles get their fair chance to act. The proposed model uses ticks to simulate time, where one tick represents one month (Wilensky, 1999).

5.2 Proposed model

The proposed model incorporates four types of turtles: the main company, third-party companies, contracts that govern the relationships between companies, and attackers. These turtles represent the key agents involved in simulating third-party cyber risk management. The main company, central to the model, is represented by a single agent, as it serves as the focal point around which the interactions with third parties and potential attackers are simulated. Third-party companies represent external entities with which the main company forms business relationships. Contracts serve as the binding agreements that dictate the terms of these relationships. Attackers represent external threats attempting to exploit vulnerabilities within the network of relationships. Table 11 provides a comprehensive list of these turtle types, along with a detailed description of their potential actions.

The model addresses three key challenges that companies face in developing an effective TPCRM program: high complexity, visibility and control, and resource constraints. These challenges were chosen for two main reasons: they are extensively discussed in the literature, and they are well-suited for computer simulation. High complexity is represented by the number of companies and relationships involved, as well as its impact on the accuracy of processes and the sophistication of cyberattacks. Visibility and control challenge is modeled through monitoring activities, reflecting

the company's ability to track data exchanges with third parties. Additionally, each action in the model incurs costs and has varying levels of effectiveness, simulating real-world resource limitations.

The number of companies and attackers is determined by the complexity parameter. This parameter not only influences the total number of companies and attackers but also affects the distribution of attack strength, simulating new and evolving cyber-attack types. Additionally, as complexity increases, so does the number of engagements sought by the main company.

Against these challenges, the model utilizes three best practices discovered: continuous monitoring and evaluation, thorough due diligence, and strong contracts. As explained before, due diligence is to conduct a risk assessment of a third party before establishing a partnership, examining factors like financial stability, reputation, and general risk profile. Therefore, makes sure the third party complies with relevant regulations and reviews their adherence to cybersecurity standards and certifications. (Abrahams et al., 2024; Ilori et al., 2024; Mohamed, 2024). These practices are chosen between the most recommended ones as they cover the whole lifecycle of a relationship. Due diligence practices are modeled as is, the main company performs due diligence assessments on a selected third party before engaging with it. If the third party conforms to the requirements of the main company, a new contract governing the relationship is created. The main company monitors the relationship and may end the contract prematurely when contract clauses are not met.

Table 11. Turtles and Their Actions

Turtle Type	Action	Description	Controls
The main company	Select a third party	Select a third-party company in a desired tier randomly.	Random selection, no control.
	Evaluate a third party	Perform due diligence on the selected third party.	Due diligence level (0 to 3): Third party assessment thoroughness level, Due diligence ratio (0.0 to 1.0): The probability of conducting due diligence assessments for each potential third-party relationship.
	Create contract	Create a new contract using contract controls with the selected third-party.	Risk appetite (1-4): Maximum acceptable third-party risk tier company to start a contract, Time: How many ticks a contract will live, Breach termination clause (true or false): Determines whether the contract automatically terminates if the third-party experiences a security breach, Monitoring level (0 to 3): Security monitoring intensity level, Monitoring ratio (0.0 to 1.0): Determines the proportion of third-party relationships that undergo security monitoring. Risk control (true or false): Determines whether the contract automatically terminates if the risk tier of the third-party dips below the acceptable risk tier.
	Cancel contract	Cancel/delete the contract.	No control.
	Renew contract	Renew the contract using contract controls.	ISO requirement (true or false): Only renew the contract if the third party has ISO 27001 certification.
	Back up data	Back up data incrementally.	Back up rate (in ticks): How often the company performs backups.
Third party company	Update risk tier	Update the cybersecurity capability parameters, new parameters are determined randomly, based on the previous parameters.	Happens in each tick, no control.
	Get ISO27001	Receive ISO27001 certification.	Happens in each tick, random possibility only for companies with high cybersecurity capabilities.
	Check for breach	Check itself against breaches, success depends on the cybersecurity capabilities of the third-party company.	Happens in each tick, no control
Contract	Monitor contract	Monitor the relationship against breaches and other requirements.	Uses parameters in the “Create contract” action.
	Breach propagation	A breach from third party company can propagate to the main company	Happens in each tick for breached third parties in contract, no control.
Attacker	Attack	Attack to a third-party company	Happens in each tick, random selection, no control.

The main company is modeled as the administrator of its third-party relationships. Business and other functions of a standard company are not included in the simulation to reduce complexity and increase focus on the subject matter.

The third-party companies modeled in this simulation represent the various external entities that the main company may engage with, such as vendors, cloud service providers, suppliers, and more. These third-party companies are structured across three distinct tiers, which reflect their level of closeness and criticality to the main company's operations. The model is designed to enable different controls for different tier third parties.

Based on Ghadge et al. (2019), the three tiers are designed to capture the different levels of business criticality and cyber risk propagation associated with third-party relationships. Tier 1 companies are the most closely integrated and business-critical partners, while Tier 3 companies have a more peripheral relationship with the primary organization. Figure 8 demonstrates the tiered design of the model.

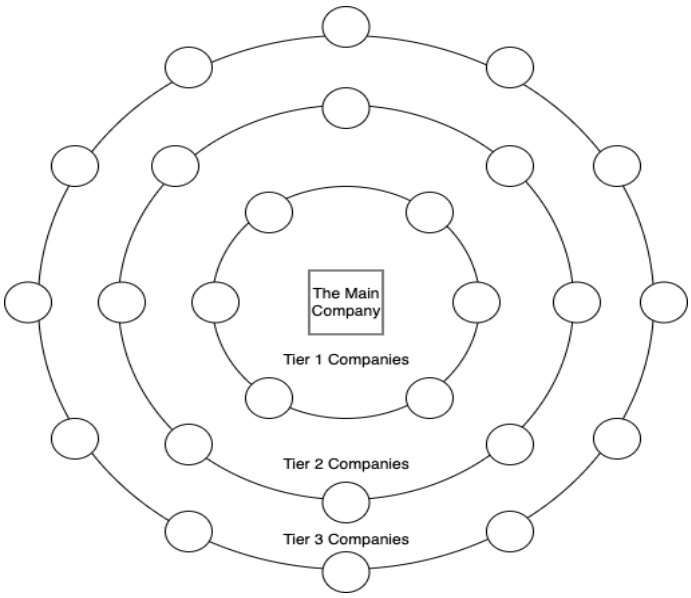

Figure 8. The tiered design of the model

Specifically:

- Tier 1 companies represent the main company's closest third-party entities, with a high degree of access, integration, and business criticality. These relationships have the highest potential for rapid risk propagation.
- Tier 2 companies have a moderate level of integration and criticality, posing moderate cyber risk exposure to the main company.
- Tier 3 companies are the more peripheral third-party entities, with a lower level of access and business impact, but still presenting cyber risks that need to be managed.

A key aspect of the model is its ability to apply varying levels of controls and management practices to the different tiers of third-party companies. This allows the model to simulate the nuanced nature of third-party relationships and their varying levels of cyber risk impact on the main company. It reflects the real-world challenges organizations face in securing their extended network of partners and suppliers.

Specifically, the model allows the main company to set distinct parameters for each tier of third-party companies, including:

- Due diligence levels: The thoroughness of the initial assessment and evaluation can be adjusted based on the third party's tier. For example, the main company may choose to conduct more comprehensive, higher-cost due diligence on Tier 1 partners versus more streamlined assessments for Tier 3 companies.
- Monitoring levels: The model enables the main company to implement different levels of continuous monitoring, from basic monitoring for Tier 3 partners to more advanced, real-time monitoring for the Tier 1 critical relationships.

- Risk appetites: The main company can set distinct risk appetite thresholds for each tier, allowing it to be more or less risk-averse when engaging with third-parties based on their level of importance and potential impact.
- Contract terms: Parameters like required ISO 27001 certification, breach clauses, and contract durations can be tailored to the specific tier of the third-party company.

Figure 9 shows the user interface of the model with controls and parameters. The next section details the parameters and controls of the model.

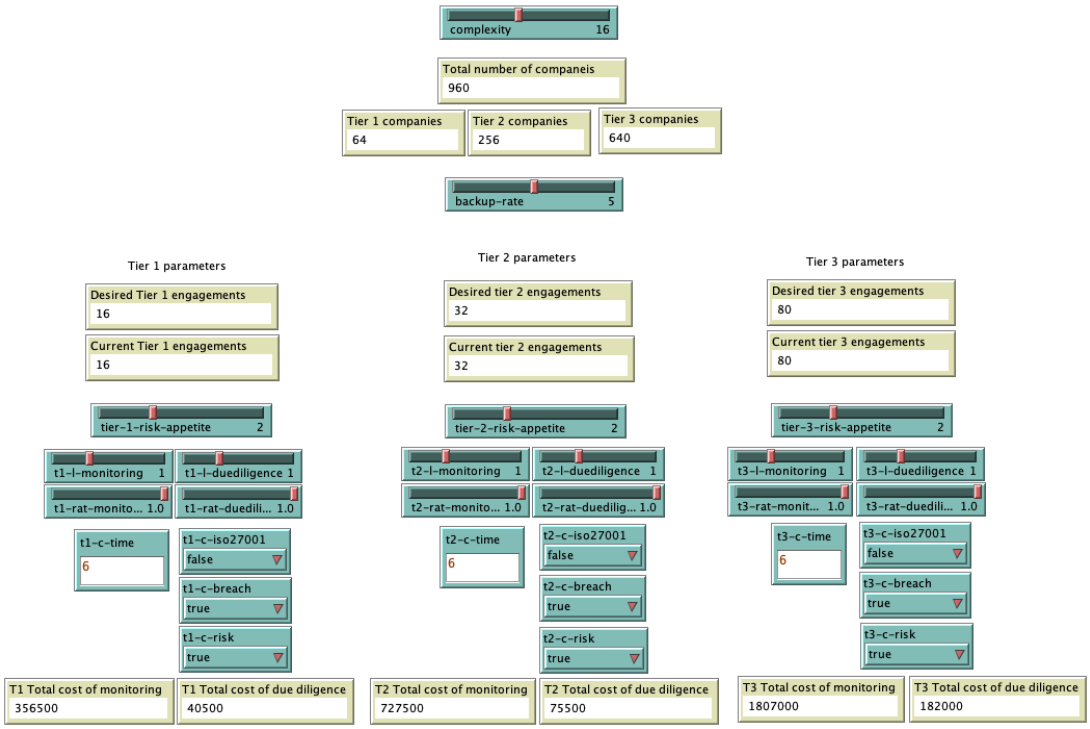

Figure 9. Controls and parameters on the model interface

5.3 Agent-based model parameters and controls

As discussed above, the model is set up using a complexity parameter. This parameter can be chosen between 5 and 30 at the beginning of the simulation. The main company has a target number of relationships that it strives to maintain during

each tick of the simulation which is calculated using the complexity parameter. The number of third-party companies and the number of attackers is also calculated using the parameter. The calculations used in the model are chosen as follows:

- Tier 1 companies: $complexity^2 \div 4$
- Targeted tier 1 relationships: $complexity$,
- Tier 2 companies: $complexity^2$,
- Targeted tier 2 relationships: $complexity \times 2$,
- Tier 3 companies: $complexity^2 \times 2.5$,
- Targeted tier 3 relationships: $complexity \times 5$,
- Attackers: $complexity^3$,
- Attack power: Random normal distribution,
    - If complexity is lower than or equal to 20, the mean is 13, the standard deviation is 5
    - If the complexity is greater than 20, the mean is 13, the standard deviation is 7.
- Number of attacks: $random(complexity^{1.5})$

complexity refers to the complexity level set in the model. *random* is a NetLogo function that returns a random integer value between 0 and the input number. The numbers are chosen arbitrarily.

Third-party companies represent the external entities with which the main company can engage. These turtles are assigned a cybersecurity capability rating based on the framework developed by Malaivongs et al. (2022). Their research analyzed previous studies and security standards to establish controls for assessing a company's cybersecurity capability using five key enablers: Organizational Direction and Process, Organizational Structure, Automation Tools, Performance Evaluation,

and Reporting. The framework categorizes each enabler into six capability tiers, ranging from 0 to 5. This thesis adopts this measurement system as turtle variables, modeling each third party's cybersecurity capabilities according to these tiers.

The third-party companies in the model are assigned random initial values ranging from 0 to 5 for each of the five cybersecurity enablers. These enabler values represent the third-party company's overall cybersecurity capability and maturity.

Over the course of each simulation tick, these enabler values have a probability of changing. Specifically, there is a 25% chance a value will increase, a 25% chance it will decrease, and a 50% chance it will remain the same. This dynamic fluctuation of third-party companies' cybersecurity capabilities reflects the real-world challenges of maintaining consistent security postures.

The model assigns each third-party company a risk tier level based on the summation of their five cybersecurity enabler values. Specifically, the risk tier is determined using the following calculation:

- If the total of the five enabler values is 19 or greater, the third-party company is assigned a risk tier of 1, indicating the lowest level of risk.
- If the total enabler value is between 13 and 18, the third party is given a risk tier of 2, representing a moderate level of risk.
- When the total enabler value is above 7 but less than 13, the third party is classified as risk tier 3, signifying a higher risk profile.
- Finally, if the total enabler value is 7 or below, the third-party company is assigned the highest risk tier of 4.

The model also introduces the possibility for third-party companies to obtain an ISO 27001 certification, which is a globally recognized standard for information security management systems. When a third-party company achieves this certification, its

enabler values remain constant and do not fluctuate for a period of 12 simulation ticks. This represents the increased stability and security assurances provided by the ISO/IEC 27001:2022 standard.

The main company in the model is designed to randomly select third-party companies to form new relationships to achieve its targeted number of relationships. The number of third-party companies selected is determined by the number of unfulfilled relationships. This unfulfilled relationship count is calculated by taking the main company's targeted relationship count and subtracting the number of current active relationships.

Specifically, the model tracks the main company's targeted number of relationships for each tier of third-party companies (tier 1, tier 2, tier 3). Based on these target relationship counts; the model determines how many additional relationships the main company needs to establish in each tier. The main company then randomly selects unengaged third-party companies from the appropriate tiers to engage with, up to the number of unfulfilled relationships.

The primary objective of the main company is to continuously meet its targeted number of relationships by forming and maintaining secure third-party partnerships. This objective is measured using a variable called business effectiveness. The effectiveness means the ratio of active relationships over targeted relationships. For example, if the company targets to have 20 relationships, but it only has 10 at a given tick, the business effectiveness for that tick is 50%. This is calculated for each tier independently, and then summed up using this algorithm:

$$busEfT1 \times (13 \div 26) + busEfT2 \times (8 \div 26) + busEfT3 \times (5 \div 26)$$

Where *busEfT* values represent the business effectiveness of respective tiers. The ratios are chosen arbitrarily to reflect the business effects of various tiers.

The main company performs due diligence assessments against the selected third-party companies. The quality and rigor of these due diligence evaluations are controlled through the parameter called due diligence level. The levels and costs are selected based on sector reports (Barrus, 2024). The acquired data is manipulated to simulate due diligence precision using this algorithm:

$$((4 - level)^2 \div 2) - \left(random((4 - level)^2)\right)$$

random is a NetLogo function that returns a random integer between 0 and the number provided. *level* means the due diligence level. The numbers are chosen arbitrarily, taking into account the maximum cybersecurity capability of 25.

At the lowest level, a due diligence level of zero indicates that the main company performs no assessment at all on the third party before engaging with them.

As the due diligence level increases, the quality and comprehensiveness of the evaluation also rises. A due diligence level of one represents an automated, lower-cost, $500, assessment that provides basic data, but with low precision.

Moving up to a due diligence level of two, the main company conducts a more extensive, manual review of the third party, with medium costs, $3.000, and medium-quality information.

Finally, at the highest due diligence level of three, the main company performs a comprehensive, onsite audit of the third-party company. This in-depth assessment comes at a significantly higher cost, $15.000, but provides the main company with high-quality, high-precision data about the third party's security posture and risk profile.

These varying due diligence levels allow the model to simulate the tradeoffs organizations face between the thoroughness of their third-party evaluations and the resources required to conduct them.

In addition to the due diligence level, the model also includes a parameter to control the ratio at which the main company chooses to perform these assessments. This ratio is set between 0 and 1, with increments of 0.1. A ratio of 0 indicates that the main company will never conduct a due diligence evaluation, regardless of the selected third party and the due diligence level. Conversely, a ratio of 1 means the main company will always perform the due diligence assessment before engaging with a new third-party company. The ratios between these extremes allow the model to simulate more nuanced decision-making by the main company. For example, a ratio of 0.5 would result in the main company assessing half of the selected third parties before deciding whether to form a new relationship. This parameter gives the model flexibility to explore how the main company's due diligence practices, in terms of both quality and frequency, impact its ability to manage third-party cyber risks effectively.

The main company in the model has a defined risk appetite that guides its third-party engagement decisions. This risk appetite is represented as a numerical value that the main company uses to evaluate the acceptability of a potential third-party partner.

The risk appetite parameter is set separately for each tier of third-party companies. For example, the main company may have a risk appetite of 2 for Tier 1 third parties, 3 for Tier 2, and 4 for Tier 3. These values indicate the maximum risk profile the main company is willing to accept when engaging with companies in each respective tier.

During the process of selecting and evaluating third parties, the main company compares the assessed risk tier of the potential partner against its own risk appetite. If the third party's risk profile is at or below the main company's appetite for

that tier, the relationship is deemed acceptable, and the main company will proceed with onboarding the third party. However, if the third party's risk tier exceeds the main company's appetite, the main company will reject that engagement opportunity.

This risk appetite parameter allows the model to simulate how an organization's willingness to accept third-party cyber risks can influence the composition of its partnership network. A more conservative risk appetite will lead the main company to be more selective, engaging only with the lowest-risk third parties. However, being too aggressive in finding the lowest risk tier partners may result in unfulfilled partnerships, as there may not be enough third parties with those risk tiers. Conversely, a higher risk appetite indicates the main company is willing to work with riskier third-party entities to potentially gain business advantages, but at the cost of increased cyber exposure.

If the main company's due diligence process determines that a selected third-party company falls within the main company's acceptable risk threshold, a contract will be established between the two entities.

This contract establishes the specific parameters that will govern the relationship between the main company and the third party. These contract parameters include factors such as the required monitoring level, the contract duration, any ISO 27001 certification requirements, and clauses related to breach consequences and risk thresholds.

The model simulates the complete lifecycle of contracts established between the main company and the third-party entities. This contract management process is a critical component of the main company's third-party cyber risk management strategy.

When the main company selects a third-party company to engage with, based on the due diligence assessment and risk appetite criteria, a new contract is created between the two parties. This contract outlines the specific terms and conditions governing the relationship, including:

- Contract duration: The length of time the contract will remain active, which varies based on the third party's tier level.
- Monitoring requirements: The level of continuous monitoring the main company will apply to the third party, ranging from basic monitoring to more advanced, real-time oversight.
- ISO/IEC 27001 certification: Whether the third party must maintain a valid ISO 27001 certification for the contract to renew after its duration.
- Breach clauses: Conditions under which the contract can be terminated prematurely due to a confirmed data breach at the third-party company.
- Risk thresholds: The maximum acceptable risk tier for the third party, beyond which the contract will be canceled.

During the active contract period, the main company continuously monitors the third-party company's security posture and compliance with the established terms. The monitoring process involves regularly assessing the third party's cybersecurity enabler values and evaluating their overall risk tier.

The accuracy and effectiveness of this monitoring process are determined by the specific monitoring level defined in the contract, similar to the due diligence level. Higher monitoring levels equate to more sophisticated, reliable detection capabilities, but also incur greater costs for the main company.

Monitoring level 1 represents a basic, lower-cost monitoring solution. It involves setting up a simple Security Operations Center (SOC) to oversee the third

party's activities. The initial setup cost for this level 1 monitoring is $2,000, with an ongoing per-contract cost of $500 per tick.

The key limitation of this basic monitoring level is that it only detects breaches at the third-party company 50% of the time. In other words, there is a 50% chance that a data breach occurring at the third party will go unnoticed by the level 1 monitoring system. There is a chance that some security incidents could go unnoticed, potentially exposing the main company to unmitigated risks.

Monitoring level 2 is a more robust monitoring approach, it involves a dedicated, medium-cost SOC. The initial setup for this level is $8,000, with a per-contract cost of $1,000 per tick.

At this monitoring level, the main company can detect all data breaches that occur at the third-party company. However, the mitigation of these breaches is not guaranteed to be fully effective, as the monitoring may not provide complete visibility and control.

Monitoring level 3, the highest monitoring level in the model is a highly advanced, enterprise-grade SOC. This comes with a significant initial investment of $20,000, plus a per-contract cost of $4,000 per tick.

This level 3 monitoring provides the main company with the highest degree of visibility and control. It ensures that all data breaches at the third party are both detected and increases mitigation chance, giving the main company the strongest possible protection against cyber risks originating from its partner ecosystem.

Monitoring costs and levels are determined using sector reports (Kobalt.io, n.d.; VC3, 2024). Their effectiveness is determined arbitrarily.

If the monitoring activities reveal that the third-party company's risk tier has exceeded the contractual threshold, or if a data breach is detected, the main company

has the ability to terminate the contract prematurely, as predefined in the contract controls.

Finally, the main company backups data in each given tick. Each backup costs 3.000$ to set up, and 2$ for each tick for each GB of data backed up (Optimal Networks, n.d.). The data is created in the relationships with the third parties, and the amount of data depends on the third party's tier.

In addition to the contract management and monitoring processes, the model also simulates the main company's data backup practices. The main company backs up its data incrementally, but the frequency of these backup operations is controlled by a parameter called "*backup-rate*".

Each backup operation carries a setup cost of $3,000. Additionally, there is an ongoing per-tick cost of $2 for every gigabyte (GB) of data that is backed up. Backup costs are determined using sector reports (Optimal Networks, n.d.). In the event of a breach, the main company loses all non-backed-up data. Estimating the value of lost data is challenging, as there are no agreed-upon industry standards or studies that provide definitive figures. For the purposes of this model, it is assumed that the value of the data is 5 times greater (10$) than the cost of the backups. However, the actual cost of data loss can vary significantly depending on the type of data, its sensitivity, and the overall impact on the organization.

The amount of data that the main company needs to back up is directly tied to its relationships with third-party companies. Specifically, the data size is dependent on the tier level of the third-party entities the main company is engaged with. Tier 1 companies generate 10 GB of data per tick, Tier 2 companies generate 5 GB per tick, and Tier 3 companies generate 2 GB per tick.

By backing up this data, the main company aims to protect itself against potential data loss in the event of a successful cyber-attack on one of its third-party partners. The backup process helps to mitigate the financial and operational impact of such breaches, as the main company can recover the lost data.

However, the backup process itself incurs significant costs, both in the initial setup and the ongoing per-tick expenses. This reflects the real-world trade-offs organizations face in balancing their data protection efforts with the financial and resource constraints of their cybersecurity programs.

Attackers are the third type of turtle in the model. They have a single variable, attack power, which is assigned randomly based on a normal distribution. For each tick, a certain number of attackers are randomly chosen to target a random third-party company. If an attacker's power exceeds the company's total enabler score, the attack is successful, resulting in a breach.

In addition to the third-party companies and the main company itself, the model also incorporates a population of attacker agents. These attackers represent the external cyber threats that may target the third-party entities and, by extension, the main company. The attackers in the model are assigned a variable called "*attack-power*" which is randomly generated with a normal distribution.

The complexity parameter in the model influences the distribution of the attackers' attack power. As the complexity increases, the normal distribution from which the attack power is drawn shifts towards higher, more powerful values. This simulates the real-world trend of cyber threats becoming more advanced and capable in high-complexity areas.

During each simulation tick, a certain number of attackers, determined by the complexity level, are randomly selected to target randomly chosen third-party companies. The algorithm of attacker selection is as follows:

$$nOf\ random(complexity^{1.5})\ attackers$$

nOf is a NetLogo function that randomly selects a given number of turtles from the given breed. What this code does is randomly select $complexity^{1.5}$ attackers.

Each selected attacker attacks a random third party. If the attacker's power exceeds the total cybersecurity enabler score of the target third party, the attack is successful, resulting in a data breach at that third-party company.

These successful attacks on third-party entities can then propagate to the main company, with the propagation timeline depending on the tier level of the breached third party. If the breach originates from a Tier 1 third-party company, it propagates to the main company in just one simulation tick. Breaches from Tier 2 third parties take two ticks to reach the main company, while those coming from Tier 3 third parties require four ticks to propagate. When a breach does make its way through to the main company, it becomes breached as well, losing all of its data that was not previously backed up. This breach of the main company's systems has significant operational impacts, making the main company inoperable, with the duration of the state dependent on the tier of the third party from which the breach originated. A Tier 1 third-party breach leaves the main company inoperational for four simulation ticks, while a Tier 2 third-party breach results in a 2-tick inoperational period, and a Tier 3 third-party breach causes just a 1-tick disruption.

The financial impact of the breach is calculated based on IBM’s 2024 report on the cost of a data breach, which estimates the average annual cost at $4.88

million. To approximate the cost per month, this figure is divided by 12, resulting in $400,000 per tick in the model.

The third-party companies in the model are designed to continuously monitor their own cybersecurity posture and take actions to detect and mitigate potential data breaches. This self-monitoring and mitigation process is a key component of the simulation.

Each third-party company checks itself for signs of a data breach in each tick. The success rate of this self-detection is directly tied to the strength of the company's cybersecurity enablers. Third-party companies with higher cumulative enabler scores have a greater likelihood of detecting if they have been breached and mitigating it. The algorithm for successfully detecting and mitigating a breach is as follows:

$$randomFloat(1) < (totalScore + bonus) \div 30$$

randomFloat is a NetLogo function that returns a random floating number between zero and the number provided, in this case, any number between 0.0 and 1.0. *totalScore* represents the cumulative cybersecurity capability score of the third party. *bonus* only comes from level 3 monitoring activities with a value of three. When the result of this calculation is true, the breach is successfully mitigated. The number 30 is selected purposely to be greater than the maximum capability score of 25, to make even the most secure companies susceptible to breaches, as a simulation of zero-day vulnerabilities.

The model also incorporates the impact of the main company's monitoring activities on the third-party's breach detection and mitigation. If the main company has an active monitoring contract with a third-party, the monitoring level specified in the contract affects the third-party's breach awareness and response.

Higher monitoring levels, such as the advanced Security Operations Center (SOC) in Monitoring Level 3, provide the main company with greater visibility into the third-party's security posture. This increased monitoring accuracy helps the third-party company detect breaches more reliably. Additionally, the more sophisticated monitoring allows for more effective mitigation of any detected breaches.

Conversely, lower monitoring levels, like the basic SOC in Monitoring Level 1, have a reduced ability to identify security incidents at the third-party. This can leave some breaches undetected, exposing the main company to unmitigated risks originating from its partner ecosystem.

The model code can be found in the Appendix, Figure 10 shows the main decisions and actions simulated in the model.

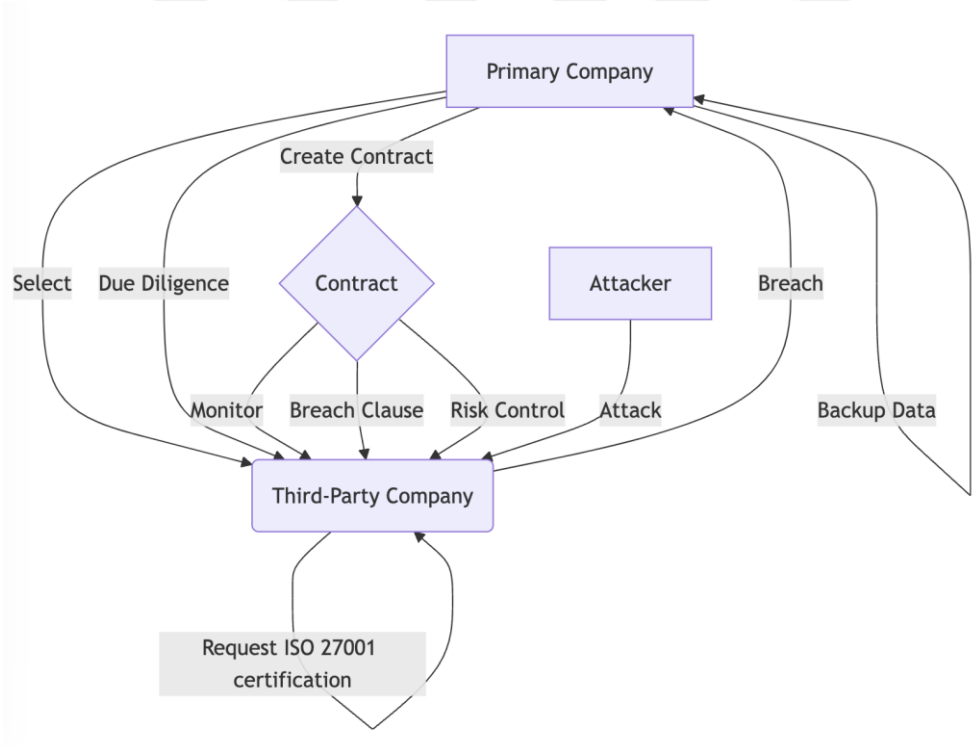

Figure 10. Decisions and actions simulated in the model

5.4 Case study test scenarios

For the purposes of this thesis, we have created an imaginary corporation called AutoSecure Inc. This fictional company serves as a model to explore third-party cybersecurity challenges and risk management strategies in a realistic business setting. AutoSecure Inc. relies on a network of third-party vendors to provide essential services, including parts manufacturing, logistics, IT support, and data storage. As the company expands its partnerships to enhance production and service quality, it faces increasing cybersecurity risks due to the larger attack surface introduced by these external relationships.

Each scenario is executed over 36 simulated months (ticks), with five simulation runs for each setup to ensure statistical reliability. Throughout all scenarios, certain parameters remained constant unless specifically varied as part of the scenario. Key metrics—such as breach frequency, breach cost, and control cost—are collected to quantify the relationship between each scenario's parameters and their effects on TPCRM outcomes. This approach provides a robust basis for assessing each scenario's impact on AutoSecure Inc.'s third-party cyber risk management.

These scenarios are crafted to simulate real-world decision-making scenarios for AutoSecure Inc., providing practical insights into scaling third-party networks, defining risk appetite, optimizing control levels, and implementing integrated strategies. Although some simplifications are made in parameter selection, the scenarios aim to reveal patterns that are broadly applicable across different organizations, especially those in complex sectors like automotive. Each scenario isolates specific TPCRM factors to evaluate how different controls and risk management strategies affect security outcomes and costs. These scenarios simulate

real-world conditions to guide AutoSecure Inc. in strengthening its third-party cybersecurity practices.

Together, these scenarios offer a comprehensive evaluation of the model's ability to simulate real-world TPCRM challenges and generate actionable insights for AutoSecure Inc. The findings from these scenarios inform best practices for managing third-party cyber risks, allowing AutoSecure Inc. to balance costs, operational impact, and security investment effectively. These scenarios were specifically chosen based on the key challenges identified in the literature review.

5.4.1 Scenario 1, complexity impact on cyber risk exposure

As AutoSecure Inc. grows, so does its network of suppliers and partners. The company now works with various third parties across production, logistics, and IT services. This increasing complexity in its third-party network raises concerns about potential vulnerabilities and increased risk exposure. The first scenario examines the impact of complexity on cyber risk exposure.

AutoSecure Inc. currently partners with eight third-party vendors, but as its production and sales expand, it plans to onboard additional partners. This scenario simulates three different levels of network complexity: 8, 17, and 26. Other parameters, such as monitoring intensity and risk appetite, remain constant, isolating the impact of network complexity on cyber risk.

The goal of this scenario is to evaluate how increasing complexity within AutoSecure Inc.'s third-party network affects its overall cyber risk exposure. It is anticipated that as AutoSecure Inc.'s network complexity increases, breach frequency and associated costs will rise, reflecting the larger attack surface. This scenario helps determine at what point additional investments in monitoring and

controls become necessary to manage the heightened risks of a complex third-party ecosystem.

5.4.2 Scenario 2, risk appetite and security posture

With increasing industry competition, AutoSecure Inc. must balance security with cost efficiency to stay profitable. The company's top management is re-evaluating its risk appetite, especially regarding vendor management. AutoSecure Inc. has traditionally maintained a moderate risk appetite, but leadership is exploring how different levels of risk appetite might impact business effectiveness and breach risks.

Risk appetite refers to the overall amount and type of risk an organization is willing to accept to pursue its strategic objectives. It reflects the organization's general attitude towards risk. For instance, a company with a high-risk appetite may prioritize aggressive growth, indicating a willingness to take on significant risks if the potential rewards align with its strategic goals.

This scenario models four distinct levels of risk appetite, ranging from highly restrictive (Level 1) to highly permissive (Level 4). By holding other parameters constant, we can isolate the impact of risk appetite on breach frequency and associated costs. Generally, lower risk appetite levels (more restrictive) lead to decreased breach frequency but may hinder the ability to achieve business targets. This analysis assists AutoSecure Inc. in understanding the practical implications of various risk appetites.

5.4.3 Scenario 3, control level effectiveness and cost-benefit analysis

AutoSecure Inc. has been weighing the costs and benefits of intensifying its cybersecurity controls for third-party vendors. Given its limited resources, the company needs to determine the optimal level of security investment to achieve adequate protection without excessive expenses.

Four control configurations are tested, from minimal controls to maximum security measures. This scenario compares the outcomes across these levels, analyzing the trade-offs between breach costs and control expenses. The results guide AutoSecure Inc. in determining the level of controls that optimally balance cost and risk.

The goal is to analyze the relationship between the intensity of cybersecurity controls and the resulting cost-effectiveness, helping AutoSecure Inc. balance protection and financial expenditure. Higher control levels are anticipated to initially reduce breach costs significantly but with diminishing returns at maximum control levels. This scenario is designed to help AutoSecure Inc. identify the most cost-effective level of security controls, ensuring adequate protection without unnecessary spending.

5.4.4 Scenario 4, the effectiveness of integrated control strategies

AutoSecure Inc. has implemented basic security measures for individual vendors, but recent industry breaches have prompted the company to consider a more integrated approach. AutoSecure Inc. wants to know whether combining strategies like monitoring and contractual clauses will provide a stronger defense than isolated controls.

This scenario tests four control combinations: due diligence alone, due monitoring alone, monitoring with contract clauses, and a fully integrated control strategy. The scenario’s purpose is to evaluate how these configurations affect breach frequency, cost, and operational impact, helping AutoSecure Inc. determine the most efficient security approach for managing third-party risks.

This scenario aims to assess the effectiveness of integrated control strategies, identifying which combinations of controls provide AutoSecure Inc. with the most comprehensive protection and operational efficiency. It is expected that integrated control strategies, such as monitoring combined with due diligence, are to offer the most effective risk reduction. This scenario aims to determine whether a layered approach enhances AutoSecure Inc.'s protection against third-party cyber threats without excessive resource expenditure.

The next chapter presents and discusses the simulation results for the given scenarios.

CHAPTER 6

SIMULATION RESULTS AND ANALYSIS

In this chapter, we present and analyze the outcomes generated by the agent-based model (ABM) developed for modeling third-party cybersecurity risks. The model simulates various scenarios, as outlined in Chapter 5, each designed to isolate and examine critical factors in third-party cyber risk management. These factors include network complexity, organizational risk appetite, control intensity, and control strategies.

By exploring the results of these simulations, we aim to provide insights into how each parameter impacts key risk metrics, such as breach frequency, breach costs, control effectiveness, and overall control costs. This analysis enables us to evaluate the effectiveness of different strategies and identify the optimal balance of security measures in complex third-party environments.

The results serve as a foundation for actionable recommendations, helping organizations enhance their third-party cybersecurity practices using empirical data and insights from the model.

6.1 Scenario 1, complexity impact on cyber risk exposure

Complexity represents one of the most significant challenges in third-party risk management, as identified in the literature review. In the model, complexity directly influences the number of third-party relationships, the sophistication of cyber-attacks, and the overall attack surface of the organization.

In this scenario, all security controls are deliberately set to zero to isolate the impact of complexity alone. Three complexity levels are tested: 8 (low complexity),

17 (moderate complexity), and 26 (high complexity). These values were chosen to represent different organizational scales, with 8 representing small businesses with limited third-party relationships, 17 representing medium-sized organizations, and 26 representing large enterprises with extensive third-party networks. Table 12 presents the parameters used in this scenario, while Figure 11 shows how breach costs increase with complexity.

Table 12. Model Parameters, Scenario 1

Parameter	Value
Complexity	Test 1: 8 Test 2: 17 Test 3: 26
Backup rate	0
Due diligence levels	All tiers, level 0, ratio 0.0
Monitoring levels	All tiers, level 0, ratio 0.0
Risk appetites	All tiers, 4
Contract controls	ISO27001: False Breach: False Risk: False

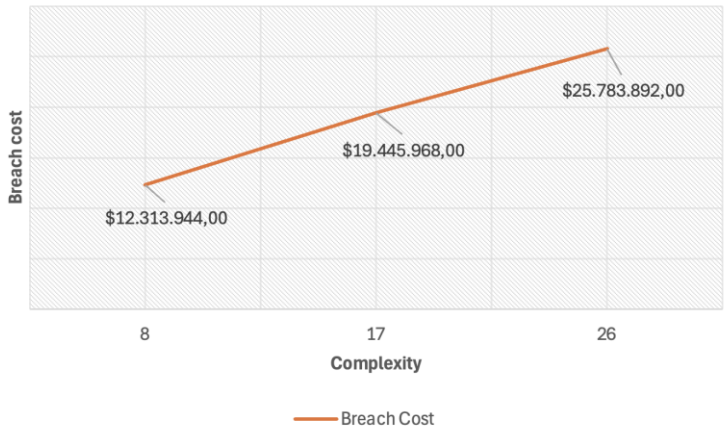

Figure 11. Breach cost for various complexities

The results demonstrate a clear correlation between complexity and breach costs. As complexity increases from 8 to 17, breach costs rise by approximately 66%. The increase from 17 to 26 results in an additional 30% rise in breach costs.

6.2 Scenario 2, risk appetite and security posture

Risk appetite is a fundamental parameter that determines an organization's willingness to take third-party cyber risks. It directly influences which third-party relationships an organization will accept and maintain.

For this scenario, all controls are set to level 1 to provide a baseline security posture, while risk appetites are varied across four levels. Risk appetite level 1 represents the most restrictive position, only accepting the most secure third parties, while level 4 represents the most permissive stance, accepting third parties with higher risk profiles. Table 13 outlines the specific parameters used in this scenario.

The results, illustrated in Figure 12, reveal a complex relationship between risk appetite and overall security posture. While lower risk appetites resulted in significantly lower breach costs, they also led to higher control costs and decreased business efficiency. The shift from risk appetite 1 to 2 produced the most substantial improvement in business effectiveness with a slight impact on control costs. Moving from risk appetite 2 to 3 gave slight changes in all results. However, moving to risk appetite 4 caused breach costs to rise substantially, and business effectiveness to slightly decline.

Table 13. Model Parameters, Scenario 2

Parameter	Value
Complexity	8
Backup rate	5
Due diligence levels	All tiers, level 1, ratio 1.0
Monitoring levels	All tiers, level 1, ratio 1.0
Risk appetites	Test 1: All tiers, 1 Test 2: All tiers, 2 Test 3: All tiers, 3 Test 4: All tiers, 4
Contract controls	ISO27001: False Breach: False Risk: False

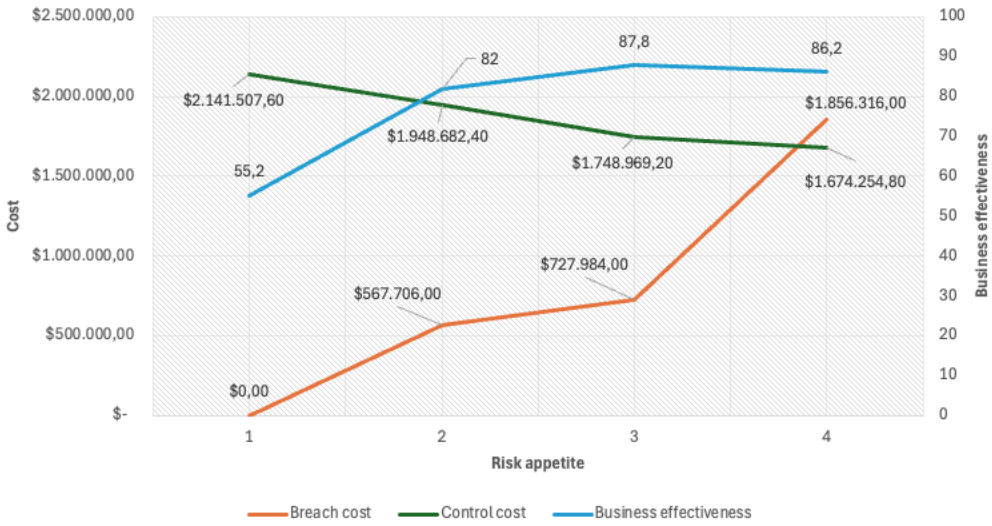

Figure 12. Risk appetite effect

6.3 Scenario 3, control level effectiveness and cost-benefit analysis

The effectiveness of monitoring and due diligence controls represents a critical consideration in TPCRM strategies. These controls constitute significant investments for organizations, and they are the primary best practices simulated in the model. This scenario examines how different levels of these controls affect both breach costs and total organizational expenses. The parameters used in this scenario are presented in Table 14.

In this scenario, control levels were adjusted from 0 (no controls) to 3 (maximum controls), with each level representing increasing sophistication and cost of implementation. Level 0 represents no formal monitoring or due diligence processes. Level 1 implements basic controls such as simple assessments and monitoring. Level 2 introduces more detailed assessments and mediocre monitoring capabilities. Level 3 represents comprehensive, continuous monitoring and thorough due diligence processes.

The results, shown in Figure 13, reveal a significant difference between having no controls (Level 0) and implementing even basic controls (Level 1). The

introduction of Level 1 controls reduced breach costs almost 99%. However, the incremental benefits of Level 2 and 3 controls showed diminishing returns. While these higher-level controls did further reduce breach costs, the increase in control costs was disproportionately higher. Level 3 controls, while providing the highest security, resulted in control costs nearly equal to the breach cost of Level 1.

Table 14. Model Parameters, Scenario 3

Parameter	Value
Complexity	17
Backup rate	5
Due diligence levels	Test 1: All tiers, level 0, ratio 0.0 Test 2: All tiers, level 1, ratio 1.0 Test 3: All tiers, level 2, ratio 1.0 Test 4: All tiers, level 3, ratio 1.0
Monitoring levels	Test 1: All tiers, level 0, ratio 0.0 Test 2: All tiers, level 1, ratio 1.0 Test 3: All tiers, level 2, ratio 1.0 Test 4: All tiers, level 3, ratio 1.0
Risk appetites	Tier 1: 2 Tier 2: 3 Tier 3: 4
Contract controls	ISO27001: False Breach: False Risk: False

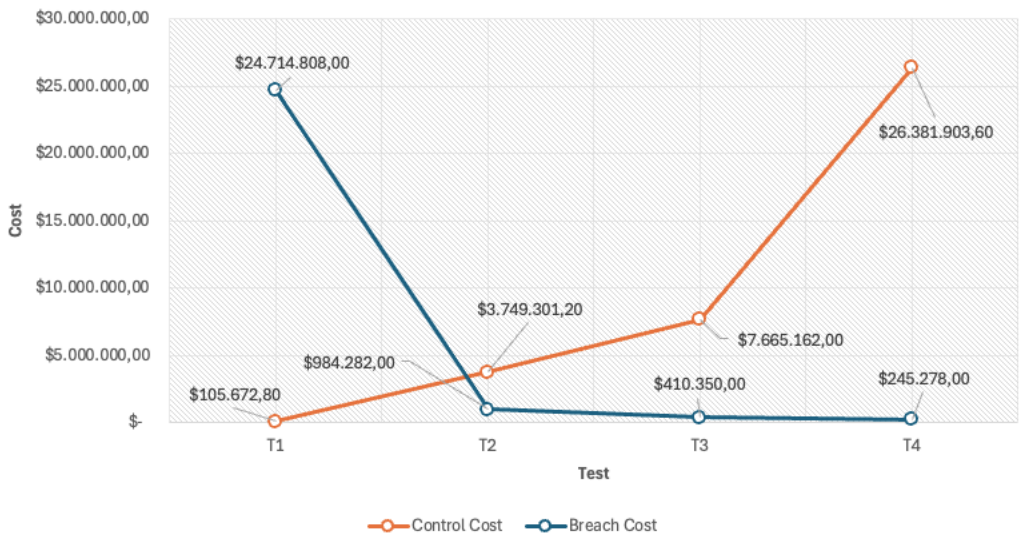

Figure 13. Control level effect on costs

6.4 Scenario 4, the effectiveness of integrated control strategies

Understanding the relative effectiveness of different control types is crucial for organizations to optimize their TPCRM investments. This scenario compares various combinations of monitoring and due diligence controls to determine which approaches provide the best balance of security and cost-effectiveness.

Five control schemes were tested to identify the most effective approach. The first two tests isolated the impact of due diligence, implementing it at Level 1 and Level 3 respectively, with no other controls active. The third test examined monitoring alone at Level 1, while the fourth test combined Level 1 monitoring with active contract clauses. The final test integrated all controls - monitoring, due diligence, and contract clauses - at Level 1. Table 15 presents the controls used for the tests.

The results, illustrated in Figures 14 and 15, demonstrate that isolated controls are significantly less effective than integrated approaches. Due diligence alone, even at Level 3, had a minimal effect on the breach cost, while consuming substantial resources. Monitoring alone performed slightly better, achieving around 25% reduction in breach costs, but still left significant vulnerabilities. However, when monitoring was combined with active contract clauses, breach costs decreased by almost 80%.

The most effective approach proved to be the integration of all three control types - monitoring, due diligence, and contract clauses - at Level 1. This combination achieved a 99% reduction in breach costs while maintaining great business efficiency. The results suggest that organizations should focus on implementing a balanced combination of controls rather than maximizing any single control type.

These findings highlight the importance of a holistic approach to TPCRM, where different control types complement each other to create a more robust security posture. The results also emphasize that more expensive controls don't necessarily translate to better outcomes and that careful consideration should be given to how different controls interact and support each other.

Table 15. Model Parameters, Scenario 4

Parameter	Value
Complexity	17
Backup rate	5
Due diligence levels	Test 1: All tiers, level 1, ratio 0.0 Test 2: All tiers, level 3, ratio 1.0 Test 3: All tiers, level 0, ratio 1.0 Test 4: All tiers, level 0, ratio 1.0 Test 5: All tiers, level 1, ratio 1.0
Monitoring levels	Test 1: All tiers, level 0, ratio 0.0 Test 2: All tiers, level 0, ratio 1.0 Test 3: All tiers, level 1, ratio 1.0 Test 4: All tiers, level 1, ratio 1.0 Test 5: All tiers, level 1, ratio 1.0
Risk appetites	Test 1-2-3-4-5: All tiers, level 2
Contract controls	Test 1-2-3: ISO27001: False Breach: False Risk: False Test 4-5: ISO27001: False Breach: True Risk: True

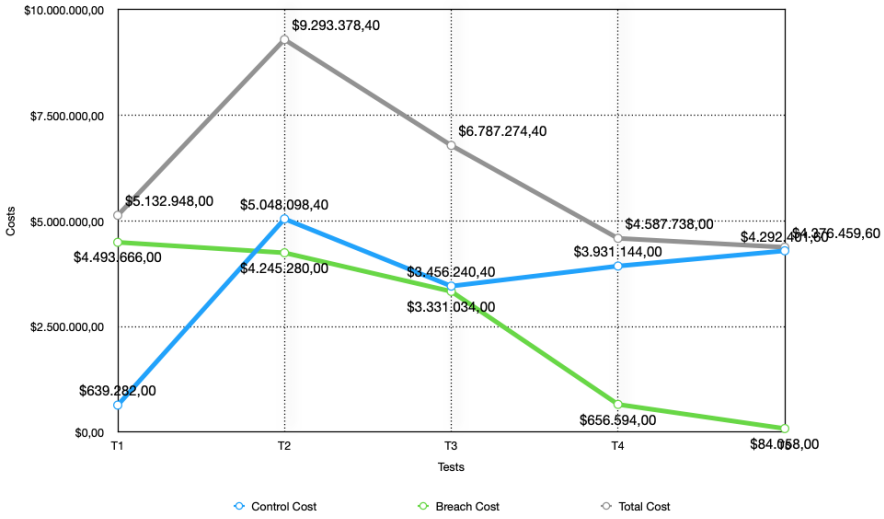

Figure 14. Monitoring and due diligence effects on costs

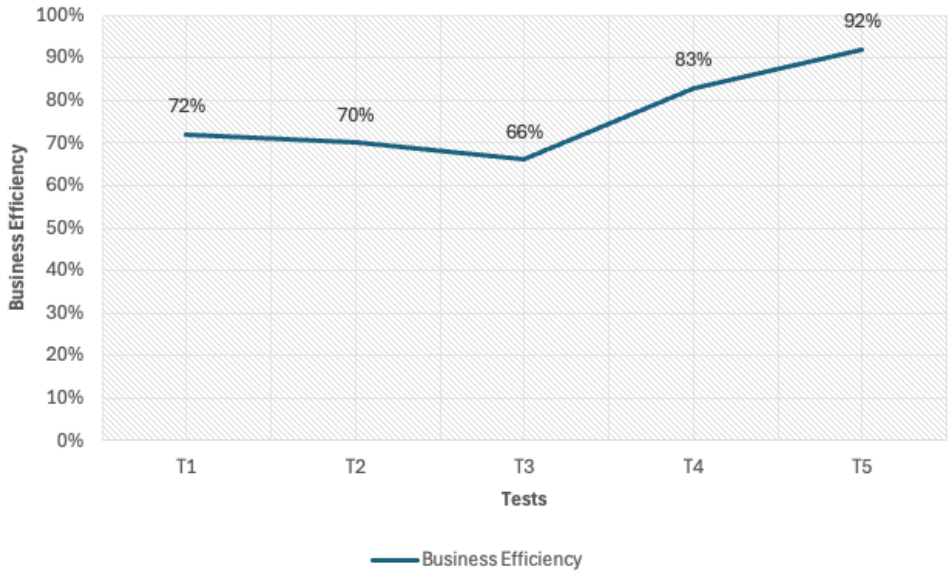

Figure 15. Monitoring and due diligence effects on business efficiency

CHAPTER 7

DISCUSSION OF ABM SIMULATION FINDINGS

All three challenges modeled in the ABM—high complexity, visibility/control, and resource constraints—led to an increase in breaches across all scenarios. High complexity, the most frequently discussed challenge in the literature, was tested first and resulted in a significant rise in breach costs. This outcome aligns with the warnings found in existing research, which emphasize the risks associated with increasingly complex third-party relationships.

In Scenario 1, the model only altered complexity levels without implementing any controls or mitigation measures. As complexity increased, breach costs rose proportionally, showing a linear relationship between the level of complexity and the financial impact of breaches. This finding has significant implications for growing organizations, suggesting that security investments should scale with the expansion of third-party networks.

Scenario 2 introduced controls by adjusting risk appetite levels. Lowering the company's risk appetite led to fewer breaches, which subsequently reduced breach costs. A significant drop in breach costs occurred when moving from risk appetite level 4 to level 3. The difference between levels 3 and 2, however, was less pronounced. Finally, setting the risk appetite to level 1 resulted in zero breaches, but this came at a high cost—business efficiency was nearly cut in half, and control costs rose substantially.

Scenario 3 examined the impact of different control levels on breach costs. As anticipated, increasing control levels led to a significant reduction in breaches. The most notable decrease in breach costs occurred between control levels 0 and 1.

While further increases in control levels continued to reduce breach costs, the accompanying rise in control costs was disproportionately higher than the reduction in breach costs, indicating diminishing returns as controls became more stringent.

In Scenario 4, various control schemes were tested to determine the most effective approach. Implementing only due diligence at different levels had minimal impact on breach costs. Similarly, performing only monitoring, without the inclusion of contractual clauses, did not significantly affect breach costs. Combining monitoring with active contractual clauses, however, led to a substantial decrease in breach costs. When due diligence was added to this setup, the lowest breach costs were observed across all tests. This suggests that a combination of monitoring, strong contractual obligations, and due diligence is the most effective strategy for minimizing breaches and associated costs.

The results of this study show the importance of finding a balance between control mechanisms in TPCRM programs. Using ABM, the tests showed that while lowering risk appetite and increasing control levels help reduce breaches, these measures often come with higher control costs and reduced business effectiveness. This outcome is consistent with what is commonly discussed in the literature, which emphasizes the challenge of managing third-party cybersecurity risks in complex environments without negatively impacting overall operations.

The tests also revealed that although increasing control levels reduce breach costs, there is a point where the extra costs associated with higher control outweigh the benefits. Beyond certain levels, the cost of implementing stricter controls becomes more significant than the decrease in breach costs. This suggests that companies need to be strategic about how much control to implement, as overly strict measures can lead to inefficiencies.

Additionally, the study shows that combining several control measures—such as due diligence, continuous monitoring, and strong contractual agreements—results in the most effective reduction of breach costs. In Scenario 4, the combination of monitoring and contractual clauses significantly lowered breach costs, whereas using only due diligence or monitoring alone did not produce much impact. This highlights the need for a comprehensive approach to TPCRM that layers multiple control methods to better manage third-party cyber risks.

CHAPTER 8

CONCLUSION AND FUTURE WORK

This study aims to answer the following research questions:

RQ1: What are the primary studies on third-party cybersecurity, and which research themes have been addressed in the literature?: The literature review (Chapters 2-4) identified three major research themes within the field of TPCRM: the importance of having a TPCRM program, the challenges associated with creating and maintaining one, and the best practices for effective TPCRM. This thesis specifically focuses on the latter two, examining the challenges of high complexity, visibility and control, and resource constraints, as well as how these challenges can be addressed through best practices such as due diligence, continuous monitoring, and strong contract management.

RQ2: What are the critical challenges to address for effective third-party cybersecurity risk management in enterprise environments?: The ABM simulations confirm that high complexity, visibility/control issues, and resource constraints significantly increase the risk and cost of breaches. This finding aligns with the concerns highlighted in the literature (Chapter 4). For instance, Scenario 1 demonstrates a clear correlation between the complexity of third-party relationships and the financial impact of breaches. Similarly, Scenario 2 and 3 show that while lowering risk appetite and increasing control levels can mitigate breaches, they also lead to higher control costs and potential reductions in business effectiveness.

RQ3: What are the best practices for an organization to manage third-party cybersecurity risks?: While implementing individual controls like due diligence or monitoring alone had a limited impact on breach costs, combining these practices

with strong contractual agreements led to a substantial decrease in breaches and associated financial losses (Scenario 4). This finding supports the literature's emphasis on a comprehensive TPCRM approach that layers multiple control methods for better risk management.

RQ4: How can agent-based models be used to simulate third-party cyber risks?: This thesis demonstrates how ABMs can effectively simulate the complex interactions between a main company, its third-party partners, and potential attackers. The developed ABM simulates various TPCRM scenarios by incorporating key challenges, best practices, and real-world cost data. The model allows researchers and practitioners to observe the impact of different control strategies on breach costs, business efficiency, and overall cybersecurity posture.

This study demonstrates the increasing importance of developing a well-rounded TPCRM strategy that balances the need for robust cybersecurity with the practical limitations of cost and business efficiency. By simulating real-world TPCRM scenarios, the ABM developed in this thesis provides insights into the complexities of managing third-party cyber risks, offering benefits to both researchers and practitioners.

For researchers, this study contributes a novel ABM that simulates the dynamic interactions between a primary organization, its third-party companies, attackers, and the contracts governing their relationships. This model can serve as a foundation for future research exploring various aspects of TPCRM, including but not limited to (1) integrating more sophisticated human behavior models; (2) incorporating the impact of emerging technologies such as AI and blockchain; and (3) investigating alternative risk assessment methodologies. Further research should prioritize validating the ABM using real-world data through collaborations with

industry partners, addressing the current limitation of relying primarily on literature findings for validation.

For practitioners, this research underscores the importance of finding a balance between implementing strong control mechanisms and maintaining operational efficiency. While lowering risk appetite and increasing control levels can reduce the likelihood and impact of breaches, these measures often come at the cost of increased expenses and potential reductions in business effectiveness. Organizations are encouraged to use the insights gained from this research to: (1) carefully evaluate their risk appetite and select appropriate control levels based on their specific operational context; (2) prioritize investing in a combination of control measures, including due diligence, continuous monitoring, and strong contracts; and (3) recognize the importance of regularly reviewing and adapting their TPCRM strategies to align with the evolving cyber threat landscape.

Future research could expand the scope of this study by adapting and applying the ABM to different industry sectors. Recognizing that TPCRM strategies often need to be tailored to specific industry needs, exploring sector-specific applications of the model would enhance its practical relevance and contribute to the development of more effective risk mitigation strategies across various industries.

The human element in TPCRM decision-making could be modeled more comprehensively in future research. Incorporating behavioral economics principles could better simulate how security professionals and organizational leaders make risk management decisions under various constraints. Additionally, the model could be expanded to include more sophisticated cost-benefit analysis tools, helping organizations better understand the long-term financial implications of their TPCRM

investments, including indirect costs of breaches such as reputational damage and lost business opportunities.

The findings of this research have important implications for existing cybersecurity standards and frameworks. While current standards like ISO/IEC 27001:2022 and ISO/IEC 27036 provide comprehensive guidance for information security management and supplier relationships respectively, and the NIST family of standards (SP 800-53, SP 800-161, and Cybersecurity Framework) offers detailed control frameworks, the simulation results suggest areas where these frameworks might be enhanced. Particularly, the model's insights regarding the effectiveness of integrated control strategies could inform future updates to these standards.

The simulation results largely validate many of the control requirements specified in current standards, especially regarding the importance of continuous monitoring and thorough due diligence. The findings particularly support ISO/IEC 27036's emphasis on supplier relationship security and the NIST Cybersecurity Framework's structured approach to risk management. However, they also suggest that the strictly tiered approach to controls often recommended by standards like ISO/IEC 27001 and NIST SP 800-53 might benefit from more flexibility. Organizations implementing these standards might consider using simulation results like those presented in this study to optimize their compliance efforts, particularly in balancing security investments across different control types.

Future standards development could benefit from incorporating more quantitative analysis of control effectiveness, similar to the approach used in this study. This could help organizations better prioritize their security investments while maintaining compliance with regulatory requirements. While NIST SP 800-161 provides detailed guidance for supply chain risk management, and ISO/IEC 27036

offers comprehensive supplier security controls, the findings suggest these standards might benefit from more specific guidance on integrating different control types, as the simulation demonstrated the superior effectiveness of combined control strategies. The results particularly support the evolution toward a more integrated approach, as seen in the latest versions of these standards, but suggest an even greater emphasis on control integration might be beneficial.

In conclusion, while this study provides valuable insights into the effectiveness of various TPCRM strategies, it also highlights the complexity of the challenges organizations face in managing third-party cyber risks. The findings suggest that successful TPCRM requires a balanced, integrated approach that considers both security requirements and business objectives. As the digital ecosystem continues to evolve, the frameworks and models developed in this research can serve as building blocks for more sophisticated tools and strategies to address tomorrow's cybersecurity challenges.

APPENDIX

MODEL CODE

```
breed [primary-companies primary-company]
breed [third-party-companies third-party-company]
breed [contracts contract]
breed [attackers attacker]



third-party-companies-own [
  tp-OP  ;; Organization Direction and Process
  tp-OS  ;; Organization Structure
  tp-AT  ;; Automation
  tp-PE  ;; Performance Evaluation
  tp-RP  ;; Reporting
  engaged?  ;; Flag to indicate if the third party is engaged with the primary company
  evaluated? ;; Flag to indicate if the third party had an assessment from the primary company
  breached? ;; Flag to indicate if the third party experienced a data breach
  breached-info? ;; Flag to indicate if the third party knows about the breach

  iso27001?
  iso-remaining-time

  tier

  risk-tier
  eval-risk-tier
  eval-remaining-time

  current-contract
]

primary-companies-own [
  breach-cost
  breach-count
  backup-size
  data-size
  backup-count
  operational?
  ticks-to-operational
  lost-data
]

attackers-own [
  attack-power
]

contracts-own [
  third-party-comp
  time
  minimum-risk
  monitor-level
  require-iso?
  breach-clause?
```

```
  ticks-to-breach
]

globals [
  total-monitoring-cost
  total-due-diligence-cost
  total-engagements

  catched-breaches
  effected-breach-count
  unknown-breaches
  due-diligence-count
  rejected-companies
  monitored-companies
  rejected-breached-companies

  global-bus-ef

  global-ticks-to-breach
  global-ticks-to-operational
  total-downtime
  total-loss-data
  total-breaches

  backup-initial-cost
  backup-tick-cost
  backup-total-cost
  data-loss-cost
  cost-per-breach

  due-diligence-costs
  due-diligence-levels
  due-diligence-ratios
  due-diligence-rates

  monitoring-setup-costs
  monitoring-costs
  monitoring-levels
  monitoring-ratios

  total-cost-of-monitorings
  total-cost-of-duediligences

  contract-iso-reqs
  contract-times
  contract-breach-reqs

  total-number-of-companies

  tier-counts
  engagement-counts

  risk-appetites
]



to setup
  clear-all
```

```
set total-downtime 0
set total-loss-data 0
set total-breaches 0

set tier-counts (list 0 ((complexity ^ 2) / 4) (complexity ^ 2)  (2.5 * (complexity ^ 2)))
set engagement-counts (list 0 (complexity) (complexity * 2) (complexity * 5))

set due-diligence-costs (list 0 500 3000 15000)
set due-diligence-levels (list 0 t1-l-duediligence t2-l-duediligence t3-l-duediligence)
set due-diligence-ratios (list 0 t1-rat-duediligence t2-rat-duediligence t3-rat-duediligence)

set monitoring-setup-costs (list 0 2000 8000 20000)
set monitoring-costs (list 0 500 1000 4000)
set monitoring-levels (list 0 t1-l-monitoring t2-l-monitoring t3-l-monitoring )
set monitoring-ratios (list 0 t1-rat-monitoring t1-rat-monitoring t1-rat-monitoring )

set contract-iso-reqs (list false t1-c-iso27001 t2-c-iso27001 t3-c-iso27001)
set contract-times (list false t1-c-time t2-c-time t3-c-time)
set contract-breach-reqs (list false t1-c-breach t2-c-breach t3-c-breach)
set risk-appetites (list 0 tier-1-risk-appetite tier-2-risk-appetite tier-3-risk-appetite)

set total-cost-of-duediligences (list 0 0 0 0)
set total-cost-of-monitorings (list 0 0 0 0)

set backup-initial-cost 3000
set backup-tick-cost 2
set backup-total-cost 0
set data-loss-cost 10
set cost-per-breach 400000

set global-ticks-to-breach (list 0 1 2 4)
set global-ticks-to-operational (list 0 4 2 1 )
set global-bus-ef (list 100)

;; Create the primary company
create-primary-companies 1 [
  set color blue
  set size 3
  setxy 0 0  ;; Place it at the center of the world
  ;; Additional setup for the primary company can be added here
  set shape "square"

  set breach-count 0
  set backup-size 0
  set data-size 0
  set backup-count 0
  set breach-cost 0
  set operational? true
  set breach-count 0
]

create-tier-companies 1
create-tier-companies 2
create-tier-companies 3

create-multi-attackers complexity ^ 3

setup-monitoring

reset-ticks
```

```
end

to create-tier-companies [tier-no]

  let radius 5 * tier-no  ;; You can adjust this value to increase or decrease the distance from the
primary company
  let angle-step 360 / (item tier-no tier-counts)
  let angle 0
  repeat (item tier-no tier-counts) [
    create-third-party-companies 1 [
      set shape "circle 2"  ;; Set the shape to a company icon
      set color red
      set size 1
      setxy (radius * cos angle) (radius * sin angle)  ;; Place at calculated position
        ;; Assign random attributes between 1 and 5
      set tp-OP (random 6)
      set tp-OS (random 6)
      set tp-AT (random 6)
      set tp-PE (random 6)
      set tp-RP (random 6)

      set engaged? false
      set evaluated? false
      set breached? false
      set breached-info? false

      set iso27001? false
      set tier tier-no
      refresh-risk-tier
      set eval-risk-tier 5
    ]
    set angle angle + angle-step  ;; Increment angle for next company
  ]

end

to create-multi-attackers [num]
  create-attackers num [
    set attack-power random-normal 13 5
    if complexity > 20 [ set attack-power random-normal 13 7 ]
    ;; Attackers are invisible
    hide-turtle
  ]
end




;; ATTACKER ACTIONS
to attack
  ;; Randomly select a third-party company
  let target one-of third-party-companies

  ;; Calculate the total attributes of the target third-party company
  let total-attributes [tp-OP + tp-OS + tp-AT + tp-PE + tp-RP] of target

  ;; Compare attack power with the total attributes
  if attack-power > total-attributes [
```

```
    ;; A data breach occurs
    ask target [
      set breached? true
    ]
  ]
end

;; THIRD PARTY COMPANY ACTIONS
to refresh-risk-tier
  if eval-remaining-time > 0 [
    set eval-remaining-time (eval-remaining-time - 1)
  ]
  if eval-remaining-time = 0 [
    set evaluated? false
  ]
  update-stats
  set risk-tier (get-risk-tier (tp-OP + tp-OS + tp-AT + tp-PE + tp-RP))
  (ifelse
    risk-tier = 1 [ set color white ]
    risk-tier = 2 [ set color green ]
    risk-tier = 3 [ set color yellow ]
    risk-tier = 4 [ set color orange ]
  )
  let current-color color
  if current-contract != 0 and current-contract != nobody [
    ask current-contract [
      draw-connection current-color
    ]
  ]
end

to-report get-risk-tier [total-score]
  (ifelse
    total-score >= 19 [
      report 1
    ] total-score >= 13 [
      report 2
    ] total-score > 7 [
      report 3
    ] [
      report 4
    ]
  )
end

to update-stats ; performed by third party companeis
  if not iso27001? [
    set tp-OP randomly-change-stat tp-OP
    set tp-OS randomly-change-stat tp-OS
    set tp-AT randomly-change-stat tp-AT
    set tp-PE randomly-change-stat tp-PE
    set tp-RP randomly-change-stat tp-RP
  ]
end

to-report randomly-change-stat [stat]
  let rnd random-float 1
  (ifelse
    rnd <= 0.25 [report min (list (stat + 1) 5)]
    rnd <= 0.5 [report max (list (stat - 1) 0)]
```

```
    rnd <= 1 [report stat]
    [report stat]
    )
end

to get-iso27001
  set iso27001? true
  set iso-remaining-time 12
end

to tick-iso27001
  set iso-remaining-time (iso-remaining-time - 1)
  if iso-remaining-time <= 0 [
    set iso27001? false
    if random 2 = 0 [
      set iso27001? true
      set iso-remaining-time 12
    ]
  ]
end

to check-for-breach [bonus]
  ;; Possibility of learning the breach
  let total-score tp-OP + tp-OS + tp-AT + tp-PE + tp-RP
  if breached? = true and random-float 1 < ((total-score + bonus) / 30) [
    set breached-info? true
  ]

  ;; Possibility of stopping the breach
  if random-float 1 < ((total-score + bonus) / 20) and breached-info? = true [
    set breached? false
    set breached-info? false
    if current-contract != 0 and current-contract != nobody [
      output-print (word "BREACH MITIGATED: Company : " self " mitigated its breach")
    ]
  ]
end

;; CONTRACT ACTIONS
to draw-connection [set-color] ;; Change engagement color. Called over target
  let primary one-of primary-companies
  ;; Visualize the relationship by creating a link
  ask third-party-comp [
    ask my-links [
      die
    ]
    create-link-to primary [
      set color set-color
    ]
  ]
end

to tick-contract
  set time time - 1

  if time <= 0 [
    let primary one-of primary-companies
    let re-contact-flag? false
    ask primary [
     if re-contract [third-party-comp] of myself [
```

```
      set re-contact-flag? true
    ]
  ]
  if not re-contact-flag? [
    ask third-party-comp [
      set engaged? false
      ask my-links [
        die
      ]
    ]
    die
  ]
]

;; Contracts add to the total data
let new-data 0
let working-tier [tier] of third-party-comp
(ifelse
  working-tier = 1 [ set new-data 10 ]
  working-tier = 2 [ set new-data 5 ]
  working-tier = 3 [ set new-data 2 ]
 )
let primary one-of primary-companies
ask primary [ set data-size data-size + new-data ]
end

to end-self
  ask third-party-comp [
    set engaged? false
    ask my-links [
      die
    ]
  ]
  die
end

to continuous-monitoring
  let working-tier [tier] of third-party-comp
  ; monitor level. levels affect accuracy
  if monitor-level > 0 [
    set total-cost-of-monitorings replace-item working-tier total-cost-of-monitorings ((item working-
tier total-cost-of-monitorings) + (item monitor-level monitoring-costs))

    let company-attributes evaluate-company third-party-comp monitor-level
    let new-eval-risk-tier get-risk-tier company-attributes
    ask third-party-comp [
      set eval-risk-tier new-eval-risk-tier
    ]

    ; risk control. if true, when level goes down, cancel contract
    if (item working-tier contract-iso-reqs) and [eval-risk-tier] of third-party-comp < (item working-tier
risk-appetites) [
      output-print (word "CONTRACTUAL: Contract is ended early with " third-party-comp " due to
risk requirements not fulfilled")
      end-self
    ]

    ; breach control
    if (item working-tier contract-breach-reqs) and [breached-info?] of third-party-comp = true and
(item working-tier contract-breach-reqs) = true [
```

```
    output-print (word "CONTRACTUAL: Contract is ended early with " third-party-comp " due to
breach requirements not fulfilled.")
    end-self
  ]

  (ifelse
    monitor-level = 3 [
      ask third-party-comp [
        if breached? = true [
          output-print (word "MONITORING LEVEL 3: Found breach in " self ". Trying to mitigate!")
          set breached-info? true
          check-for-breach 3
        ]
      ]
    ] monitor-level = 2 [
      ask third-party-comp [
        if breached? = true [
        output-print (word "MONITORING LEVEL 2: Found breach in " self ". Trying to mitigate!")
          set breached-info? true
          check-for-breach 0
        ]
      ]
    ] monitor-level = 1 [
      if random 2 = 0 [
        ask third-party-comp [
          if breached? = true [
            output-print (word "MONITORING LEVEL 1: Found breach in " self ". Trying to
mitigate!")
            set breached-info? true
            check-for-breach 0
          ]
        ]
      ]
    ]
  )
 ]
end

to propagate-breach
 if [breached?] of third-party-comp = true [
  output-print (word "BREACH DANGER: A contracted company " third-party-comp " in tier " [tier]
of third-party-comp " is currently breached. It will affect the primary company in " ticks-to-breach "
tick/s if not mitigated" )
  let cur-tier [tier] of third-party-comp
  if ticks-to-breach = 0 [
    ask one-of primary-companies [
      get-breached myself
    ]
  ]
  set ticks-to-breach ticks-to-breach - 1
  if ticks-to-breach < 0 [ set ticks-to-breach 0 ]
 ]
 if [breached?] of third-party-comp = false [
  set ticks-to-breach (item [tier] of third-party-comp global-ticks-to-breach)
 ]
end
```

```
;; PRIMARY COMPANY ACTIONS
to select-company-to-engage [tier-number]
  let ddl (item tier-number due-diligence-levels)
  let selected one-of third-party-companies with [engaged? = false and tier = tier-number]
  if selected != nobody [
    ; check due diligence level and ratio
    ifelse (item tier-number due-diligence-levels) != 0 and random-float 1 <= (item tier-number due-
diligence-ratios) [
      set total-cost-of-duediligences replace-item tier-number total-cost-of-duediligences ((item tier-
number total-cost-of-duediligences) + (item ddl due-diligence-costs))
      let due-diligence-report evaluate-company selected (item tier-number due-diligence-levels)
      let assessed-risk-tier get-risk-tier due-diligence-report
      if assessed-risk-tier <= (item tier-number risk-appetites) [
        start-contract selected
      ]
    ]
    [
      start-contract selected
    ]
  ]
end

to-report evaluate-company [target level]
  let total-attributes ([tp-OP] of target + [tp-OS] of target + [tp-AT] of target + [tp-PE] of target + [tp-
RP] of target)
  let breach-status-points 0
  if [iso27001?] of target [
    ask target [
      set evaluated? true
      set eval-risk-tier get-risk-tier total-attributes
      if breached? [ set breach-status-points 10 ]
    ]
    report total-attributes - breach-status-points
  ]

  let randomizer ((4 - level) ^ 2) / 2 - (random ((4 - level) ^ 2))
  ask target [
    set evaluated? true
    set eval-risk-tier get-risk-tier (total-attributes + randomizer)
    if breached? [ set breach-status-points 10 ]
  ]
  report total-attributes + randomizer - breach-status-points
end

to start-contract [target] ;; Target is third party
  output-print (word "CONTRACTUAL: New contract with " target " at tier " [tier] of target)
  create-contracts 1 [
    set third-party-comp target
    set minimum-risk (item [tier] of target risk-appetites)
    set require-iso? (item [tier] of target contract-iso-reqs)
    set time (item [tier] of target contract-times) + 1
    set breach-clause? (item [tier] of target contract-breach-reqs)
    set monitor-level (item [tier] of target monitoring-levels)
    set ticks-to-breach (item [tier] of target global-ticks-to-breach)
    let contract-holder self
    ask target [
      set current-contract contract-holder
      set engaged? true
```

```
    ]

    ask self [
      draw-connection [color] of target
    ]
    hide-turtle
  ]
end

to-report re-contract [target] ;; Happens when contract ends with time
  let working-tier [tier] of target
  if [monitor-level] of [current-contract] of target > 0 [
    if [eval-risk-tier] of target <= (item working-tier risk-appetites)  [
      if (item working-tier contract-iso-reqs) = true and [iso27001?] of target = true [
        ask target [
          ask current-contract [
            set time (item working-tier contract-times)
          ]
        ]
        output-print (word "CONTRACTUAL: Contract renewed with " target " at tier " working-tier "
with risk tier " ([eval-risk-tier] of target) )
        report true
      ]
      if (item working-tier contract-iso-reqs) = false [
        ask target [
          ask current-contract [
            set time (item working-tier contract-times)
          ]
        ]
        output-print (word "CONTRACTUAL: Contract renewed with " target " at tier " working-tier "
with risk tier " ([eval-risk-tier] of target) )
        report true
      ]
    ]

    (ifelse
      [eval-risk-tier] of target > (item working-tier risk-appetites) [ output-print (word
"CONTRACTUAL: Contract NOT renewed with " target " at tier " working-tier " due to risk
requirements." ) ]
      (item working-tier contract-iso-reqs) = true and [iso27001?] of target = false [ output-print (word
"CONTRACTUAL: Contract NOT renewed with " target " at tier " working-tier  " due to ISO
requirements." ) ]
    )

    report false
  ]

  ;; If not monitoring, renew directly
  output-print (word "CONTRACTUAL: Contract renewed with " target " at tier " working-tier " with
risk tier unknown")
  ask target [
    ask current-contract [
      set time (item working-tier contract-times)
    ]
    ]
  report true
end

to cancel-contract [target]
  ask target [
```

```
    ask current-contract [
      end-self
    ]
  ]
end

to setup-monitoring
  let working-tier 0
  foreach monitoring-levels [ level ->
    set total-cost-of-monitorings replace-item working-tier total-cost-of-monitorings ((item working-
tier total-cost-of-monitorings) + (item working-tier monitoring-setup-costs))
  ]
end

to get-breached [thecontract]
  let level [tier] of [third-party-comp] of thecontract
  let tpc [third-party-comp] of thecontract
  set ticks-to-operational (item level global-ticks-to-operational)

  output-print (word "COMPANY BREACHED: Breached from tier " level " company " tpc " .
Operational in " ticks-to-operational " ticks.")
  output-print (word "COMPANY BREACHED: Lost not backed up data: " (data-size - backup-size))

  set breach-count breach-count + 1
  set breach-cost breach-cost + cost-per-breach
  set breach-cost breach-cost + ((data-size - backup-size) * data-loss-cost)
  set lost-data (lost-data + (data-size - backup-size))
  set total-loss-data total-loss-data + lost-data
  set data-size backup-size


  set operational? false
  set color red

  if [breach-clause?] of thecontract [
    output-print (word "CONTRACTUAL: Contract canceled with " tpc " due to breach clause.")
    cancel-contract [third-party-comp] of thecontract
  ]

end

to backup-data
  if data-size > 0 [
    set backup-size data-size
    set backup-total-cost backup-total-cost + backup-initial-cost
    output-print (word "BACKUP: Backed up data " backup-size " GB")
  ]
end

to update-backup-cost
  let tick-cost backup-tick-cost * backup-size
  set backup-total-cost backup-total-cost + tick-cost
end

;; GO TICK PROCEDURE
to go
  let primary one-of primary-companies
  if not [operational?] of primary [
    set total-downtime (total-downtime + 1)
  ]
```

```
  let bus-ef-t1 (((count third-party-companies with [engaged? = true and tier = 1] / (item 1
engagement-counts)) * 100))
  let bus-ef-t2 (((count third-party-companies with [engaged? = true and tier = 2] / (item 2
engagement-counts)) * 100))
  let bus-ef-t3 (((count third-party-companies with [engaged? = true and tier = 3] / (item 3
engagement-counts)) * 100))
  let bus-ef ((bus-ef-t1 * (13 / 26)) + (bus-ef-t2 * (8 / 26)) + (bus-ef-t3 * (5 / 26)))
  if ticks > 2 [
    set global-bus-ef lput bus-ef global-bus-ef
  ]
  show global-bus-ef
  output-print (word "==== STARTING TICK " ticks "====")
  output-print (word "Company is operational: " [operational?] of primary)
  output-print (word "Current contracts: " count contracts)
  output-print (word "Current business efficiency: " bus-ef)
  output-print (word "Average business efficiency: " (mean global-bus-ef))
  output-print (word "Current data: " [data-size] of primary " GB")
  output-print (word "Current data backed up: " [backup-size] of primary " GB")
  output-print (word "Backup cost per tick: " ([backup-size] of primary * backup-tick-cost) "$")


  let mon-l-1 count contracts with [monitor-level = 1]
  let mon-l-2 count contracts with [monitor-level = 2]
  let mon-l-3 count contracts with [monitor-level = 3]
  output-print (word "Monitoring with level 1: " mon-l-1 )
  output-print (word "Monitoring with level 2: " mon-l-2 )
  output-print (word "Monitoring with level 3: " mon-l-3 )
  output-print (word "Current monitoring cost per tick: " ( (mon-l-1 * (item 1 monitoring-costs)) +
(mon-l-2 * (item 1 monitoring-costs)) + (mon-l-3 * (item 3 monitoring-costs)) ) "$")

  output-print ("")
  output-print ("")

  set backup-total-cost (backup-total-cost + ([backup-size] of primary * backup-tick-cost))
  output-print (word "Total cost of due diligences: " (sum total-cost-of-duediligences) "$")
  output-print (word "Total cost of monitoring: " (sum total-cost-of-monitorings) "$")
  output-print (word "Total cost of backups: " backup-total-cost "$")

  output-print ("")
  output-print ("")

  output-print (word "Total number of breaches " [breach-count] of primary)
  output-print (word "Total cost of breaches: " [breach-cost] of primary "$")
  output-print (word "Total downtime: " total-downtime " tick/s")
  output-print (word "Total loss of data: " [lost-data] of primary " GB")

  output-print ("")
  output-print ("")

  ;; Third party companies
  ask third-party-companies [
    refresh-risk-tier
    if iso27001? = true [
      tick-iso27001
    ]
    if risk-tier = 1 and random 5 = 0 and iso27001? = false [
      get-iso27001
    ]
```

```
    check-for-breach 0
  ]

    ;; Primary company run
  (ifelse [operational?] of primary = true [
    let counter 0
    repeat 3 [
      let remaining-engagements (item (counter + 1) engagement-counts) - (count third-party-
companies with [engaged? = true and tier = (counter + 1)])
      repeat (remaining-engagements * 2) [
        if (count third-party-companies with [engaged? = true and tier = (counter + 1)]) < (item (counter
+ 1) engagement-counts) [
          select-company-to-engage (counter + 1)
        ]
      ]
      set counter counter + 1
    ]
    if backup-rate > 0 [
      ask primary-companies [
        update-backup-cost
        if ticks mod backup-rate = 0 [
          backup-data
        ]
      ]
    ]
  ]
  [
    set global-bus-ef lput 0 global-bus-ef
    ask primary [
      set ticks-to-operational ticks-to-operational - 1
      if ticks-to-operational = 0 [
        set operational? true
        set color blue
      ]
    ]
  ])

  ;; Contracts
  ask contracts [
    continuous-monitoring
    propagate-breach
    tick-contract
  ]

  ;; Attacks happen
  ask n-of (random complexity ^ 1.5) attackers [
    attack
  ]
  output-print (word "==== END OF TICK " ticks " ====")
  output-print ("")
  output-print ("")
  tick
end

to go-for-ticks
  repeat tick-count [
    go
  ]
end
```

REFERENCES

Abrahams, T. O., Farayola, O. A., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2024). Reviewing Third-Party Risk Management: Best Practices in Accounting and Cybersecurity for Superannuation Organizations. *Finance & Accounting Research Journal*, *6*(1), 21–39. https://doi.org/10.51594/farj.v6i1.706

Aliane, N., & Zakariya, A. (2023). Enhancing Cyber Security Resilience in the Industrial Sector: A Comprehensive Framework for Third-Party Risk Management. *International Journal of Cyber Criminology*, *17*(2). https://doi.org/10.5281/ZENODO.4766716

Ashiku, L., & Dagli, C. (2020). Agent Based Cybersecurity Model for Business Entity Risk Assessment. *2020 IEEE International Symposium on Systems Engineering (ISSE)*, *177*, 1–6. https://doi.org/10.1109/isse49799.2020.9272234

Barrus, R. (2024, June 13). *How Much Do Vendor Due Diligence Reviews Cost?* https://www.pivotpointsecurity.com/how-much-do-vendor-due-diligence-reviews-cost/

Boyens, J. M., Paulsen, C., Bartol, N., Winkler, K., & Gimbi, J. (2020). *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry*. https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8276.pdf

Boyens, J., Smith, A., Bartol, N., Winkler, K., Holbrook, A., & Fallon, M. (2022). *Cybersecurity supply chain risk management for systems and organizations* (NIST SP 800-161r1; p. NIST SP 800-161r1). National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.SP.800-161r1

Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation*, *34*(7), 342–353. https://doi.org/10.1016/j.technovation.2014.02.001

Bradbury, D. (2022, March 22). *Updated Okta Statement on LAPSUS$*. https://www.okta.com/blog/2022/03/updated-okta-statement-on-lapsus/

Bronson, H. E. (2022). *Five Common Shortcomings of Third-Party Management Programs in Financial Organizations and Recommended Risk Management Strategies* [Dissertation/Thesis, Utica University]. https://www.proquest.com/dissertations-theses/five-common-shortcomings-third-party-management/docview/2664178554/se-2

Chingombe, R. (2023). *Impact of Risk Attributes on Vendor Risk Assessment and Classification* [Capella University]. https://www.ssrn.com/abstract=4620534

Cinar, B. (2023). Supply Chain Cybersecurity: Risks, Challenges, and Strategies for a Globalized World. *Journal of Engineering Research and Reports*, *25*(9), 196–210. https://doi.org/10.9734/jerr/2023/v25i9993

Cisternelli, E. (2024, February 27). *7 Cybersecurity Frameworks That Help Reduce Cyber Risk*. https://www.bitsight.com/blog/7-cybersecurity-frameworks-to-reduce-cyber-risk

European Union Agency for Cybersecurity. (2021). *ENISA threat landscape for supply chain attacks.* Publications Office. https://data.europa.eu/doi/10.2824/168593

Faife, C. (2022, April 20). *Okta ends Lapsus$ hack investigation, says breach lasted just 25 minutes*. https://www.theverge.com/2022/4/20/23034360/okta-lapsus-hack-investigation-breach-25-minutes

Ghadge, A., Weiß, M., Caldwell, N. D., & Wilding, R. (2019). Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Management: An International Journal*, *25*(2), 223–240. https://doi.org/10.1108/SCM-10-2018-0357

Giacchero, A., & Moretti, J. (2021). A Possible holistic framework to manage ICT third-party risk in the age of cyber risk. *Risk Management Magazine*, *16*(1), 30–42. https://doi.org/10.47473/2020rmm0082

Goodin, D. (2024, April 2). *The XZ Backdoor: Everything You Need to Know*. https://www.wired.com/story/xz-backdoor-everything-you-need-to-know/

Greenfield, V. A., Welburn, J. W., Schwindt, K., Ish, D., Lohn, A. J., & Hartnett, G. S. (2023). *Cybersecurity and Supply Chain Risk Management Are Not Simply Additive: Implications for Directions in Risk Assessment, Risk Mitigation, and Research to Secure the Supply of Defense Industrial Products*. RAND Corporation. https://doi.org/10.7249/RR-A532-1

Haller, J., & Wallen, C. M. (2016). *Managing Third Party Risk in Financial Services Organizations: A Resilience-Based Approach.*

Hammi, B., Zeadally, S., & Nebhen, J. (2023). Security Threats, Countermeasures, and Challenges of Digital Supply Chains. *ACM Computing Surveys*, *55*(14s), 1–40. https://doi.org/10.1145/3588999

Hanafizadeh, P., Keating, B. W., & Khedmatgozar, H. R. (2014). A Systematic review of Internet banking adoption. *Telematics and Informatics*, *31*(3), 492–510. https://doi.org/10.1016/j.tele.2013.04.003

Heath, B., Hill, R., & Ciarallo, F. (2009). A Survey of Agent-Based Modeling Practices (January 1998 to July 2008). *Journal of Artificial Societies and Social Simulation*, *12*(4).

Ilori, O., Nwosu, N. T., & Naiho, H. N. N. (2024). Third-party vendor risks in IT security: A comprehensive audit review and mitigation strategies. *World Journal of Advanced Research and Reviews*, *22*(3), 213–224. https://doi.org/10.30574/wjarr.2024.22.3.1727

Joint Task Force Interagency Working Group. (2020). *Security and Privacy Controls for Information Systems and Organizations* (Revision 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

Kaseya. (2021). *Incident Overview & Technical Details*. https://helpdesk.kaseya.com/hc/en-gb/articles/4403584098961-Incident-Overview-Technical-Details

Keizer, E. G. (2022). *Third-Party Risk Management in the Financial Services Industry*. Radboud Universiteit Nijmegen.

Keskin, O. F., Caramancion, K. M., Tatar, I., Raza, O., & Tatar, U. (2021). Cyber Third-Party Risk Management: A Comparison of Non-Intrusive Risk Scoring Reports. *Electronics*, *10*(10), 1168. https://doi.org/10.3390/electronics10101168

Kobalt.io. (n.d.). *Comparing Costs: Building an In-House SOC vs. Third-Party Managed Cybersecurity for Businesses*. Retrieved September 2, 2024, from https://kobalt.io/comparing-costs-building-an-in-house-soc-vs-third-party-managed-cybersecurity-for-businesses/#

Kosling, K. (2024, June 6). *What Are 5 Top Cybersecurity Frameworks?* https://www.itgovernanceusa.com/blog/top-4-cybersecurity-frameworks

Krehel, O. (2022, January 27). *The 2021 Kaseya Attack Highlighted the Seven Deadly Sins of Future Ransomware Attacks*. https://www.forbes.com/sites/forbestechcouncil/2022/01/25/the2021-kaseyaattack-highlighted-the-seven-deadly-sins-of-future-ransomware-attacks

Kwong, J. K., & Pearlson, K. (2024). Supply Chain Cybersecurity and Small and Medium-Sized Enterprises (SMEs): Exploring Shortcomings in Third Party Risk Management of SMEs. *57th Hawaii International Conference on System Sciences*. 57th Hawaii International Conference on System Sciences. https://hdl.handle.net/10125/107183

Macal, C. M., & North, M. J. (2009). Agent-based modeling and simulation. *Proceedings of the 2009 Winter Simulation Conference (WSC)*, 86–98. https://doi.org/10.1109/WSC.2009.5429318

Mohamed, I. A. (2024). Cyber Risk Management of Third-Party Relationships: The Need for an Assessment Guidelines to Regulate Private Sectors in Libya. *2024 IEEE 4th International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA)*, 7–12. https://doi.org/10.1109/MI-STA61267.2024.10599763

Monev, V. (2021). The "Self-Assessment" Method within a Mature Third-Party Risk Management Process in the Context of Information Security. *2021 International Conference on Information Technologies (InfoTech)*, 1–7. https://doi.org/10.1109/InfoTech52438.2021.9548373

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29; p. NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

Niknejad, N., Ismail, W., Ghani, I., Nazari, B., Bahari, M., & Hussin, A. R. B. C. (2020). Understanding Service-Oriented Architecture (SOA): A systematic literature review and directions for further investigation. *Information Systems*, *91*, 101491. https://doi.org/10.1016/j.is.2020.101491

Oladimeji, S., & Kerner, S. M. (2023, November 3). *SolarWinds hack explained: Everything you need to know*. https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

Optimal Networks. (n.d.). *How Much Does Data Backup Cost for Small Business?* Retrieved September 2, 2024, from https://www.optimalnetworks.com/how-much-does-data-backup-cost-for-small-business/

Ornstein, J. T., & Hammond, R. A. (2021). Agent-Based Modeling in Public Health. In *New Horizons in Modeling and Simulation for Social Epidemiology and Public Health* (1st ed., pp. 67–77). Wiley. https://doi.org/10.1002/9781118589397

Putrus, R. (2017). A Risk-Based Management Approach to Third-Party Data Security, Risk and Compliance. *ISACA Journal*, *6*(2017). https://www.isaca.org/resources/isaca-journal/issues/2017/volume-6/a-riskbased-management-approach-to-thirdparty-data-security-risk-and-compliance

Roberts, L. (2023). *Countermeasures For Preventing Malicious Infiltration on the Information Technology Supply Chain* [Dissertation/Thesis, Purdue University]. https://figshare.com/articles/thesis/_strong_Countermeasures_for_Preventing_Malicious_Infiltration_on_the_Information_Technology_Supply_Chain_strong_/23258228

Ryerse, J. (2024, May 30). *Top 11 cybersecurity frameworks in 2024*. https://www.connectwise.com/blog/cybersecurity/11-best-cybersecurity-frameworks#:~:text=ISO%2027001%20and%20ISO%2027002%20are%20two%20of%20the%20most,robust%20policies%20and%20best%20practices.

Sen, S., Kotlarsky, J., & Budhwar, P. (2020). Extending Organizational Boundaries Through Outsourcing: Toward a Dynamic Risk-Management Capability Framework. *Academy of Management Perspectives*, *34*(1), 97–113. https://doi.org/10.5465/amp.2015.0191

Takefuji, Y. (2022). Security Enhancement of Third Parties Is Needed in Global Supply Chain Management. *Journal of Applied Security Research*, 1–8. https://doi.org/10.1080/19361610.2022.2086785

VC3. (2024, September 3). *How Much Do Managed Cybersecurity Services Cost?* https://www.vc3.com/blog/managed-cyber-security-services-cost

Venugopal, R., Damaraju, A., & Basavaraju, S. (2024). *Third Party Risk Management Tool Selection Framework (TPRMTSF)*. https://doi.org/10.2139/ssrn.4852691

Vestad, A., & Yang, B. (2024). A Survey of agent-based modeling for cybersecurity. *AHFE International*. 15th International Conference on Applied Human Factors and Ergonomics (AHFE 2024). https://doi.org/10.54941/ahfe1004768

Zawaideh, F. H., Abu-ulbeh, W., Majdalawi, Y. I., Zakaria, M. D., Jusoh, J. A., & Das, S. (2023). E-Commerce Supply Chains with Considerations of Cyber-Security. *2023 International Conference on Computer Science and Emerging Technologies (CSET)*, 1–8. https://doi.org/10.1109/CSET58993.2023.10346738