Master's thesis Business Information Technology
Faculty of Electrical Engineering, Mathematics and Computer Science (EEMCS)

Collaborative Cyber Security in the Retail Sector

A collaborative approach to mitigating cyber security risks in the retail sector

Author:
Jurriën Wagenaar

Examination Committee:
Prof. dr. Jos van Hillegersberg (UT/IEBIS)
Dr. Klaas Sikkel (UT/SCS)
Jarno Roos MSc. RE (KPMG/RC-IPS)

October 30th, 2014

UNIVERSITY OF TWENTE.

KPMG

COLLABORATIVE CYBER SECURITY IN THE RETAIL SECTOR

A collaborative approach to mitigating cyber security risks in the retail sector.

October 30th, 2014

Author

Jurriën Wagenaar

Programme Business Information Technology
Faculty of Electrical Engineering, Mathematics & Computer Science

E-mail j.c.n.wagenaar@alumnus.utwente.nl

UNIVERSITY OF TWENTE.

Graduation committee

Prof. dr. Jos van Hillegersberg

Department Industrial Engineering & Business Information Systems
Faculty School of Management & Governance
E-mail j.vanhillegersberg@utwente.nl

Dr. Klaas Sikkel

Department Services, Cybersecurity & Safefy
Faculty Faculty of Electrical Engineering, Mathematics & Computer Science
E-mail k.sikkel@utwente.nl

KPMG Supervisor

Jarno Roos MSc. RE

Department Information Protection Services
E-mail roos.jarno@kpmg.nl
KPMG Advisory N.V. Amstelveen

PREFACE

Dear reader,

Thank you for your interest in my master thesis. It's written as the final part of my master programme in Business Information Technology, at the University of Twente. This research project is the icing on the cake of my master programme and the result of many months hard work. Yet, the joyful event of completion has arrived. The completion means the end of my "student career" at the University of Twente. The years I spend as a student have played an important role in the development of my personal, academic and professional skills. The time has come for a new opportunity.

I would like to thank the people that were important to me during the time I was working on my thesis. First of all my supervisors from the University of Twente: Jos van Hillegersberg and Klaas Sikkel and my supervisor from KPMG: Jarno Roos. Their ideas have given this research a direction and their constructive feedback helped me to turn it into something beautiful. Second, I'd like to thanks KPMG's Information Protection Technology business unit for giving me the opportunity to do my research in their unit and for supporting my research by dedicating time, resources, facilitating contacts with interviewees. And of course for the good time I had as an intern at the office in Amstelveen! Third, I would like to thank the interviewees for their time and effort they invested in this research. Fourth, a big thanks to my friends Ruud Verbij and Hardwin Spenkelink for reviewing my thesis extensively and providing me with additional feedback and new ideas.

Last but not least, I'd like to thank my family and my girlfriend Stysia for their great deal of support and help during the development of this thesis.

I wish you a pleasant reading.

Kind regards,

Jurriën

MANAGEMENT SUMMARY

Cyber security is an important topic on the CIO's agenda. Cyber threats are on the rise in every sector and the retail sector is no exception. Both the frequency and the impact of cyber incidents have increased with financial and reputational damage as main effects. Collaborative cyber security is the business-to-business sharing of knowledge and information related to cyber security. This research shows how collaborative cyber security can be used to mitigate cyber threats in the retail sector.

To mitigate the growing amount of cyber risks in the retail sector, this research recommends retail organizations to collaborate with each other in the field of cyber security. Key to collaborative cyber security is the exchange of information and knowledge between organizations. Exchanging information leads to better detection of threats and more accurate analyses. Exchanging knowledge leads to the development of solutions of higher quality and saves organizations from developing the same solutions.

By identifying cyber threats to the retail sector, types of collaborative cyber security and critical success factors to collaboration this research has developed the "Collaboration Layer". The Collaboration Layer is designed as an extension of the NIST Cyber Security Framework and identifies cyber security activities to which a collaborative approach is desirable. These cyber security activities have been identified through a literature research and external validation with interviews with c-level executives from retail organizations with major operations in the Netherlands.

This research recommends to use the Collaboration Layer, in order to identify the cyber security activities to which a collaborative approach is desirable. The Collaboration Layer is applicable to retail organizations regardless of size, degree of cyber security risk or cyber security maturity. It enables them to integrate collaboration into their cyber security program in order to mitigate cyber risks.

Additionally, this research shows the retail sector is interested in a collaborative approach to cyber security. At the time of writing, the outcomes of this research have resulted in the first steps being taken towards the establishment of a collaboration. Collaborative cyber security is beneficial and directly applicable to the retail sector.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

CSF NIST Cyber Security Framework

DoS Denial of Service

EISA Enterprise Information Security Architecture

ICB Industry Classification Benchmark

IEC International Electrotechnical Commission

ISAC Information Sharing & Analysis Center

ISMS Information Security Management System

ISO International Organization for Standardization

ITU International Telecommunication Union

NCSC National Cyber Security Centre

PoS Point-of-Sale

SABSA Sherwood Applied Business Security Architecture

1

INTRODUCTION

The use of information systems to support business has known a large increase over the last two decades. Information systems cover increasingly large parts of organizations and even cross organizational borders. Allowing information systems to cross organizational borders can improve efficiency: systems can communicate directly without human intervention. An example from the retail industry is vendor-managed inventory, in which the retailer delegates the responsibility of maintaining inventory of agreed materials to a supplier. For this to work, the retailer provides the supplier access to the information systems containing inventory level information. [79]

Such information systems bring numerous advantages, but expose the organization to risks as well. Cyber crime is an increasingly large issue for information systems [13, 37]: this issue becomes larger when information systems are accessible outside of the company. External access also allows malicious parties to attempt to gain unauthorized access, without having physical access to the organization. Traditional cyber security at the borders of the organizational domain and the environment is no longer sufficient.

An example of a security incident crossing organizational borders took place at the Target Group, a large US-based retail organization. Target faced a security breach and disclosed credit card information and personal data of more than 110 million customers. Sources close to the investigation state that intruders gained access to Target's network by using credentials that were provided to a service company: *Fazio*. These credentials were stolen by breaking into Fazio's information systems. [46]

The Target security breach illustrates that cyber security is not limited to a single organization: the breach was made possible because of a vulnerability at Fazio. The effects of data breach aren't limited to a single organization either. In case of the Target example its customers and issuers of the exposed credit cards are affected as well. It is estimated that Target could be facing losses of up to $420 million as a result of this breach, including reimbursement associated with banks recovering the costs of reissuing millions of cards; fines from the card brands for PCI non-compliance; and direct Target customer service

costs, including legal fees and credit monitoring for tens of millions of customers impacted by the breach [46].

Retail organizations like Target take an important place in our society and own increasingly large data stores. Besides credit card data, privacy sensitive information is accumulated. Examples of privacy sensitive information are purchasing information, surfing behaviour and walking routes through brick-and-mortar stores. Having more information available means that more information can be stolen, and the consequences of a data breach can be higher. This is an incentive for retail organizations to invest in adequate protection against cyber threats.

The current environment in which cyber threats impose an increasing risk to organizations calls for new effective mitigatory and preventive measures. A potential measure is collaborative cyber security: sharing information and knowledge about cyber security between organizations. Past research shows that sharing information and knowledge between organizations has positive effects [28], and often is a motivator for the establishment of strategic alliances between organizations [74]. Joint efforts offer benefits for *cyber security* as well, because collaboration allows organizations to use a larger pool of knowledge and more information from a larger population of systems. This allows organizations to get a better grip on their cyber risks [78].

In this research the effects of collaborative cyber security on the retail sector are studied. The goal of the research is to identify how collaborative cyber security can be used to mitigate cyber threats in the retail sector. The retail sector as a whole is too large for this research, therefore results are obtained from the retail sector in the Netherlands.

2

RESEARCH BACKGROUND

The retail sector is subject to a lot of movement as can be read from the introduction. This research focuses on cyber security collaboration in the retail sector in the Netherlands and this chapter provides background knowledge about the most important subjects to this research: retail, cyber security, cyber threats and collaboration. Special attention is paid to retail in the Netherlands.

2.1 RETAIL SECTOR

The retail sector is home to all organizations that sell products to the *consumer*. The types of organizations are very diverse. Some focus on a specific kind of product or service, others sell a diversity of products or services. The Industry Classification Benchmark (ICB) definition of retail is used [23]. Retail is considered a supersector under the consumer services industry. Its subsectors are shown in figure 1.

5300 Retail	5330 Food & Drug Retailers	5333 Drug Retailers
		5337 Food Retailers & Wholesalers
	5370 General Retailers	5371 Apparel Retailers
		5373 Broadline Retailers
		5375 Home Improvement Retailers
		5377 Specialized Consumer Services
		5379 Specialty Retailers

Figure 1: The retail sector and its subsectors [23]

2.1.1 *Retail in the Netherlands*

The retail sector in the Netherlands is diverse. It varies from one-men businesses that are specialized in one type of product to very large retailers that sell thousands of products. The maturity of cyber security at the different retail organizations differs a lot. Large retail organizations often take some cyber security measures, yet a lot of large retail organizations are still in the process of developing basic security measures to mitigate risks related to cyber threats.

2.2 CYBER SECURITY

When conducting research on the subject of cyber security, it becomes clear that cyber security is about protecting digital assets. Yet, when looking for clear definitions there are several available, varying from very abstract to very concrete.

DEFINITION For this research the definition provided by the International Telecommunication Union (ITU) [36] is chosen, because the definition is broad and provides information about the goals of cyber security. The aspects of confidentiality, integrity and availability – which play an important role in information security – are part of the definition as well. These three aspects are known as the CIA triad.

ITU definition:

> *Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.*
>
> *Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.*
>
> *Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:*
>
> - *Availability*
> - *Integrity, which may include authenticity and non-repudiation*
> - *Confidentiality*

2.3 CYBER THREATS

Cyber incidents and related costs are on the rise as shown in previous research [78]. Cyber threats actors are increasingly sophisticated, targeted and serious, with yearly increases of up to 250% in amount of incidents measured [13]. Besides the amount of incidents, the costs related to cyber incidents are also on the rise. A global study conducted by HP & Ponemon Institute [37] shows an increase of 30% in costs of cyber crime in 2013 compared to the previous year. Business disruption is the largest external cost factor.

The increase of incidents and related costs keep on rising, which makes cyber security very urgent. Not surprisingly, preventing IT security incidents and protecting data are the two main priorities of corporate IT strategy [42].

THE NETHERLANDS The increase of cyber threats especially applies to the Netherlands. The Dutch National Coordinator for Security and Counter-terrorism reports six times as much high risk cyber incidents in 2012 compared to 2006 [56]. McAfee even reports that cyber crime in The Netherlands costs 1.50% of GDP [52]. This percentage is rather high, compared to other developed countries in the research (see table 1). An increasing amount of cyber incidents which account for 1.50% of the GDP make cyber security a very current subject.

Table 1: Costs of cyber crime to society as percentage of GDP [52]

Country	Percentage of GDP
Japan	0.02%
France	0.11%
United Kingdom	0.16%
European Union	0.41%
United States	0.64%
Netherlands	1.50%
Germany	1.60%

2.3.1 *Cyber threats to retail organizations*

Like any other type of organization, retail organizations can be the victim of a cyber attack. The last couple of years a few major incidents have occurred, causing retail organizations to leak the personal and

credit card information of millions of customers as well as employees. Examples of such incidents can be found on major cyber security news websites and blogs. Several recent cyber incidents are given in table 2. The effect of such incidents is not limited to the disclosure of information: financial and reputational damage are amongst other effects [78].

Table 2: Significant data breaches in the retail sector

Company name	Date	Damage
Target Corp.	December 2013	110M credit card numbers & personal data of customers [46]
Wm Morrison Supermarkets plc	March 2014	Theft of 100,000 employee details from Morrisons supermarkets [8]
Tesco PLC	February 2014	2,000 customer details [16]
Home Depot, Inc	September 2014	Information from 56M credit cards disclosed. [45]
Dairy Queen	October 2014	Theft of credit card information from the cash registers of 395 stores. [44]
Sears Holdings Corp.	October 2014	Theft of credit card information from the cash registers of 1200 Kmart stores. [7]

CYBER THREATS TO RETAIL IN THE NETHERLANDS Although the major retail cyber incidents happened outside of The Netherlands, incidents happen in The Netherlands as well. The Dutch retail sector has been subject to the skimming of bank cards [67], privacy issues [68]. Customer data has also been leaked, as can be seen from table 3.

Table 3: Data breaches in the Dutch retail sector

Company name	Date	Damage
CheapTickets.nl	October 2011	Personal information of 715,000 customers. [84]
Baby-dump	February 2012	Personal information of 134.000 customers. [11]
Perry Sport	May 2012	Personal information of 95.000 customers. [87]
Bol.com	July 2012	Personal information of 84,000 customers. [66]

2.4 COLLABORATION

Collaborative cyber security in the context of this research involves all types of collaboration initiatives *between* organizations. Two conditions apply:

- Participants from more than one organization are involved;
- the goal of the collaboration initiative is to improve cyber security.

Collaboration in the area of cyber security has the potential to decrease damage caused by cyber threats [78]. Exchanging information on information security between organizations allows increasing the accuracy of the detection of threats, by collectively correlating information about threats [24]. In addition, organizations belonging to the same industry typically suffer from the same cyber threats. Sharing and correlating information could help detecting those threats in an early stage and mitigate the damage [51, 89].

With cyber security becoming a larger problem, the retail sector can be a victim as well. The organizations in this sector are increasingly accumulating data and will even more rely on data and IT systems in the future. With the dependence on data and IT increasing, the impact of a cyber security incident becomes larger.

Cyber security is no longer in the hands of a single organization. To mitigate cyber security related risks, organizations have to work together. As Hamel et al. [28] shows in a research to the internal working of 15 strategic alliances, collaboration between organizations has proven to be successful. But does this also apply to collaboration in the area of cyber security in the retail sector?

3

RESEARCH DESIGN

The amount of cyber threats have been increasing over the last couple of years. These threats impose risk to retail organizations, because a successful cyber attack can cause significant data loss as can be seen in table 2, and consequently financial and reputational damage [78].

The goal of this research is to investigate how cyber attacks in the retail sector can be prevented and negative impact of cyber attacks can be mitigated using collaborative cyber security.

In section 3.1 the main problem is elaborated. In section 3.2 a solution design is proposed. Section 3.3 introduces the research questions.

3.1 PROBLEM STATEMENT

The main problem in this research is the *rise of cyber incidents and related costs in retail organizations*. Chapter 2 indicates an increase of cyber incidents and related costs. The retail sector is not spared as can be seen from the incidents described in section 2.3.

3.1.1 *Additional issues*

There are additional issues that play an important role in the retail sector, and increase the severity of the main problem. These issues follow below.

CONNECTED ORGANIZATIONS IMPOSE A RISK Information systems that cross organizational borders can subject an organization to additional risks. Such systems are designed to allow systems *outside* the organization to access systems *within* the organization and vice versa. A consequence is that the system outside the organization could be located in an organization that doesn't take adequate security measures. This means that a malicious entity is able to access your organization's information systems through another organization.

Illustrated in figure 2 are two *secure* organizations. Organization A has an agreement with organization B about the exchange of credit card information. When B is requesting access to credit card information A, organization A provides the requested credit card information to B.

In figure 3 organization B is *not secure*: malicious software has been installed somewhere in the computer systems of B. B's organization is requesting credit card information, which seems normal to A, since they have an agreement to do this. Yet, *without A knowing*, the credit card information is escaping from the information system through malicious software at B. This is obviously not what is supposed to happen.

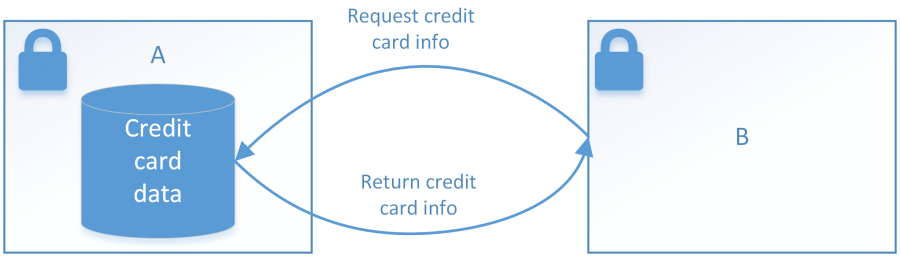

Figure 2: Normal collaboration through an information system that is accessible from outside

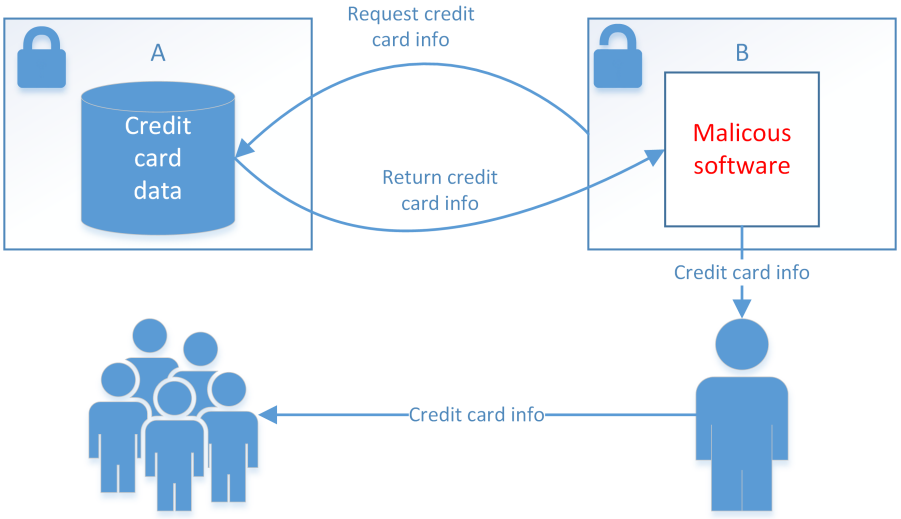

Figure 3: Credit card information is leaked *through* a compromised organization

What the example in figure 2 and 3 shows, is that although organization A is a secure organization, it is still vulnerable because its business partner, B, is not adequately protected.

This issue contributes to the main problem, because this type of interconnected information systems are becoming more common in re-

tail organizations. This makes adequate protection from cyber threats more difficult because an organization has to ensure that its business partners are also adequately protected against cyber threats, in order to protect its own digital assets.

IT IS THE KEY TO RETAIL INNOVATION In today's retail organizations IT already plays an important role, and new developments emphasize IT even more. Desai et al. [18] and Erich [19] describe a number of trends in retail grocery, of which the majority highly relies on the availability of consumer data and IT systems. For instance, one of the key changes in the business model of retail organizations is the creation of purchase occasions beyond the physical store: goods are ordered online and picked up later or delivered at home. Marketing is also taking a more digital approach by making extensive use of social media and involving the crowd by asking their opinions and letting them decide on new products ('crowd sourcing'). Retailers are learning more about their customers and are able to analyze large amounts of data about their customers. Customers on the other hand, are also willing to engage with retailers through loyalty programs and personalized offers.

Relying on IT-based innovations contributes to the main issue because these IT-based innovations are prone to cyber attacks, which can interfere with future innovations.

THE RETAIL SECTOR IS OF NATIONAL IMPORTANCE The Netherlands has defined twelve sectors that are considered 'critical infrastructures'. Critical infrastructures are concerned with products, services and supporting processes that can disrupt society heavily when unavailable [34]. It is important to national security that these sectors are operating well.

The food sector is amongst these twelve sectors. In the light of national security, the end points of the food sector are the most important. Retail organizations, especially supermarket organizations, take an important place at the end points of the food sector, as they provide the food to the Dutch consumers [33]. Because the retail sector is part of the critical infrastructure, there is a clear incentive to take additional measures to protect the retail sector.

3.2 RESEARCH OBJECTIVES

The main objective of this research is to identify how *collaborative cyber security* can be used to mitigate the rising amount of cyber threats in retail organizations.

3.2.1 *Scope*

Because of the extensiveness of the retail sector, this research focuses on *large retail organizations in the Netherlands* to obtain information and validate results. In previous sections organizations within the retail sector have shown to be very relevant to the topic because they are often the target of cyber attacks (table 2) and they are part of critical infrastructure (section 3.1.1). The results of this research can assist cyber security experts when reconsidering the current cyber security practices in the retail industry.

The scope is limited to large retail organizations: they are expected to have basic cyber defense activities in place that could be improved using collaborative cyber security. This is in contrast to small retail organizations that often do not have the basic cyber security activities in place to which collaboration can be integrated with.

3.3 RESEARCH QUESTIONS

The goal of this research is formulated in the following main research question:

> *How can collaborative cyber security be used to mitigate cyber threats in retail organizations?*

To answer the main research question, several aspects have to be researched. First, it is necessary to identify which cyber threats impose risk to the retail sector. Second, the different types of collaborative cyber security have to be identified in order to understand how collaborative cyber security can be used. Third, knowledge about the critical factors to the success of collaborative cyber security is needed in order to develop an appropriate solution. Therefore critical success factors to the solution have to be gathered. With the knowledge of the first three questions, a framework is created. How to design such a framework is addressed in the fourth question. This leads to the following research questions.

RQ1. Which cyber threats impose risk to the retail sector?

RQ2. Which types of collaborative cyber security exist?

RQ3. What are the critical success factors for a collaborative cyber security solution in the retail sector?

RQ4. What would be an appropriate collaboration framework for the retail sector?

3.4 RESEARCH METHODOLOGY

This section explains which methods and techniques are used to answer the research questions and the research goal. The research model for this research is depicted in figure 4 on page 15.

3.4.1 *Research question 1*

RQ1: Which cyber threats impose risk to the retail sector?

To answer this question, a threat model is created. Threats have been identified using both academic literature and publicly available resources such as annual reports on threats and news sources. Since the identified threats should match the environment that is used to validate the solution, special attention is paid to the Netherlands. Threats in this geographic region might differ from global threats. To identify the relevance for the retail sector, the results are tested against the opinions of experts in the sector. In this way additional threats can be added to the model or irrelevant threats can be removed from the model. This research question is elaborated in chapter 5.

3.4.2 *Research question 2*

RQ2: Which types of collaborative cyber security exist?

Existing academic literature is used to investigate the different types of collaboration in general and collaboration in cyber security. Additionally existing collaboration initiatives can be researched to see what types of collaborative cyber security exist. In chapter 6 this research question is elaborated.

3.4.3 *Research question 3*

> *RQ3: What are the critical success factors for a collaborative cyber security solution in the retail sector?*

Through a literature review, barriers and incentives to collaboration have been identified. The results are used to establish critical success factors for the introduction of collaborative cyber security in an organization. In chapter 7 this research question is elaborated.

3.4.4 *Research question 4*

> *RQ4: What would be an appropriate collaboration framework for the retail sector?*

The answers to the previous research questions are used to research what type of framework is needed for the retail sector. It is discussed whether a new framework has to be developed or an existing framework can be extended. This research question is elaborated in chapter 8.

3.4.5 *Main question*

> *How can collaborative cyber security be used to mitigate cyber threats in retail organizations?*

With the research questions answered, the main research question can be answered. The framework that is suggested in chapter 8 is designed in chapter 9, as a extension of the NIST Cyber Security Framework. Chapter 10 explains how the developed framework can be used to mitigate cyber threats in retail organizations. Recommendations for the realization of collaborative cyber security are made along with recommendations for the implementation of collaborative activities on top of the NIST Cyber Security Framework.

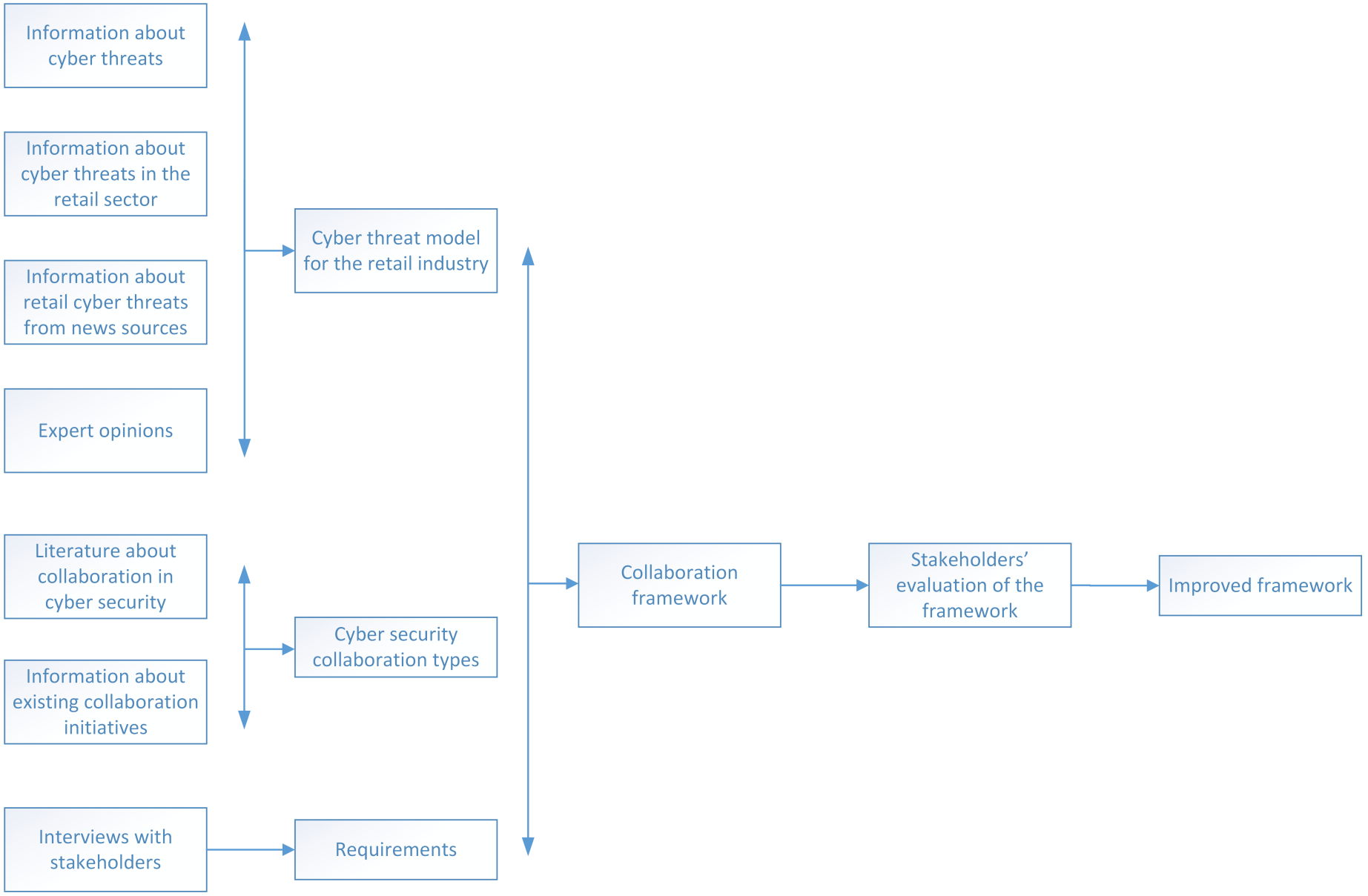

Figure 4: Research model

4

RELATED WORK

There have already been some efforts in the key areas of this research. This chapter describes the most relevant research in the threat classification, collaboration in cyber security and integration of cyber security in organizations.

4.1 THREAT CLASSIFICATION

There is a variety of cyber attacks known to individuals and organizations. Different types of attacks require different types of measures to prevent attacks from happening or mitigate the impact. There are several classifications to categorize different cyber attacks based on properties they share. It makes sense to classify different attacks based on a specific property, as mitigation and prevention measures are often effective for multiple attacks sharing this specific property.

There are different types of taxonomies to classify the different threats. Jiang [39] and Jiang et al. [40] state that existing work on taxonomies can be assigned into four groups.

- *Based on vulnerability*: taxonomies that classify threats and attacks based on the vulnerability in the system, which is the origin of a threat.
- *Based on a list of terms*: a list of predefined terms is established. Attacks and threats can be assigned to each of the terms.
- *Based on application*: this approach classifies threats and attacks per application or for a specific application.
- *Based on multiple dimensions*: these taxonomies define several dimensions, each with several characteristics, which together classify the threat or attack.

An example of a vulnerability-based taxonomy is the taxonomy of Cebula & Young [12]. They introduce a taxonomy of operational risk. It positions operational risks into one of four vulnerability categories that identify the source of the risk. Each of the categories has several

subcategories, which add up to a total of 57 subcategories (see figure 5).

1. Actions of People	2. Systems and Technology Failures	3. Failed Internal Processes	4. External Events
1.1 Inadvertent	**2.1 Hardware**	**3.1 Process design or execution**	**4.1 Disasters**
1.1.1 Mistakes	2.1.1 Capacity	3.1.1 Process flow	4.1.1 Weather event
1.1.2 Errors	2.1.2 Performance	3.1.2 Process documentation	4.1.2 Fire
1.1.3 Omissions	2.1.3 Maintenance	3.1.3 Roles and responsibilities	4.1.3 Flood
1.2 Deliberate	2.1.4 Obsolescence	3.1.4 Notifications and alerts	4.1.4 Earthquake
1.2.1 Fraud	**2.2 Software**	3.1.5 Information flow	4.1.5 Unrest
1.2.2 Sabotage	2.2.1 Compatibility	3.1.6 Escalation of issues	4.1.6 Pandemic
1.2.3 Theft	2.2.2 Configuration management	3.1.7 Service level agreements	**4.2 Legal issues**
1.2.4 Vandalism	2.2.3 Change control	3.1.8 Task hand-off	4.2.1 Regulatory compliance
1.3 Inaction	2.2.4 Security settings	**3.2 Process controls**	4.2.2 Legislation
1.3.1 Skills	2.2.5 Coding practices	3.2.1 Status monitoring	4.2.3 Litigation
1.3.2 Knowledge	2.2.6 Testing	3.2.2 Metrics	**4.3 Business issues**
1.3.3 Guidance	**2.3 Systems**	3.2.3 Periodic review	4.3.1 Supplier failure
1.3.4 Availability	2.3.1 Design	3.2.4 Process ownership	4.3.2 Market conditions
	2.3.2 Specifications	**3.3 Supporting processes**	4.3.3 Economic conditions
	2.3.3 Integration	3.3.1 Staffing	**4.4 Service dependencies**
	2.3.4 Complexity	3.3.2 Funding	4.4.1 Utilities
		3.3.3 Training and development	4.4.2 Emergency services
		3.3.4 Procurement	4.4.3 Fuel
			4.4.4 Transportation

Figure 5: Cebula & Young's taxonomy of operational risk [12]

Icove et al. [32] introduce a list of 24 terms (see table 4). Using a list of terms is popular and simple, yet the terms do not tend to be mutually exclusive [30].

Microsoft's STRIDE [38] provides six categories: spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege. The categories provide a clear threat classification and an expansion of the CIA principles [65].

Table 4: List of terms by Icove et al. [32]

Wiretapping	Trojan horses	IP spoofing
Masquerading	Password sniffing	Session hacking
Trap doors	Eavesdropping on Emanations	Logic bombs
Tunneling	Unauthorized data copying	Scanning
Salamis	Viruses and worms	Harassment
Dumpster diving	Degradation of service	Traffic analysis
Software piracy	Excess privileges	Timing attacks
Covert channels	Denial of service	Data diddling

Howard & Longstaff [30] introduce a taxonomy of computer and network incidents, that is based on 7 dimensions (see figure 6). Every dimension has several characteristics (3 to 11 per dimension).

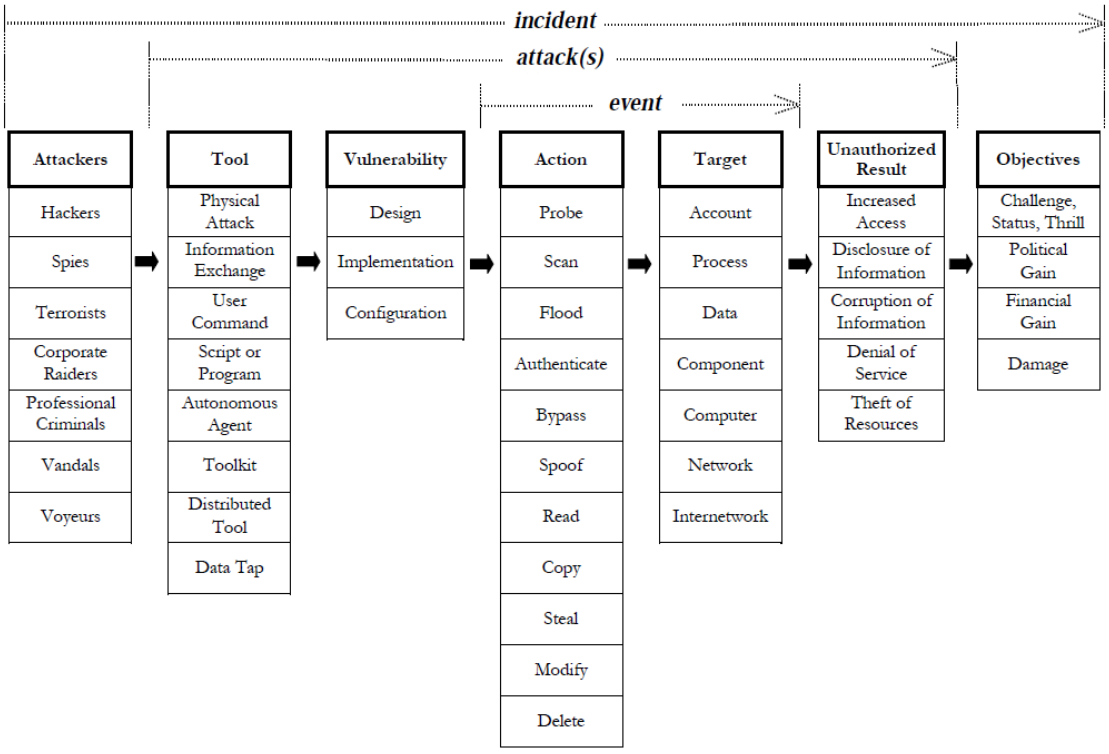

Figure 6: Howard & Longstaff's computer and network incident taxonomy [30]

4.1.1 *Considerations*

The aforementioned taxonomies vary in complexity from a small set of threat categories to more extensive taxonomies that support the categorization of a threat to a very detailed level. When choosing a certain taxonomy, it is important to look at the purpose and the implications of choosing a specific taxonomy. Choosing a very simple taxonomy may result in inappropriate actions, because threats requiring a different approach could be assigned to the same category. The categories are too general for this purpose and need refinement. A very detailed taxonomy on the other hand, could require too much different approaches from a system than is necessary.

4.2 COLLABORATION

Information exchange is a crucial element in collaborative cyber security, but which information is exchanged and in which way differs.

There are different frameworks that describe exchange models. Zhao et al. [89] propose a framework on collaborative information sharing, that aims to improve community cyber security. Xu [85] identifies the need to use collaborative cyber defense against collaborative cyber attacks and presents a framework to evaluate the effectiveness of collaborative defense against collaborative attacks.

Participating organizations can decide to exchange all available information, but are often afraid of disclosing sensitive or competitive information [10, 88]. Privacy preservation therefore plays an important role in literature related to collaboration. Tsai et al. [76] propose a mechanism to minimize the amount of information shared. Minimizing the amount of information shared should increase the willingness to share. Lincoln et al. [48] propose a set of data sanitization techniques that enable community alert aggregation and correlation while maintaining privacy for alert contributors.

4.3 CYBER SECURITY IN ORGANIZATIONS

Cyber security can be integrated into organizations in many ways. ways. There are IT security frameworks that provide best practices at high-level to help determine what should be in a security program. Additionally there are risk management methodologies that are more specific and focused at the enterprise architecture.

4.3.1 *IT security frameworks*

ISO/IEC 27000 SERIES The ISO/IEC 27000 series is a series of standards created by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) that specify the requirements of an Information Security Management System (ISMS). ISO/IEC 27001 specifies the requirements for an ISMS and allows for auditing and third party certification.

NIST SP800-53 The NIST SP800-53 provides security and privacy controls for federal information systems and organizations with the exception of those related to critical infrastructure. [64]

NIST CYBER SECURITY FRAMEWORK The NIST Cyber Security Framework (CSF) was created to improve critical infrastructure cyber security. It contains cyber security activities, outcomes and informative references. It is technology neutral and offers a flexible and risk-based implementation that can be used with a wide variety of existing cyber security risk management processes. The framework was designed to complement an organization's risk management processes and cyber security program rather than replacing it. [57]

4.3.2 *IT security methodologies*

GARTNER EISA Gartner was the first to present how information security should be incorporated into enterprise architecture. This resulted in Enterprise Information Security Architecture (EISA) [59]. The Gartner EISA consists of three levels of abstraction (conceptual, logical and implementation) and three viewpoints (business, information and technical), yet it offers only a general description of the structure and no specific methodology for implementing the framework [69].

SABSA The Sherwood Applied Business Security Architecture (SABSA) is a risk-driven EISA that focuses on business initiatives. SABSA has a similar structure as the Zachman framework, but focuses on business-to-security methodology where Zachman doesn't. [59] SABSA consists of a six-layered architecture with horizontal layers of contextual, conceptual, logic, physical and component and the vertical layer of security service management. SABSA is more practical in comparison to Gartner as it comes with a methodology. [69]

4.3.3 *Considerations*

There are different ways of integrating security in organizations. The methodologies focus more on the implementation of security in the enterprise architecture, frameworks focus more on high-level contents of a security program. Where the methodologies are concrete, the frameworks are more abstract and provide information on which controls should be in place and which security activities should be part of the security strategy.

5

CYBER THREATS IN THE RETAIL SECTOR

For an effective defense against cyber threats, it is necessary to know which threats impose a risk to organizations in the retail sector (research question 1). The threats are gathered through a literature research and validated through interviews with experts. A threat model is created from the results.

5.1 THREAT MODELING

Threat modeling is the process of enumerating and risk-rating malicious agents, their attacks and those attacks' possible impact on the system's assets [72]. As can be read from the definition, threat modeling is used to identify threats and impact on a *system*. Within a sector many organizations exist, each with their own systems. Making a separate threat model for every system in every organization would not serve the purpose of this research. In this case, a threat model for a *sector* is required.

Information about cyber threats is already available. By using existing threat information and information about the impact on retail organizations, different threats that face the retail sector are identified. This information is turned into a list of threats and their risk rating: the threat model. This model is validated by experts. The threat modeling approach is depicted in figure 7.

Figure 7: Threat modeling approach

The downside of using existing threat information is the lack of a commonly used classification. Most research reports tend to use their own set of definitions. Trustwave [75] e.g. is talking about a threat category called '*website and web application attacks*', Verizon [77] mentions '*web attacks*' while the BRC [9] generalizes such attacks to '*hacking*'. The lack of a common classification is an obstacle to categorize threats.

A solution to the lack of a common classification, is to find an existing classification in which the identified threats can be categorized. By assigning the identified threats to the different categories of one classification, it can be determined which category contains the most threats. It is very likely that this category is an important area of focus for the application of collaborative cyber security.

The lack of consistent naming of threats between the reports indicates the need for a simple, abstract model. Such a model is necessary in order to categorize the threats correctly, as it is difficult to categorize the threats in a model with a lot of details. From the classifications and taxonomies described in chapter 4, Microsoft's STRIDE matches this need: its six threat categories match the level of detail that is used in the threat reports.

Microsoft STRIDE [38] provides a threat modeling technique which uses six threat categories, related to how an intruder gets into the system. By using the classifications introduced in Microsoft's STRIDE approach, the mentioned threats can be assigned to one of the six groups of STRIDE. Each of the six categories stands for something an attacker can do to an application, and for each category the risk can be determined. The six defined categories, and their definitions can be found in table 5.

The approach of figure 7 is applied in the next sections. Threat information is gathered in section 5.2, the threat model based on this threat information is created in section 5.3 and the model is validated in section 5.4.

Table 5: STRIDE threats and definition [38]

Threat	Definition
Spoofing	An attacker tries to be something or someone he/she is not.
Tampering	An attacker attempts to modify data that's exchanged between your application and a legitimate user.
Repudiation	An attacker or actor can perform an action with your application that is not attributable.
Information disclosure	An attacker can read the private data that your application is transmitting or storing.
Denial of service	An attacker can prevent your legitimate users from accessing your application or service.
Elevation of privilege	An attacker is able to gain elevated access rights through unauthorized means.

5.2 THREAT INFORMATION

This section contains two parts. First information about global threats is gathered, this is completed with information about threat in the Netherlands.

5.2.1 *Global cyber threats*

On a global level there are several organizations and research institutes that produce reports about general risks and cyber risks. The main challenge is to find the right information. Plenty of reports present data on the retail sector and on cyber threats, yet a combination of cyber risks and the retail sector is something that's missing. By aggregating the useful information from the different reports, several important threats can be identified. Table 6 shows the global threats to the retail sector that are identified in major reports.

Table 6: Global threats to the retail sector

Report	Most important threats
Verizon [77]	POS intrusion, denial of service, web app attacks
Locton [50]	Denial of service, data compromises, cyber extortion
Trustwave [75]	Web attacks
Whitehat [82]	Information leakage, cross-site scripting
Willis [83]	Loss or disclosure of confidential information, loss of reputation, malicious acts and cyber liability

5.2.2 *Cyber threats in the Netherlands*

In addition to global threats shown in table 6, this section provides information about threats specific to the Netherlands. Although the Netherlands is often represented in global reports, sources providing information specifically about the Netherlands are difficult to find.

The Dutch National Cyber Security Centre (NCSC) reports that the most important threats within government bodies are *malware infections, information exposure, phishing, and DDoS attacks* [54]. This is the only information about threat types that is publicly available and unfortunately it is not retail-specific. Despite the NCSC report not being directly related to retail, it can enrich the identified global threats by

adding threats specifically related to the Netherlands. Therefore the threats identified by NCSC are incorporated into the threat model.

5.3 THREAT MODEL

The identified threats in the previous sections cannot be placed into the threat model directly: first it has to be determined in which of the six categories of STRIDE they fit best. If threats do not fit in the model, it is explained why and they are omitted if necessary. Below the threats from the global reports (table 6) and the Dutch report are grouped together and per group it is discussed in which STRIDE category the group of threats belongs.

POS INTRUSION Point-of-Sale (PoS) intrusion involves the modification of data between the PoS systems and the user and is mentioned by Verizon [77]. At PoS systems retail transactions are conducted. Attackers interfere with communications between the user's payment card and the application. This group of threats has a clear relation with STRIDE's category *tampering* because the modification of data that is exchanged between the user and the system.

DENIAL OF SERVICE Verizon [77] and Locton [50] mention Denial of Service (DoS) and distributed denial of service (DDoS) is mentioned by the NCSC [54]. DoS and DDoS are threats that attempt to prevent legitimate users from accessing applications or services and therefore are related to the *Denial of service* STRIDE category.

WEB ATTACKS Web attacks focus on the application itself [15]. Trustwave mentions web attacks and more specifically, SQL injections [75] to be relevant to retail. Web app attacks are mentioned by Verizon [77] and are considered to be web attacks as well. Whitehat [82] mentions cross-site scripting, which is also a type of web attack. Categorizing web attacks is more difficult, as their effects and goals can be categorized under multiple categories of STRIDE [15]: it depends on how the web attack is conducted. Unfortunately the sources that mention web attacks do not mention any information that helps in determining which STRIDE category is applicable: web attacks cannot be taken into account for the STRIDE threat model.

DATA COMPROMISE Lockton [50], Whitehat [82], Willis [83] and the NCSC [54] respectively mention data compromise, information leakage, loss/disclosure of confidential information and information

exposure. All are related to the leakage of information out of the organization. This kind of threat is directly related to STRIDE's *information disclosure* category since this kind of threats allow an attacker to read private data stored or transmitted in an organization's applications.

CYBER-EXTORTION Lockton [50] describes cyber extortion as a threat that can be carried out through different attack types such using a DDoS attack on the target or infect the target with a Trojan virus. This puts the attacker in a powerful position to extort money from the target. Cyber extortion is an attack goal that can be achieved through cyber attacks from different STRIDE categories. The example of DDoS would be a *denial of service*, but a Trojan virus could be positioned in the *elevation of privilege* category. Because there are threats in different categories that enable cyber extortion, cyber extortion itself does not belong to a STRIDE category.

LOSS OF REPUTATION Willis [83] mentions loss of reputation as the most important risk to retail. Loss of reputation can be the *effect* of a variety of cyber threats. The Target example in chapter 1 mentions the loss of credit card data and personal data, which also caused reputational damage. Kaspersky [41] reports that loss of reputation is a very serious risk, and often relates it to information disclosure but to 'incidents' in general as well. Although loss of reputation is the *effect* of a cyber incident and not the *cause*, the report of Kaspersky provides reasons to believe that loss of reputation in their report can be categorized as STRIDE category *information disclosure*.

The report of Willis [83] mentions loss of reputation separate from 'loss or disclosure of confidential information'. Loss or disclosure of confidential information was previously categorized as STRIDE category information disclosure. It is likely that Willis relates loss of reputation to something else than information disclosure.

In the case of Willis, this specific threat is omitted from the model, as it is unrelated to a specific STRIDE category. In the case of Kaspersky, it is assigned to 'information disclosure'.

MALICIOUS ACTS In the report of Willis [83] malicious acts is reported but no explanation is given. A malicious act in general involves something or someone doing something intentionally wrong: this could be related to any of the STRIDE categories. Because there is no clarity about the STRIDE category to which this threat belongs, it is omitted.

CYBER LIABILITY This risk is mentioned in the report of Willis [83]. Cyber liability relates to taking responsibility in case of cyber incidents. An example is that companies in the US have to inform customers when their data is leaked. This can be costly since the company has to reach all users, and it is likely that it harms the company's reputation. Das [17] supports this: cyber liability insurances are used to cover significant business and litigation costs *to address a breach episode*, which involves the disclosure of information. This threat is addressed to the STRIDE category of *information disclosure*.

MALWARE INFECTIONS This threat is mentioned by the NCSC [54] and refers to software installed on a client's computer system. This software can be used for a variety of purposes, such as obtaining financial information, setting up botnets, saving keystrokes and collecting browsing behavior, therefore this threat can be home to multiple categories of STRIDE. Malware could gain access to files it doesn't have authorization for (elevation of privilege), make resources unavailable (denial of service) or leak information (information disclosure). This threat doesn't belong to a specific STRIDE category and is omitted from the threat model.

PHISHING The NCSC describes phishing as a threat to organizations [54]. Phishing is an umbrella term for digital activities with the object of tricking people into giving up their personal data. With this data criminal activities such as credit card fraud and identity theft can be employed. With personal data such as credentials, an attacker can gain access to a company's information systems. This means phishing can also indicate threats that are in several categories of STRIDE: the same as with malware infections applies: it is unclear in which category phishing belongs and it is omitted.

5.3.1 *Risk rating of threats*

Now that the identified threats are placed into the classification, the risk rating of each of the classification categories is determined. Because there is no quantitative information in terms of downtime, costs, etc. available for each of the threats, a different approach is needed. This different approach involves the usage of the only quantitative information that is available: how often a specific threat related to a STRIDE category is mentioned in the used sources.

In table 7 sources that say something about a threat are grouped per STRIDE category. This gives the following results: *information disclo-*

Table 7: STRIDE threat categories literature review

Threat	References
Spoofing	-
Tampering	[77]
Repudiation	-
Information disclosure	[17, 41, 50, 54, 82, 83]
Denial of service	[50, 54, 77]
Elevation of privilege	-

sure (mentioned in six sources) is the most common threat, followed by *denial of service* (mentioned in three sources) and *tampering* (mentioned in one source).

5.4 VALIDATION

In the previous sections an effort was made to identify the threats to the retail sector. The resources used are global threat reports containing information about the retail sector and a general report about cyber security in the Netherlands. Whether the threats identified in the previous section reflect the actual threats in the practice has to be verified by interviewing experts in the sector.

5.4.1 *Interview questions*

For the validation of the threats using interviews, questions are made. The purpose of this interview is to validate the literature research and if necessary add missing threats and remove irrelevant threats. The following boundaries define the validation interviews.

> **Type of experts:** security experts with a strong affinity to the retail sector
> **Target of the interview:**
> remove irrelevant threats from the model;
> add relevant threats that are missing to the model;
> discover the source of threats.

The interview questions that are formulated within these boundaries can be found in appendix B.1. For the validation of the STRIDE threat model, every threat category is explained to the interviewee to avoid

confusion. Next the interviewees were invited to indicate the categories that impose the largest risks to the interviewee's organization.

5.4.2 *Results*

For the validation of the threat model four people have been interviewed. The interviewees who wish to remain anonymous include three c-level [1] cyber security experts from large retail organizations employing significant activities in the Netherlands and an independent cyber security expert. More details about the interviewees can be found in appendix B.2.

The interviewees were asked to rank the STRIDE threats, which resulted in the interviewees giving a top-2 of threats, and in some cases a third or fourth threat that they also considered worth mentioning. The results have been summarized in table 8.

The results from the interviews show that *information disclosure* and *denial of service* impose the most risks for retail organizations. Three out of four interviewees rank respectively information disclosure and denial of service as the number one and two threat categories. One out of four interviewees ranked denial of service as the most important threat category and acknowledges the importance of information disclosure, but ranks it lower as this organization of this interviewee does not handle much customer data.

From the other STRIDE categories, elevation of privilege, spoofing and tampering are also mentioned and threats with an interface to repudation have been discussed. These threats however, do not play a role as significant as information disclosure and denial of service.

Table 8: Summary of interview validation

	Interviewee			
Threat	1	2	3	4
Spoofing	4	-	-	3
Tampering	-	-	-	-
Repudiation	-	-	-	-
Information disclosure	1	1	2	1
Denial of service	2	2	1	2
Elevation of privilege	3	-	-	-

1 C-level refers to the highest-level executives in senior management, of which the title often starts with 'chief'.

RANKING THE RESULTS Information disclosure is in most cases considered to be a larger risk than denial of service. The risk of information disclosure is considered larger because of reputation-related issues: when customer information is exposed, this could mean permanent loss of customers. Denial of service on the other hand, could cause loss of customers for a certain period of time but the chances of the customers to return are considered to be higher.

The interviewed security experts consider the other threat categories to be less important than information disclosure and denial of service. It is difficult to determine an order of importance for these four categories since only a few sources report on these categories. Therefore, these four categories are placed at the same level below information disclosure and denial of service.

5.5 CONCLUSION

The literature research and validation through interviews has resulted in a ranked list of cyber threats. This list can be used to provide an answer to research question 1: *"which cyber threats impose risk to the retail sector?"*.

There's consensus between literature and practice about the top-2 threat categories: both literature and practice consider information disclosure the most important threat category, followed by denial of service (table 7 and table 8).

From the four remaining threat categories, spoofing, tampering and elevation of privilege are also mentioned but especially from the interviews it becomes clear these threat categories are far less important than the top-2 information disclosure and denial of service. Repudiation is not mentioned at all.

When ranking the threat categories, the top-2 is followed by the occurrence of the other threat categories, closing with repudiation. It should be noted that cyber security efforts should not only focus on the two threat categories identified as main issues in this chapter, the other threat categories also require sufficient protection.

The threats are ranked as follows.

1. Information disclosure
2. Denial of service
3. Spoofing, tampering, elevation of privilege
4. Repudiation

6

COLLABORATION

This chapter is dedicated to research question 2: "Which types of collaborative cyber security exist?". First different types of collaborative cyber security are illustrated in section 6.1, and placed into a classification in section 6.2. In section 6.3 existing initiatives on collaborative cyber security are explained. The last section concludes the chapter and provides an answer to the research question.

6.1 TYPES OF COLLABORATION

Collaboration between organizations can take many different shapes. The type of collaboration varies from initiatives as simple as quarterly meetings with colleagues from other organizations to automatic data exchange between participating organizations. Because there is a lot of diversity in collaboration, it makes sense to investigate the different types of collaboration. A previously conducted literature study by the author of this research investigated the state of art in the area of collaborative cyber security. The result of this study was a set of five attributes that define a cyber security collaboration [78].

The following five attributes are identified and described below. These attributes serve as a foundation for the classification that is introduced in this chapter.

- Type of collaboration
- Ownership
- Architecture
- Collaborating parties
- Type of data shared

6.1.1 *Type of collaboration*

Sharing intelligence on cyber security level between organizations is traditionally done by the use of telephone, mail, face-to-face conversations and meetings [73]. The use of IT solutions to automate this process potentially improves the value of the collaboration process by accelerating the access to knowledge and integrating cyber security defense systems of multiple organizations.

MANUAL SHARING A way of collaborating that could be realized using existing infrastructure, is sharing knowledge through structured mailing lists, newsgroups and internet forums. Knowledge has to be added and requested in a manual fashion. When a local team of security experts doesn't know how to handle in case of a specific threat, they can consult others through such mailing lists, newsgroups and internet forums [25, 49]. It is used as a way to acquire extra information on specific threats. This appears to be very much like the traditional sharing of intelligence described above, yet it allows a user to search the stored knowledge as it is available digitally.

An example is the *Network of practice* described by Papadaki & Polemi [60]. It is a platform in which participants can share information through forums and repositories. In addition, it provides tools to make existing knowledge easily accessible.

AUTOMATIC SHARING Data can be collected, analyzed and distributed in an automated fashion. Yu et al. [86] for instance, describe data (security, system, application logs, etc.) being collected from end user devices and streamed to a central database, which is automatically processed, stored and indexed in the cloud. The resulting information is made available for members participating in the system. This is what Zhao & White [89] call 'Routine Information Sharing': the type of data collected is usually meta-data of digital connections. Incident-specific information is also shared, but has a less automated nature.

6.1.2 *Ownership*

An important property of a collaborative cyber security system is who owns the system and who makes the decisions regarding the accessibility of information. Throughout the literature study the following types of ownership structures are found.

SHARED OWNERSHIP The collaborative system is owned by a group of companies, which pool their resources to collectively provide security for their computer systems [26]. The companies in the network share in costs of maintenance and they are able to benefit from knowledge from others in the network. Decision making might be more difficult with multiple owners, because the members of the network have to be in accordance with each other.

THIRD PARTY A third party manages security for a group of firms, this usually is based on a for-profit model. The third party is the owner of the system and makes decisions [26]. Such third party organizations benefit from economies of scale because they can share skilled security professionals and a security support infrastructure across organizations. In addition, attack information from multiple organizations can be correlated to provide a more effective response [88].

6.1.3 *Architecture*

Information has to be shared between the participating organizations, and has to be obtained from the participating organizations as well. To support this process, a certain type of IT architecture is required. Architectures can roughly be categorized into two categories: centralized architecture and distributed architecture.

CENTRALIZED ARCHITECTURE A centralized architecture contains a number of distributed nodes that are connected and coordinated through a central unit [29]. The nodes provide the central unit with the information they collect, processing is performed at the central unit (see figure 8). A key advantage of the use of a centralized architecture is increased threat detection accuracy: all data from the nodes flows to the central unit [24, 80]. This provides the central unit with more information to identify threats and to perform analytics, and allows the central unit to inform the nodes *directly*. In addition, it can be offered as a service (SaaS), or as a web service so it can be implemented in a Service-Oriented Architecture [27].

Centralization has an important disadvantage as well: there's a single-point-of-failure. Since the system is controlled from a single central unit, all operations are relying on the availability of the central unit. If this central unit is not working, the entire architecture is not working. Traffic bottlenecks are another danger [24], yet traffic volume can be reduced by moving certain processing activities to the nodes [80].

DISTRIBUTED ARCHITECTURE In a decentralized architecture, a centralized unit is absent. The peers in the system organized individually [29], and are connected to each other (see figure 9). The advantage is that the failure of a single node doesn't have much impact on the system. This has a downside: the amount of information in every single node is much lower than in a centralized setting. The latter lowers the accuracy of detection [24, 80].

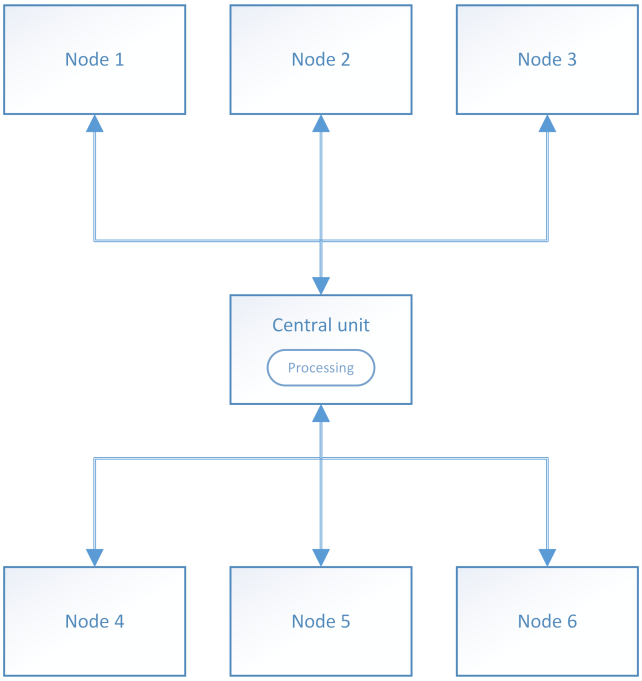

Figure 8: Centralized architecture

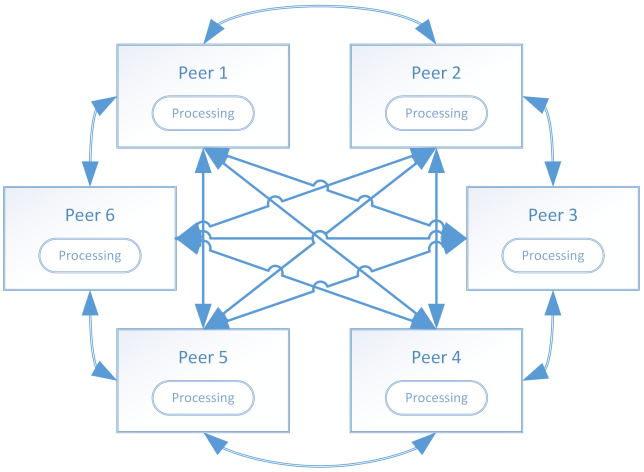

Figure 9: Distributed architecture

6.1.4 *Collaborating parties*

There are different types of compositions in collaborative cyber security. A network of information exchange, can be limited to organizations of a specific type or it can be open to any organization with disregard to the industry the organization is in or the position it has in this industry.

Research has illustrated different types of collaboration within specific groups of organizations. Horizontal collaboration (between companies that have the same role in the same industry), types that focus on vertical collaboration (between companies that have a different role in the same industry) and open collaboration (between companies that do not necessarily share the same role or industry).

OPEN COLLABORATION For this type of sharing network, there are no special requirements for joining: everyone can participate. An example is the Internet Storm Center's DShield. DShield analyses users logs from firewalls from volunteers around the world. The results are accessible by anyone [10]. The web forums described by Goodall et al. [25] describe information sharing through mailing lists and newsgroups, which are accessible by everyone.

HORIZONTAL COLLABORATION Collaborating on a horizontal level involves organizations that conduct the same kind of activities in the same industry. They possibly are competitors, but can both benefit from shared knowledge. An example of industry collaboration on a horizontal level is an Information Sharing & Analysis Center (ISAC). ISACs are established under Presidential Decision Directive/NSC-63 in the United States and are responsible for critical infrastructure protection in several key industries [26].

VERTICAL COLLABORATION In this type of collaboration the exchange of information takes place among organizations working in the same industry, but with different positions, in a supply chain for example. Their business processes are often connected and they rely on each other to create value. The benefits of being connected also bring risks: IT has removed the traditional layers that used to protect an organization's assets and processes [71]. Information security risks of organizations in a supply chain are interlinked, shared and can propagate from one to another. Therefore it is important for organizations in a supply chain to collaborate [31]. A suggested solution to facilitate information security sharing in this scenario, is to set up an investment pool amongst supply chain members, that allows one allocation of resources to the members that need it the most. Organizations that face the largest losses, can protect themselves by allocating their resources to the security of organizations that are the most susceptible to targeted attacks and disruption risks [31].

6.1.5 *Type of data shared*

There are different types of data that can be exchanged in collaborative cyber security networks. The types vary from simple information about the direction or origin of data to detailed information about events.

IP ADDRESSES An IP address identifies the source of malicious packets towards an organization. Klump & Kwiatkowski [43] propose a system that facilitates the sharing of potentially dangerous IP addresses in order to detect and prevent intrusion. By sharing information about dangerous communication sources, damage can be limited to just the first participant that receives the communication.

SECURITY LOGS Zhang et al. [88] illustrate a system that correlates security logs in an anonymized fashion. Port scanning and (distributed) denial of services attacks can be successfully detected through such a system, and potentially other attacks as well. The anonymization is used to overcome the barrier of sharing sensitive information which is faced by some organizations. In addition, logs across organizations are correlated to improve the system's response.

EVENTS When events such as a security incident occur at a participating organization, information about these events is shared [14]. This information can vary from simple network information to detailed activity reports produced by complex applications such as intrusion or anomaly detection systems [48]. In addition, proposed *countermeasures* can also be shared amongst the participants [76].

6.2 CLASSIFICATION

The five identified attributes identified by previous research of this author can be used to classify a type of collaborative cyber security [78]. In this section a classification table is created based on these attributes.

6.2.1 *Classification table*

The attributes illustrated above can be used to classify existing and new collaborative cyber security initiatives. To classify a collaborative cyber security initiative, for each of the attributes a *type* is chosen. The type describes the interpretation of the attribute in the collaboration that is being classified. Table 9 is the collaborative cyber security classification based on the defined attributes. For every attribute, several already identified types [78] are given.

EXTENSIBILITY The classification (table 9) is extensible. The types that are currently listed below each of the attributes are discovered

in the literature research used to identify the attributes. Additional types can be added to each of the attributes.

In the light of this research, the classification table is useful in the case of newly developed collaborative cyber security initiatives. For each of the attributes requirements can be defined, that must be met in order to prevent misunderstanding of collaboration amongst collaboration partners. This leads to the defined attributes with a type attached to each attribute. These types and requirements are used as development guidelines.

Table 9: Collaborative cyber security classification table

Attribute	Type of collaboration	Ownership	Architecture
Type	Manual sharing Automatic sharing ⋮	Shared ownership Third party ⋮	Centralized architecture Distributed architecture ⋮

Attribute	Collaborating parties	Type of data shared
Type	Open collaboration Horizontal collaboration Vertical collaboration ⋮	IP addresses Security logs Events ⋮

6.3 EXISTING INITIATIVES

There are some existing efforts on collaborative cyber security as well. This section describes several existing initiatives.

6.3.1 *Information Sharing & Analysis Centers*

The Information Sharing & Analysis Centers (ISACs) are collaborative initiatives in which organizations within a specific sector collaborate. ISACs are often established under pressure of the government. In the United States, most ISACs were established in response to Presidential Directive 63. This directive mandated that public and private sectors share information about physical and cyber security threats and vulnerabilities to help protect the U.S. critical infrastructure [22].

One of the most advanced ISACs is the Financial Services ISAC (FS-ISAC), established in the United States in 1998, right after the previously mentioned Presidential Directive 63. In the meantime, the FS-

ISAC has members and partners across the whole world. [22] The FS-ISAC provides its members with resources to support their cyber security practices. These resources include an automated emergency notification service, biweekly threat conference calls and reports on industry trends.

A series of cyber incidents at large retail organizations in the United States were reason for the Retail Industry Leaders Association (RILA, a sector association) to adopt the practices of the FS-ISAC and establish a retail equivalent: the Retail Cyber Intelligence Sharing Center (R-CISC). In the R-CISC retailers are sharing cyber threat information among themselves and the R-CISC provides training, education and research resources for retailer organizations. [62]

In the Netherlands, such ISACs also exist for critical infrastructure sectors. The Dutch government provides support for establishment and operating the ISAC. Examples are ISACs for the financial, energy, telecom and healthcare sectors. [55]

6.3.2 *Collaboration in the oil & gas industry*

Collaboration is part of the cyber security operations at an organization in the oil & gas sector. A cyber security expert in the oil & gas sector explains in an interview that there are frequent meetings between cyber security experts from competing organizations [3].

In this sector, frequent meetings are held in order to exchange information about threats. Although the participating organizations are competitors, the participants share the idea that cyber security is an area in which collaborating is more beneficial, rather than competing. Threat information is exchanged in a standardized format between participants through a portal and through e-mail. A standardized format is a necessity: it gives all participants a clear understanding of threat information and reduces misinterpretations.

The collaboration is successful because the frequent meetings keep the participants up to date about recent developments at other organizations. Additionally, the frequent meetings lower the threshold for participants to contact one another outside the meetings.

6.4 CONCLUSION

In this chapter different types of collaborative cyber security are studied. The results are used to make a classification that can be used to

classify existing and new applications of collaborative cyber security. The classification contains the following categories.

- Type of collaboration: the way knowledge and information is shared across organizations.
- Ownership: the type of ownership structure that is maintained.
- Architecture: the system architecture that facilitates the collecting and exchanging of information is organized.
- Collaborating parties: the composition of the group of organizations that collaborate.
- Type of data shared: the characteristics of the information that is collected and exchanged.

The five attributes are used to make a classification (table 9 on page 39). For each of the attributes, several possible types that were found in the literature review are given. The classification itself is extensible: new types of attributes can be added to the classification.

The classification can be used to classify both existing and newly developed initiatives of collaborative cyber security. The classification attributes can serve as a foundation for the establishment of requirements for such a collaborative cyber security initiative, to prevent misunderstanding between collaborating organizations.

7

CRITICAL SUCCESS FACTORS

Introducing something new to an organization is not guaranteed to succeed. There are many barriers that prevent a change from being successful. Moving from 'traditional' cyber security towards collaborative cyber security inevitably reveals barriers that are in the way of successful adoption. The elements that are necessary for the successful design of collaborative cyber security are called 'critical success factors'.

Because the success of collaborative cyber security depends on these critical success factors, they are researched beforehand. The findings are used as guidelines for the design of a collaborative cyber security solution.

In this chapter the critical success factors for collaborative cyber security are identified through reviewing academic literature. The third research question is answered: "what are the critical success factors for a collaborative cyber security solution in the retail sector?".

7.1 LITERATURE

There are many barriers that prevent the successful adoption of a collaborative approach. To get an indication, the research of Robinson & Disley [63] has identified challenges for information sharing in the context of network and information security and presents a set of barriers (figure 10) based on a conducted Delphi study.

The literature mainly focuses around two topics: trust and data privacy. These two factors appear to be the most fundamental ingredients for collaborative cyber security.

7.1.1 *Trust*

Collaboration requires the exchange of information between participants. This information is often sensitive as it is related to the security of an organization.

High	Medium	Low
1. Poor quality information; 2. Misaligned economic incentives stemming from reputational risks; 3. Poor management;	4. Type of participants; 5. Legal Barriers related to fear of legal or regulatory action; 6. Fear or leaks; 7. Group size; 8. Misaligned economic incentives stemming from group behaviour – externalities; 9. Social barriers from government; 10. Misaligned economic incentives stemming from poor decision-making about investment in security; 11. Norms of rivalry;	12. Legal barriers related to Freedom of Information; 13. Misaligned economic incentives stemming from the costs of participating in IEs; 14. Misaligned economic incentives stemming from competitive markets; 15. Legal barriers related to competition law violations.

Figure 10: Challenges and barriers to information sharing [63]

TRUSTED ENVIRONMENT Participants need a trusted environment in which they can share necessary information without high risks. Feledi et al. [21] states that participants have to be able to trust their peers with whom they share crucial and sensitive information about the state of their information security and their knowledge on the subject.

When exchanging sensitive information a trusted sharing environment is a prerequisite. An organization sharing sensitive information has to trust the other participants not to use the shared information for malicious purposes [6].

TRUSTED PARTICIPANTS Trust plays also an important role in one of the key aspects of collaborative cyber security: the use of information and knowledge of multiple participants [78]. The accuracy of cyber defensive measures can increase when information from multiple participants is correlated. Therefore the participants of a collaboration have to be trustworthy since the strength of cyber defense depends on the information of all participants [90].

7.1.2 *Data privacy*

Exchanging data is of key importance to collaborative cyber security. Disclosure of cyber security related information imposes risks for the organization disclosing it, because it is sensitive information that can be of highly competitive value [88]. The risks of disclosing sensitive

information include malicious parties obtaining the information (either intentional or accidental) [70], and revealing trade secrets [10].

For some organizations privacy issues can be the reason not to collaborate. This may negatively impact the size and diversity of the collaboration [48, 70], while size and diversity are important to collaboration.

TRADE-OFF There is a trade-off between either disclosing information and safeguarding privacy: exchanging unmodified information with all possible details could provide the most benefits to collaboration, yet it also imposes the largest privacy risks. Mitigating these privacy risks often involves measures that involve disclosing less information or modifying information in a way that makes it less privacy-sensitive but also less useful. Organizations have to deal with the trade-off between privacy and information loss [6, 88].

7.1.3 *Additional factors*

Besides data privacy and trust the studied literature makes notice of other factors as well, yet they play a smaller role.

TIME AND EFFORT Bruce and Fink [10] consider time and effort of communicating as one of the main barriers. This is a barrier that can be reduced by automating part of the communication. Automatically sharing information brings up the data privacy barrier, because it is more difficult to control which types of information are shared and which types are kept private.

As time has a direct relation to costs, Gupta and Zhdanov [26] state that substantial start-up costs may outweigh the benefits to join a collaborative cyber security network.

EXPECTING RESULTS Feledi et al. [21] note that part of the motivation to share information is the expectation to receive knowledge of equal value. When this is not happening, the participants are reluctant to share information themselves. The absence of useful information could lead to a vicious circle in which the participants share less and less, thus rendering the collaboration useless.

7.1.4 *Fundamental factors*

The reviewed literature suggests trust and data privacy to be the most fundamental factors for successful collaboration. These two factors are closely related: trust is considered to be a prerequisite for sharing sensitive information and data privacy is a mitigation measure to deal with a sharing environment in which trust has to be created.

The study of Robinson and Disley [63] ends similarly: the major barrier for participating in a collaboration, is that it carries risks for the participating organization's reputation if sensitive information is leaked or disseminated. Robinson and Disley [63] recommend developing trust and ensuring appropriate rules and structures to mitigate this barrier.

7.2 IDENTIFYING CRITICAL SUCCESS FACTORS

From the literature follow four critical success factors to collaborative cyber security. Between these four factors an interplay exists: when one factor changes, it causes the other factors to change as well.

DETAILED DATA The literature shows that organizations like to keep the data they share private because it can contain sensitive information. Yet, it turns out that detailed data is a necessity for the performance of collaborative cyber security: it leads to better threat analysis. It is critical to the success of collaborative cyber security to find ways to share data at the highest level of detail as possible. Therefore this factor is in relation with trust factor: trust between participants allows the elevation of the level of detail.

TRUST The literature explicitly mentions trust. A trusted environment allows participants to share information without high risks, so trust between the participants lowers the barriers to sharing detailed data. As explained in the previous paragraph, this is an enabling factor for sharing of detailed data.

COLLABORATIVE CYBER SECURITY PERFORMANCE Related to trust, is collaborative cyber security performance. When the performance is low, this has a negative effect on trust as participants expect information from the collaboration. When the performance is high, this lowers the risk of the participating organizations. The framework should

perform: participating organizations should at least get something in return for their efforts.

RISK Risk is related to the other factors, as it is directly related to the main goal of collaborative cyber security: lowering risk. When risk increases, it has a negative effect on data detail and trust. It is therefore an important factor, which can be lowered by the proper functioning of collaborative cyber security.

The causalities between the different critical success factors can be seen in figure 11 (page 48).

7.3 CONCLUSION

Returning to the research question: "what are the critical success factors for a collaborative cyber security solution in the retail sector?", this chapter shows there are four factors that are critical to the success of such collaborative cyber security. Additionally this chapter indicates the influence these factors have on each other.

The following four factors are critical for the success of collaborative cyber security.

- High level of data detail;
- trust between participants;
- high collaborative cyber security performance;
- low level of risk.

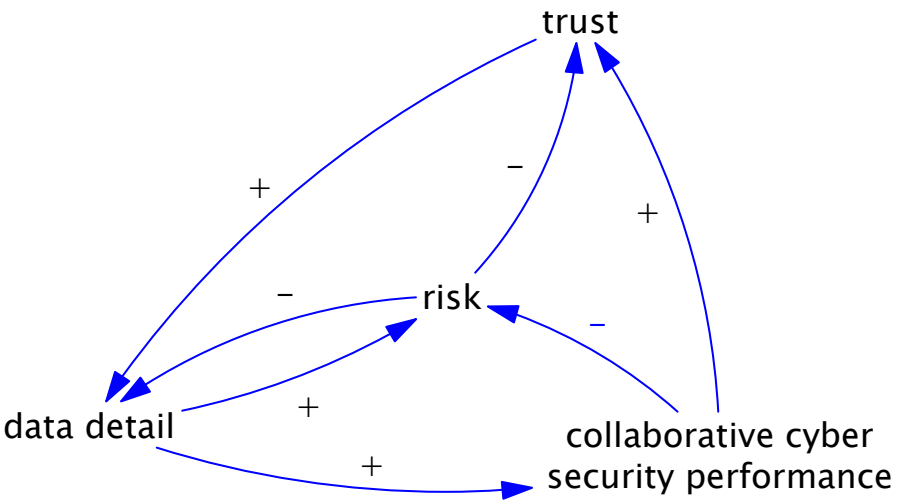

Figure 11: The causalities between different critical success factors

8

FRAMEWORK

The previous chapters capture knowledge about cyber threats relevant for the retail sector, different ways of collaboration and requirements for collaboration. In this chapter it is discussed what would be an appropriate collaboration framework for the retail sector, in order to provide an answer to RQ4.

8.1 TYPE OF FRAMEWORK

To decide which type of framework would be appropriate, the information from RQ1, RQ2 and RQ3 is used.

CYBER THREATS RELEVANT TO RETAIL In chapter 5 the most relevant threat categories to the retail sector can be found. This research shows that *information disclosure* and *denial of service* impose the largest risks, followed by spoofing, tampering, elevation of privilege and repudiation.

Information disclosure and denial of service are the threat categories that are considered to impose the largest risk to retail by both literature and practice, and therefore the focus areas of the framework. This does not imply that collaborative cyber security should only focus on the top threats, but the top threats indicate the areas in which the most results can be achieved.

COLLABORATION TYPES In chapter 6 the collaborative cyber security classification table (table 9) has been created. This classification table can serve as a foundation for recommendations regarding the introduction of collaborative cyber security into an organization.

CRITICAL SUCCESS FACTORS Chapter 7 has identified four critical success factors for collaborative cyber security. These follow below, along with how they should be incorporated into the framework.

- High level of data detail.

The framework shouldn't put any limitations on the amount of detail of the data shared.

- Trust between the participants.

For the framework it is important that it promotes trust rather than that it is a barrier to trust.

- High collaborative cyber security performance.

It is important that the performance of collaborative cyber security is high: participants of the collaboration have to get something in return of their investments in the collaboration.

- Low level of risk.

The goal of the framework is to mitigate cyber threats – and by doing so, reducing cyber risks for an organization – using collaborative cyber security. Using the framework can also *impose* additional risks, because potential sensitive information is shared with participating organizations. If the framework does not reduce risk then it does not meet its goals. It is likely that participants of a collaboration are only willing to invest more resources if the outcomes lead to risk reduction.

8.1.1 *Framework structure*

The retail sector consists of many organizations with their own risk control frameworks and security architectures, such as the major ones described in chapter 4. From the interviews conducted to validate previous parts of this research it was discovered that there are a lot of differences between the cyber security maturity levels in organizations. For the framework that is designed to be effective, it is important that the framework works with these different types of organizations. A flexible framework that provides benefits to any organization regardless of maturity level or used risk control framework and security architecture is needed.

The framework that is developed can be an entirely new framework, or an addition to an existing framework. The barriers for an organization to adopt an addition to the framework that is currently used are expected to be lower than the barriers when replacing the current framework. Replacing an existing framework is likely to require more

resources than extending the current framework. An addition to an existing framework is therefore desirable.

8.1.2 *NIST Cyber Security Framework*

From the frameworks described in chapter 4 the CSF is the most suitable for the purpose indicated in the previous section. CSF enables organizations to apply the principles and best practices of risk management to improving security and resilience of critical infrastructure [57]. The following properties make the CSF the preferred choice.

- Interoperability with other frameworks;
- flexibility;
- completeness.

INTEROPERABILITY WITH OTHER FRAMEWORKS The CSF is designed to *complement* an organization's risk management processes and cyber security program, rather than *replacing* it. The CSF is technology neutral. It offers a flexible and risk-based implementation that can be used with a broad array of existing cyber security risk management processes.

FLEXIBILITY The CSF is flexible in terms of organization size, threat exposure and cyber security sophistication. The great degree of flexibility makes the CSF applicable to use in diverse kinds of organizations. There is a good match between the CSF and the retail sector, as is applicable to the different organizations the retail sector is home to.

COMPLETENESS The CSF combines controls from other standards, making it one of the most complete frameworks for cyber security. For every control in the CSF references to other industry accepted standards such as COBIT 5, NIST SP 800-53 and ISO/IEC 27001:2013 are given.

The CSF covers almost all topics of the ISO/IEC 27001:2013 [58] and NIST SP 800-53, which has a lot of overlap with ISO/IEC 27001:2013 [47]. The CSF incorporates both.

The CSF contains five functions, divided into 22 categories, with a total of 98 subcategories. The functions together provide a high-level,

strategic view of the lifecycle of an organization's management of cyber security risk. The categories are subdivisions of the functions, placed into groups of cyber security outcomes. The subcategories further divide the categories into specific outcomes of technical and/or management activities. Each subcategory contains cyber security activities and processes that are based on global standards: the informative references. [57] Figure 12 provides a diagram of the framework.

The extension of the CSF focuses on the subcategories of the CSF and identifies the subcategories that could potentially benefit from collaborative cyber security.

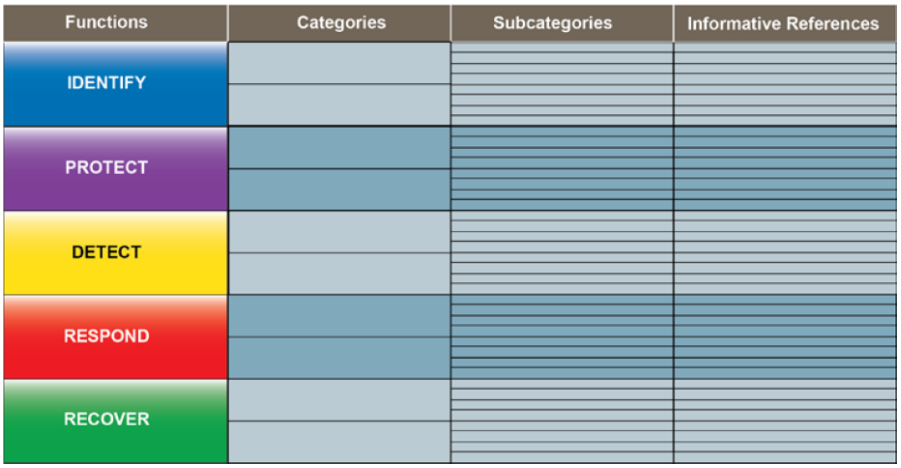

Figure 12: NIST Cyber Security Framework [57]

8.2 CONCLUSION

The organizations in the retail sector differ a lot from each other in terms of size, threat exposure and cyber security sophistication. This chapter explains the need for a framework that is applicable to the organizations in this sector. There's a need for a flexible framework that is able to operate with these organizations, despite all the differences.

The CSF matches this need and is chosen as an appropriate framework for the retail sector. The CSF itself doesn't explicitly include collaboration between organizations, therefore in the next chapter a design for collaboration using the CSF is introduced.

9 COLLABORATION LAYER

In this chapter the so-called "Collaboration Layer" is designed. The Collaboration Layer is an extension of the NIST Cyber Security Framework (CSF), and indicates the focus areas for collaborative cyber security. The focus areas provide an organization directions for locating the appropriate activities for which a collaborative approach is desirable.

9.1 APPROACH

The design starts by studying the CSF's framework core. The framework core consists of functions, categories and subcategories (see fig. 12). The subcategories describe cyber security activities and processes that are commonly found in critical infrastructure sectors.

The subcategories of the framework core are subject to the *collaboration assessment*. For each of the subcategories is determined whether this subcategory could potentially benefit from collaboration. The subcategories that remain after the collaboration assessment are placed in the framework.

The collaboration assessment process contains three assessments: the manual, literature and practice assessments (figure 13).

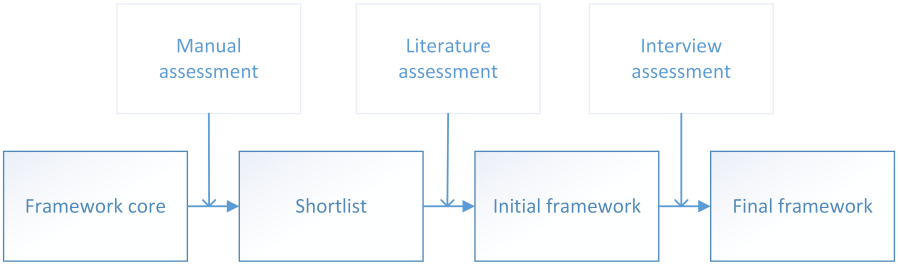

Figure 13: The collaboration assessment

MANUAL ASSESSMENT Not all subcategories of the CSF benefit from collaborative cyber security, therefore each of the subcategories is checked against criteria established later in this chapter. The subcategories that match the criteria are added to a *shortlist*.

Each of the subcategories in the shortlist are used for the literature and practice assessment.

LITERATURE ASSESSMENT The subcategories in the shortlist serve as input for the literature assessment. In the literature assessment it is determined whether collaboration is desirable according to academic literature per subcategory.

By removing the subcategories in which collaboration is not considered to be desirable, an *initial framework* is created. The initial framework contains only the subcategories in which collaboration is considered to be desirable by academic literature.

PRACTICE ASSESSMENT To determine whether collaboration in the subcategories in the initial framework is also considered to be desirable by the practice, experiences from the field are gathered.

By interviewing cyber security experts from the retail sector, their opinions on collaboration in each of the subcategories are collected. The subcategories for which collaboration is not considered to be desirable are be removed from the initial framework, leading to the final framework.

9.2 MANUAL ASSESSMENT

In the manual assessment, first all organization-specific activities are filtered out. Second, the activities that wouldn't benefit from additional knowledge or additional information are filtered out.

The following criteria have been established to identify whether the activities of a subcategory are suitable for collaborative cyber security.

- The activity is not organization-specific.
- The activity could benefit from additional knowledge.
- The activity could benefit from additional information.

This results in a shortlist of 19 subcategories. This shortlist can be found in figure 14.

Functions	Categories	Subcategory	Description
Identify	Risk Assessment	ID.RA-2	Threat and vulnerability information is received from information sharing forums and sources.
		ID.RA-3	Threats, both internal and external, are identified and documented.
Protect	Awareness and Training	PR.AT-1	All users are informed and trained.
		PR.AT-3	Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities.
	Data Security	PR.DS-4	Adequate capacity to ensure availability is maintained.
	Information Protection Processes & Procedures	PR.IP-7	Protection processes are continuously
		PR.IP-8	Effectiveness of protection technologies is shared with appropriate parties.
Detect	Anomalies and Events	DE.AE-2	Detected events are analyzed to understand attack targets and methods.
		DE.AE-3	Event data are aggregated and correlated from multiple sources and sensors.
	Continuous Monitoring	DE.CM-1	The network is monitored to detect potential cybersecurity events.
		DE.CM-2	The physical environment is monitored to detect potential cybersecurity events.
		DE.CM-4	Malicious code is detected.
		DE.CM-6	External service provider activity is monitored to detect potential cybersecurity events.
	Detection Processes	DE.DP-4	Event detection information is communicated to appropriate parties.
		DE.DP-5	Detection processes are continuously improved.
Respond	Communications	RS.CO-3	Information is shared consistent with response plans.
		RS.CO-4	Coordination with stakeholders occurs consistent with response plans.
		RS.CO-5	Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.
Recover	Communications	RC.CO-3	Recovery activities are communicated to internal stakeholders and executive and management teams.

Figure 14: Shortlist

9.3 LITERATURE ASSESSMENT

The 19 subcategories that are in the shortlist of figure 14 are compared with existing academic literature. In academic literature a lot can be found about collaboration, and there is a clear relation between literature and most of the subcategories from the CSF.

9.3.1 *Main findings*

DETECTION OF ATTACKS THAT OCCUR IN MULTIPLE SYSTEMS Subcategory ID.RA-2 is suggesting that threat and vulnerability information is received from information sharing forums and sources. Literature suggests that some threats can only be detected because they occur in multiple networks simultaneously. They can only be detected if organizations – in addition to receive – share threat and vulnerability information in order to make detection of such threats possible. [90, 89]

REINVENTING THE WHEEL According to the literature a main advantage of collaboration is reusing knowledge. A solution to a certain threat that is already developed at organization A can help organization B which doesn't have to develop the solution all over again: it eliminates the duplication of work [53]. Additonally, knowledge outside the own organization can be used to develop better solutions in collaboration with other organizations. For the framework the exchange of knowledge is beneficial to the improvement of protection processes (PR.IP-7) and the detection of malicious code (DE.CM-4).

DATA QUALITY The literature suggests that data quality improves when data is correlated from multiple organizations. This leads to a more effective response [88], can be used to make more refined tools [70]. This is especially useful in the detection function of the CSF (DE.AE-2, DE.AE-3, and DE.CM-1).

COMPLEXITY OF PHYSICAL DATA Exchanging information about physical security is not recommended by the literature. Phillips et al. [61] state exchanging this type of information can dramatically complicate controlling physical access (DE.CM-2).

9.3.2 *Initial framework*

The results of the literature assessment are summarized in the literature column of table 10 on page 58, where a plus symbol (+) indicates collaboration is desirable and a minus symbol (–) indicates collaboration is not desirable. The main findings are described below and detailed findings can be found per subcategory in appendix A (page 85).

It turns out that the academic literature does not support DE.CM-2 (*The physical environment is monitored to detect potential cyber security events*), yet it is still interesting to see the results for this subcategory in the practice assessment. Therefore this subcategory stays in the initial framework, yet with a negative recommendation from literature.

9.4 PRACTICE ASSESSMENT

The remaining subcategories in the initial framework are validated through interviews with experts. The interviewees – who wish to remain anonymous – are c-level [1] cyber security experts from large retail organizations employing significant activities in the Netherlands. An overview of the interviewees is provided in appendix B.2.

The opinions of the interviewees are summarized in the *practice* column of table 10. The plus (+), box (□) and minus (–) respectively correspond to the positive, moderate and negative groups that are explained below.

- Positive: all the interviewees consider a collaborative approach desirable for this subcategory.
- Moderate: the majority of the interviewees consider a collaborative approach desirable for this subcategory.
- Negative: the majority or all of the interviewees do not consider a collaborative approach to this subcategory desirable.

The practice assessment has identified for each of the subcategories whether collaboration is desirable according to the interviewees. Seven subcategories can be marked as 'positive', eight are marked as 'moderate' and the remaining three subcategories are marked 'negative'.

In both the positive and negative groups, the participants were unanimous about whether collaboration is desirable or whether it is not. Yet, the subcategories that are marked 'moderate' (□) in table 10 allow some discussion about whether they should be included in the final framework.

The main findings are described below, detailed findings about the interviews can be found in appendix A.

1 C-level refers to the highest-level executives in senior management, of which the title often starts with 'chief'.

Table 10: Results of the literature and practice assessments

Subcategory	Literature	Practice	Subcategory	Literature	Practice
ID.RA-2	+	+	DE.CM-2	–	–
ID.RA-3	+	□	DE.CM-4	+	+
PR.AT-1	+	□	DE.CM-6	+	□
PR.AT-3	+	–	DE.DP-4	+	+
PR.DS-4	+	–	DE.DP-5	+	+
PR.IP-7	+	+	RS.CO-3	+	□
PR.IP-8	+	□	RS.CO-4	+	+
DE.AE-2	+	□	RS.CO-5	+	+
DE.AE-3	+	□	RC.CO-3	+	–
DE.CM-1	+	□			

9.4.1 *Main findings*

LIMITED SHARING The practice assessment reveals that organizations do consider that collaboration has potential benefits to cyber security, yet they are reluctant to share information because it is considered sensitive. They are especially reluctant when it comes to information that comes from inside the organization (i.e. internal network traffic). The barrier to sharing is lower when it comes to sharing information that originates from outside the organization. If information is shared, it should be information from attacks coming from outside the organization, which is considered not to be sensitive.

THE NEED FOR A FORUM From the practice assessment it also turns out that organizations do not collaborate because there haven't been efforts to start collaborating. The interviewees indicate they would be interested in joining a forum for facilitating the exchange of information and knowledge amongst trusted participants. They would join an existing forum rather than starting one.

INTERNAL DEVELOPMENT From the practice assessment it turned out that organizations first want to bring their detection processes within their organizations to an adequate level before considering collaboration. In the first place, the organization should be able to defend itself, collaboration is considered beneficial and can be the next step (DE.AE-2, DE.AE-3).

THREATS NOT SERIOUS ENOUGH The interviewees consider the threats they face not serious enough to take additional measures on top of the measures they already take. Still, the interviewees are positive about collaborative cyber security and they consider collaboration an additional measure when necessary.

9.5 FINAL FRAMEWORK

The subcategories from table 10 to which collaboration is considered to be desirable for both literature and practice (marked with a + twice) are placed into the final framework. The opposite applies to the subcategories marked with a – twice. Whether the other subcategories are included into the final framework is discussed hereafter.

9.5.1 *Discussion*

In this section the remaining subcategories are discussed. The discussion is based on literature and practice findings, which can be found appendix A.

ID.RA-3: THREATS, BOTH INTERNAL AND EXTERNAL, ARE IDENTIFIED AND DOCUMENTED Collaboration in this subcategory is considered to be beneficial according to literature and moderately by practice. The main issue the practice has with collaboration in this subcategory is that the interviewed organizations are reluctant to share internal documentation as these are considered sensitive. Additionally, an interviewee tells threats aren't documented in his organization.

Although the the exchange of documentation of internal threats might be out of the question at first, the exchange of documentation of external threats is still valuable. In case threats aren't documented yet, this is something that can still be done in the future.

Although there are some barriers, collaboration in this subcategory still has benefits: it is included in the final framework.

PR.AT-1: ALL USERS ARE INFORMED AND TRAINED A limitation from the practice in this area is that training is considered to be specific. Collaboration would be difficult as there are too much differences between the collaborating organizations. It is suggested though,

that it could be beneficial to collaborate in the case the trainings split up into a common part and a company-specific part.

Although the interviewees weren't unanimously positive about this subcategory, collaboration could still offer benefits to organizations. Therefore, this subcategory is considered to be desirable and it is included in the final framework.

PR.AT-3: THIRD-PARTY STAKEHOLDERS (E.G., SUPPLIERS, CUSTOMERS, PARTNERS) UNDERSTAND ROLES & RESPONSIBILITIES Although the literature suggests organizations could benefit of economies of scale by collaborating on the training of third-party stakeholders. The practice doesn't agree: it is the responsibility of the third-party stakeholders to make sure their roles and responsibilities are arranged.

The difference between the literature and practice is mainly related to the type of collaboration that is suggested. The literature aims at benefits because trainings are organized in a more efficient way when collaborating. In practice this is not the case: the retail organizations do currently not invest in trainings for third-party stakeholders: it would be less beneficial and not desired to take responsibility for these tasks as a retail organization. Therefore this subcategory does not take place in the final framework.

PR.DS-4: ADEQUATE CAPACITY TO ENSURE AVAILABILITY IS MAINTAINED Literature suggests to collaborate in order to save costly computational resources by sharing intrusion detection resources. The view from the practice on this is that it would most likely involve the integration of IT systems across organizations. The practice considers this rather a risk than a benefit. Also, with current technologies as cloud computing, availability is not much of an issue. The risks of collaborating would outweigh the benefits: this subcategory does not take place in the final framework.

PR.IP-8: EFFECTIVENESS OF PROTECTION TECHNOLOGIES IS SHARED WITH APPROPRIATE PARTIES The literature adds that effectiveness of protection technologies should be shared within the group of organizations that are collaborating. The practice does not expect big benefits from collaboration in this area: news about a certain technology not working travels fast. Sharing how technology can be applied and what the added value is could be more useful.

The practice appears to have ideas about this subcategory, yet the ideas are going beyond the purpose of this subcategory. These ideas

can find their place in other subcategories such as ID.RA-2 rather than this subcategory. Therefore this subcategory is not part of the final framework.

DE.AE-2: DETECTED EVENTS ARE ANALYZED TO UNDERSTAND ATTACK TARGETS AND METHODS The literature is very positive about collaboration in this subcategory as it can result in better analysis. The practice agrees but places one important remark: organizations should in the first place be able to analyze events and to understand attacks independent of other organizations. Collaboration can be a valuable addition.

With the practical remark in mind, this subcategory can be added to the final framework as it is considered to have benefits a collaborative approach is used.

DE.AE-3: EVENT DATA ARE AGGREGATED AND CORRELATED FROM MULTIPLE SOURCES AND SENSORS In line with the previous subcategory (DE.AE-2) the literature and practice both agree on the benefits of collaborating on this subcategory. The interviewees indicate that this subcategory demands more intensive collaboration than the previous one. It is more intensive because collaboration in this subcategory would require collecting large amounts of data from different organizations, where in DE.AE-2 smaller parts would be exchanged.

The practice states that this could be beneficial, although it would require serious cyber threats before they would engage in such intensive collaboration. This subcategory therefore is a valuable addition to the final framework and is incorporated.

DE.CM-1: THE NETWORK IS MONITORED TO DETECT POTENTIAL CYBER SECURITY EVENTS Collaboration is considered to be desired by literature as detection of events can improve. The practice in some cases seems to be reluctant to share internal information and would like to share only external data. Additionally one interviewee mentions that they already exchange information about the detection with vendors of the network monitoring and detection software in order to improve the software.

Although some organizations may prefer to only exchange less sensitive external data, this data could still be of value and in a later stage it could be decided to also include (a subset of) internal data. Despite vendors taking this role, collaboration on this subcategory could definitely be valuable and should be considered. This subcategory is incorporated into the final framework.

DE.CM-2: THE PHYSICAL ENVIRONMENT IS MONITORED TO DETECT POTENTIAL CYBER SECURITY EVENTS The literature does not consider this to be desirable: a collaborative approach complicates physical access control dramatically. The practice adds that their environments are too specific to share specific information about it. Additionally privacy-related issues could arise. As both literature and practice do not show support for this subcategory, it is not incorporated into the final framework.

DE.CM-6: EXTERNAL SERVICE PROVIDER ACTIVITY IS MONITORED TO DETECT POTENTIAL CYBER SECURITY EVENTS The practice thinks it could be advantageous to check common external service providers for compliancy but there are some barriers. Sharing specific information about external service providers could e.g. lead to legal disputes. Letting other organizations perform compliancy checks at external service providers could also puts up a barrier: who is responsible for the quality and in case something goes wrong. Literature related to this subcategory takes a different direction: organizations can benefit from collaborating if this is about cyber threats that reside at the systems of external service providers.

This subcategory imposes serious barriers while it is not clear whether it could beneficial in the retail sector. There's also a gap between what literature and practice say about this subcategory. Therefore this subcategory is not incorporated in the final framework.

RS.CO-3: INFORMATION IS SHARED CONSISTENT WITH RESPONSE PLANS The literature states that response plans can be improved by incorporating information from external sources. In the practice assessment it turned out that the practice thinks it is desirable to incorporate the sharing of information with collaborating organizations in the response plans, although the added value might be low. It is suggested that sharing should be done at the evaluation stage, or earlier in case other organizations are put at risk.

Although the added value might be low, this subcategory can still be of value and assist in making better response plans. Therefore it is placed in the final framework.

RC.CO-3: RECOVERY ACTIVITIES ARE COMMUNICATED TO INTERNAL STAKEHOLDERS AND EXECUTIVES AND MANAGEMENT TEAMS The literature states that the evaluation of the response effectiveness is required to be shared. The main issues for the practice involve the disclosure of recovery activities: why should they disclose informa-

tion if the effects of a cyber attack remained invisible to the outside world.

To overcome the issues found in the practice, organizations could decide to disclose only the evaluation of recovery activities to partner organizations that are trusted. This lowers the barrier to share and could be beneficial. Therefore this subcategory is placed in the final framework.

The remaining 14 subcategories make up the final framework (see figure 15).

Functions	Categories	Subcategory	Description
Identify	Risk Assessment	ID.RA-2	Threat and vulnerability information is received from information sharing forums and sources.
		ID.RA-3	Threats, both internal and external, are identified and documented.
Protect	Awareness and Training	PR.AT-1	All users are informed and trained.
	Information Protection Processes & Procedures	PR.IP-7	Protection processes are continuously improved.
Detect	Anomalies and Events	DE.AE-2	Detected events are analyzed to understand attack targets and methods.
		DE.AE-3	Event data are aggregated and correlated from multiple sources and sensors.
	Continuous Monitoring	DE.CM-1	The network is monitored to detect potential cybersecurity events.
		DE.CM-4	Malicious code is detected.
	Detection Processes	DE.DP-4	Event detection information is communicated to appropriate parties.
		DE.DP-5	Detection processes are continuously improved.
Respond	Communications	RS.CO-3	Information is shared consistent with response plans.
		RS.CO-4	Coordination with stakeholders occurs consistent with response plans.
		RS.CO-5	Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.
Recover	Communications	RC.CO-3	Recovery activities are communicated to internal stakeholders and executive and management teams.

Figure 15: Final framework

9.6 CONCLUSION

Throughout this chapter the subcategories of the CSF were assessed. The subcategories for which a collaborative approach is desirable were identified and placed in a shortlist, an initial and a final frame-

work. The final framework contains the focus areas for collaborative cyber security, which make up the vital parts of the Collaboration Layer.

The Collaboration Layer complements the CSF and indicates in which areas an organization should consider collaborating with other organizations in order to improve cyber security.

The final result is depicted in figure 16: the CSF and the Collaboration Layer. The CSF is at the core, surrounded with its five functions. Surrounding the functions is the Collaboration Layer, with the subcategories of the collaboration layer listed per function.

Risk Assessment	
ID.RA-2	Threat and vulnerability information is received from information sharing forums and sources.
ID.RA-3	Threats, both internal and external, are identified and documented.

Communications	
RC.CO-3	Recovery activities are communicated to internal stakeholders and executive and management teams.

Communications	
RS.CO-3	Information is shared consistent with response plans.
RS.CO-4	Coordination with stakeholders occurs consistent with response plans.
RS.CO-5	Voluntary information sharing occurs with external stakeholders to achieve broader cyber security situational awareness.

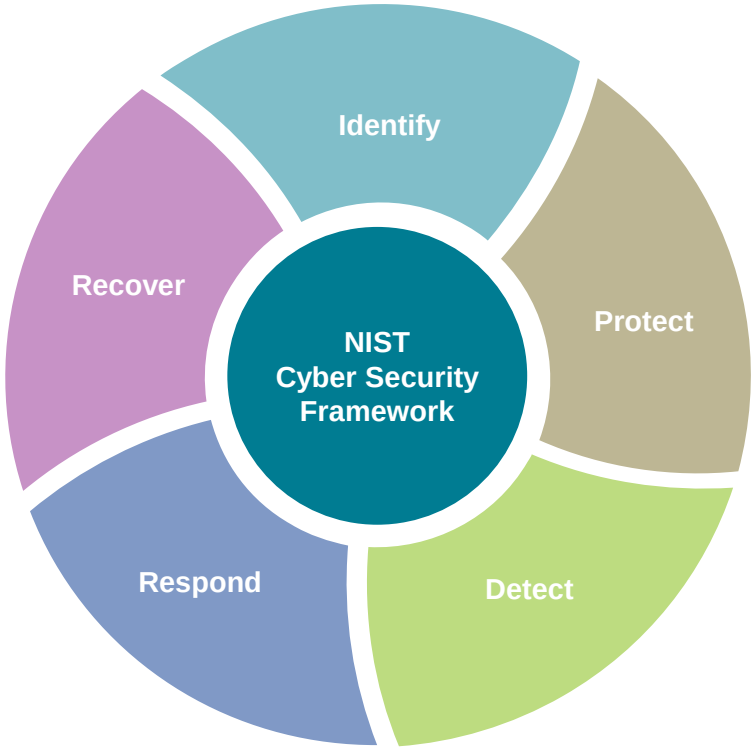

Figure 16: Collaboration Layer

Awareness and Training	
PR.AT-1	All users are informed and trained.
Information Protection Processes & Procedures	
PR.IP-7	Protection processes are continuously improved.

Anomalies and Events	
DE.AE-2	Detected events are analysed to understand attack targets and methods.
DE.AE-3	Event data are aggregated and correlated from multiple sources and sensors.
Continuous Monitoring	
DE.CM-1	The network is monitored to detect potential cyber security events.
DE.CM-4	Malicious code is detected.
Detection Processes	
DE.DP-4	Event detection information is communicated to appropriate parties.
DE.DP-5	Detection processes are continuously improved.

10

APPLICABILITY

In the previous chapter, the collaboration layer (figure 16) is designed. To answer the main research question – *how can collaborative cyber security be used to mitigate cyber threats in retail organizations* – it is necessary to explain how the collaboration layer is used in order to mitigate cyber threats in retail organizations.

How the collaborative layer can be used is explained by providing recommendations on the type of collaborative cyber security that is suitable for the retail sector (section 10.1). The classification table (table 9) that is developed in chapter 6 is used as a guideline. Per attribute recommendations follow based on findings throughout this research.

Recommendations for the implementation collaborative cyber security follow in section 10.2. Per function of the CSF possibilities are described.

How the main threats to the retail sector, given in chapter 5, can be mitigated is explained in 10.3, and the last part of this chapter reports on the state of affairs regarding collaborative cyber security in the retail sector in the Netherlands.

10.1 RECOMMENDATIONS FOR CREATING A COLLABORATION

Using the classification table (table 9) recommendations regarding the integration of collaborative cyber security can be done. Per attribute is discussed what is desirable for collaborative cyber security in the retail sector.

10.1.1 *Type of collaboration*

Table 9 suggests two options for this attribute: manual and automatic sharing. The functioning of the Collaboration Layer does not rely on whether threats are automatically shared amongst the participants or whether this is done manually. Between the lines of the interviews can be read that the interviewees are reluctant to share data because it can

contain sensitive information. Sharing data automatically gives an organization less control over the data that is shared so *manual sharing* is preferred initially, until a certain degree of trust is created between the participants. With enough trust, automatic sharing can be the next step. Using automatic sharing information can be spread across multiple organizations much faster, allowing for faster response to emergency situations.

10.1.2 *Ownership*

The ownership attribute defines who owns the collaboration and makes the decisions. Two described options are shared ownership and third-party ownership. From the practice findings in section 9.4.1 it turns out organizations in the retail sector are interested in joining an existing forum for sharing information and knowledge. Starting a new forum is considered to be time and resource consuming: this excludes "shared ownership", as this requires one of organizations to take the initiative. It is recommended a third-party leads the establishment of a collaboration forum for the retail sector.

10.1.3 *Architecture*

Decisions about the architecture of collaborative cyber security are mostly related to the way information is exchanged. In the case of manual collaboration existing communication channels such as email are suitable and should be used as they are already existing. In the case information is exchanged automatically, the architecture needs to provide a structure to support the automatic exchange of information.

Since manual sharing is suggested as first type of sharing for collaboration in the retail sector, existing communication channels are suggested to be used.

When automatic sharing is considered, a distributed architecture is suggested: the interviewees say that in the first place they want to be able to defend themselves (section 9.4.1). In a distributed architecture an organization stays in charge of its own processes, in contrast to a centralized architecture that provides a shared processing platform to the participants.

10.1.4 *Collaborating parties*

The classification defines horizontal, vertical and open collaboration. The Collaboration Layer focuses on exchanging information that could be usable by other organizations that face similar situations. It is beneficial when the collaborating organizations have many similarities, so information about similar aspects can easily be exchanged. Organizations that perform the same role in the same sector show much similarities as their activities are equivalent. Horizontal collaboration focuses on obtaining the benefits from the similarities across collaborating organizations, therefore horizontal collaboration is recommended.

10.1.5 *Type of data shared*

The collaborative layer is not limited to just sharing data but also other resources such as efforts to develop trainings for users (subcategory PR.AT-1).

The types of data that are shared in accordance with the Collaboration Layer are as follows:

- Threat and vulnerability information (ID.RA-2)
- Event data (DE.AE-2, DE.AE-3, DE.DP-4)
- (Network) security logs (DE.CM-1, DE.CM-4)

A recommendation for sharing data is the introduction of an standardized format: this gives all participants a clear understanding of threat information and reduces misinterpretations (section 6.3, [3]).

10.2 RECOMMENDATIONS PER NIST FUNCTION

The NIST Cyber Security Framework (CSF) consists of five functions to which the subcategories in the Collaboration Layer belong. Below recommendations per function are given.

10.2.1 *Identify*

The identify function contains the necessary activities to develop and implement appropriate safeguards to ensure the delivery of the organization's core business.

The Collaboration Layer in this function consists of ID.RA-2 and ID.RA-3, both in the Risk Assessment category. ID.RA-2 describes receiving threat and vulnerability information from information sharing forums and sources. A collaborative approach includes in addition to *obtaining* information from forums and other sources the *adding* information.

ID.RA-3 describes the documentation of identified threats. Different organizations that face the same threats can benefit from threat documentation from an organization that has faced the threat already, and vice versa. This can speed up the process of finding a solution: existing documentation can aid in the process of developing a solution.

10.2.2 *Protect*

The protection function involves the implementation of appropriate safeguards to ensure the delivery of the organization's core business.

Collaboration is suggested in PR.AT-1 and PR.IP-7, respectively part of Awareness & Training and Information Protection Processes & Procedures categories.

PR.AT-1 involves the informing and training of users. Collaborating offers potential benefits for organizations because they can develop security awareness trainings together. An example is the development of e-learning courses for check-out operators. Because the activities performed by check-out operators are very similar across different organizations, an e-learning course could be developed for multiple retail organizations, lowering the costs of development per organization.

PR.IP-7 concerns the continuous improvement of protection processes. Looking at incidents that have occurred at other organizations can be of use to the improvement of these processes. They can learn from incidents that haven't occurred yet but could impose risks in the future.

10.2.3 *Detect*

Collaboration has a lot to offer for the detect function, as it covers six of the fourteen subcategories in the Collaboration Layer. The categories of Anomalies & Events, Security Continuous Monitoring and Detection Processes are covered.

In the Anomalies & Events DE.AE-2 and DE.AE-3 are part of the Collaboration Layer. A collaborative approach to these subcategories would involve the sharing of detected events and anomalies with collaborating organizations and obtaining detected events and anomalies in return (DE.AE-2). Event data obtained within the organization can be enriched with event data obtained from other organizations (DE.AE-3).

The Security Continuous Monitoring category can benefit from the exchange of network event detection information. Network monitoring activities can be improved by including detection patterns of incidents that have previously occurred at other organizations (DE.CM-1) and the same concerns the detection of malware (DE.CM-4).

Collaborative cyber security has potential benefits for the category of Detection Processes. DE.DP-4 describes communicating event detection information, which can be shared with other organizations in order to solve similar vulnerabilities quickly.

DE.DP-5 describes continuous improvement of detection processes. To support improvement processes, organizations can learn from incidents that occurred at other organizations and vice versa.

10.2.4 *Respond*

The Respond function contains the appropriate activities that are developed and implemented in order to take action regarding a detected cyber security event.

RS.CO-3 and RS.CO-4 are part of the Communications category and contain information about the response plan. They respectively consider information sharing and coordination with stakeholders. Collaboration in these two subcategories involves disclosing information about the measures that are taken in response to a cyber incident. This increases situational awareness, as suggested by RS.CO-5.

10.2.5 *Recover*

The Recover function is about developing and implementing the appropriate activities to maintain plans for resilience and to restore capabilities or services that were impaired due to a cyber security event.

The recovery activities are communicated to internal stakeholders, executives and management teams. Collaboration can be of use to create situational awareness by communicating how recovery activities take place and how successful the recovery activities are.

10.3 MITIGATING THE MAIN THREATS USING COLLABORATIVE CYBER SECURITY

The Collaborative Layer provides a number of areas to which collaboration is beneficial for cyber security. The main threats to retail organizations in the Netherlands are information disclosure and denial of service, as explained in chapter 5.

The Collaborative Layer can be used to successfully mitigate these threats by improving identification, protection and detection activities.

Threats related to denial of service are mitigated by taking measures that are beneficial to availability. With more information and knowledge about threats available from collaborating organizations, threats to availability impose less risk as better treatments are available. Collaborative measures to this threat are mainly found in the identify and detection functions.

The same holds for information disclosure: when protection of digital assets improved by the availability of knowledge and information from other organizations the risk lowers. Additionally information disclosure benefits from the protection function, in which awareness & training takes an important place.

11

CONCLUSION

The retail sector has been the subject of many cyber attacks in the past several years. Both the frequency and impact of incidents have increased, with financial and reputational damage as effect. The impact of cyber attacks is not limited to retail organizations: the retail sector is part of the critical infrastructure and considered to be of national importance. This means that consumers can and will be affected as they rely on retail organizations for their vital necessities.

To mitigate the impact of cyber attacks in the retail sector, this research introduced collaborative cyber security as a mitigation measure. The main task of collaboration is to facilitate the exchange of knowledge and information. By exchanging knowledge and information, organizations can obtain knowledge and information beyond the boundaries of their own organizations. The exchange of knowledge and information can be beneficial to cyber security activities because a solution to a threat has to be developed only once. This saves organizations from developing the same solutions.

To integrate collaborative cyber security into cyber security processes and activities of an organization, this research introduces the Collaborative Layer. The Collaborative Layer has identified focus areas for collaborative cyber security activities through a literature study and practice validation. It is an extension of the NIST Cyber Security Framework, which is known for its flexibility. The Collaborative Layer on top of the NIST Cyber Security Framework enables organizations regardless of size, degree of cyber security risk or cyber security sophistication to integrate collaboration into their cyber security program or can be used to establish a new cyber security program.

Two important barriers for the implementation of the Collaborative Layer are identified. Collaborative cyber security is not possible without exchanging information. Whether the information is useful, depends on the level of detail. The first barrier is the reluctance to share detailed information. Sharing detailed data involves a risk as detailed data can be sensitive. To overcome this barrier and to make collaborative cyber security possible, trust between participants is the key.

The second barrier are the difficulties of bootstrapping a collaboration. The organizations interviewed in this research are in general very

positive about collaboration, yet they are not willing to do the initial investment of starting a collaboration. This barrier can be overcome, i.e. by allowing a third party to start a forum to bring the participating organizations together. At the moment of writing, the outcomes of this research have resulted in taking the first steps towards the establishment of such a forum.

Organizations in the retail sector can successfully mitigate the cyber threats by engaging in business-to-business collaboration in the activities and processes specified by the Collaboration Layer. Using the Collaboration Layer is the first step into the direction of collaborative cyber security.

11.1 LIMITATIONS AND SUGGESTIONS FOR FURTHER RESEARCH

To this research and the results are some limitations and suggestions for further research. These are discussed below.

IMPLEMENTATION OF THE COLLABORATION LAYER Chapter 10 gives recommendations about the implementation of the Collaboration Layer. Yet, the Collaboration Layer still remains an abstract indication of the areas that offer the opportunity to collaborate. A research opportunity is to identify how the Collaboration Layer should be implemented and to develop a pragmatic guide for the implementation.

RESEARCH BIAS The findings described in this research are the results of an extensive literature research in combination with practice validation. A limitation to this research is the research bias. The located literature is often positive about collaboration in cyber security. This is a relatively new research area and research criticizing the existing research has yet to come.

REPRESENTATIVITY This research focuses on the retail sector in the Netherlands, but is largely validated in a niche of this sector: supermarket organizations. Whether this research is representative for the whole retail sector depends on whether this niche is representative for the whole retail sector in the Netherlands and whether retail in the Netherlands is representative for the global retail sector.

The validation results suggest the research to be representative for the retail sector in the Netherlands: validation outside the supermarket niche shows very similar results. Whether the results are representa-

tive for the global retail sector is doubtful: cyber threats in the Netherlands differ a lot from the ones in the United States as can be seen from table 2 and table 3. Looking at table 2 it is hard to imagine that a cyber security expert would consider threats in the retail sector "not to be serious enough", as the interviewees in this research perceive cyber threats (ch. 9).

It is likely that the results from this research are representative for the entire retail sector in the Netherlands. Future research could focus on the global reproducibility of this research.

LEGAL AND REGULATORY COMPLIANCE A suggestion for future research is the in the legal area. The exchange of information between organizations could at some point show legal conflicts. Privacy laws for example, could put additional requirements on the exchange of different types of data, especially when related customers or employees. It is suggested that it is researched which types of data could cause conflicts on legal and regulatory level.

DATA DETAILS A major barrier for organizations is sharing detailed data. Yet, detailed data is very important for the success of collaboration. There are existing techniques to anonymize data without losing useful content, which could find its way into exchange of information in the retail sector. It is suggested to conduct research in order to find a suitable solution for sharing detailed data in an anonymized fashion within the retail sector.

BIBLIOGRAPHY

[1] Interview with a cyber security expert in the retail sector. Personal communication, August 2014.

[2] Interview with an independent cyber security expert in the retail sector. Personal communication, August 2014.

[3] Interview with a cyber security expert in the oil & gas sector. Personal communication, June 2014.

[4] Interview with a cyber security expert in the retail sector. Personal communication, August 2014.

[5] Interview with a cyber security expert in the retail sector. Personal communication, August 2014.

[6] H. Bahsi and A. Levi. Preserving organizational privacy in intrusion detection log sharing. In *3rd International Conference on Cyber Conflict, ICCC 2011 - Proceedings*, Tallinn, Estonia, 2011.

[7] BBC News. Kmart shops hit by payment card hack attack. http://www.bbc.com/news/technology-29595214, October 2014.

[8] BBC News. Wm Morrison supermarket suffers payroll data theft. http://www.bbc.com/news/business-26574161, March 2014.

[9] British Retail Consortium. Retail Crime Survey 2013. Technical report, 2013.

[10] J. Bruce and G. Fink. Shopping for danger e-commerce techniques applied to collaboration in cyber security. In *Proceedings of the 2012 International Conference on Collaboration Technologies and Systems, CTS 2012*, pages 251–258, Denver, CO, United States, 2012. ISBN 9781467313827.

[11] O. Bruno. Datalek: gegevens Baby-dump op straat. https://www.bof.nl/2012/02/17/datalek-gegevens-klanten-baby-dump-op-straat/, February 2012.

[12] J. Cebula and L. Young. A taxonomy of operational cyber security risks. Technical Report December, Software Engineering Institute, 2010.

[13] K.-K. R. Choo. The cyber threat landscape: Challenges and future research directions. *Computers & Security*, 30(8):719–731, Nov. 2011. ISSN 01674048.

[14] M. Choras. Comprehensive Approach To Information Sharing for Increased Network Security and Survivability. *Cybernetics and Systems*, 44(6-7):550–568, Oct. 2013. ISSN 0196-9722.

[15] J. Christ. Web Based Attacks. Technical report, SANS Institute, 2007.

[16] M. Clinch. Now UK supermarket falls victim to hacking attack. http://www.cnbc.com/id/101417191, February 2014.

[17] A. Das. Data Breach and Privacy Update. Technical report, Wilson Elser, Chicago, 2013.

[18] P. Desai, A. Potia, and B. Salsberg. Retail 4.0: The future of retail grocery in a digital world. http://csi.mckinsey.com/knowledge_by_region/global/future_of_retail_grocery_in_a_digital_world, 2013.

[19] M. Erich. ING Food 2030. https://www.ing.nl/zakelijk/ing-economisch-bureau/sectoren/2012/06/20120626_Food_2030.aspx, June 2012.

[20] D. Feledi and S. Fenz. Challenges of Web-based Information Security Knowledge Sharing. In *2012 Seventh International Conference on Availability, Reliability and Security (ARES)*, pages 514–521, Prague, Czech Republic, 2012.

[21] D. Feledi, S. Fenz, and L. Lechner. Toward web-based information security knowledge sharing. *Information Security Technical Report*, 17(4):199–209, 2013.

[22] Financial Services ISAC. About FS-ISAC. https://www.fsisac.com/about, August 2014.

[23] FTSE International Limited. Industry structure and definitions. http://www.icbenchmark.com/ICBDocs/Structure_Defs_English.pdf, 2012.

[24] C. Fung and R. Boutaba. *Cooperation in Intrusion Detection Networks*. John Wiley & Sons, 2011.

[25] J. R. Goodall, W. G. Lutters, and A. Komlodi. I know my network: Collaboration and expertise in intrusion detection. In *Computer Supported Cooperative Work - Conference Proceedings, CSCW 2004*, pages 342–345, Chicago, IL; United States, 2004.

[26] A. Gupta and D. Zhdanov. Growth and Sustainability of Managed Security Services Networks: An Economic Perspective. *MIS Quarterly*, 36(4):1109–1130, 2012.

[27] M. Hafner, M. Memon, and R. Breu. Security as a Service - A Reference Architecture for SOA Security. *Journal of Universal Computer Science*, 15(15):2916–2936, 2009.

[28] G. Hamel, Y. Doz, and C. Prahalad. Collaborate with your competitors and win. *Harvard business review*, 67(1):133–139, 1989.

[29] J. Hernandez-Ardieta. Information sharing models for cooperative cyber defence. In *Cyber Conflict (CyCon), 2013 5th International Conference on*, Tallinn, Estonia, 2013.

[30] J. Howard and T. Longstaff. A common language for computer security incidents. *Sandia National Laboratories*, (October), 1998.

[31] C. Huang, R. Behara, and Q. Hu. Managing risk propagation in extended enterprise networks. *IT professional*, (August), 2008.

[32] D. Icove, K. Seger, and W. VonStorch. *Computer crime: a crimefighter's handbook*. O'Reilly & Associates, Sebastopol, CA, 1995.

[33] Instituut Fysieke Veiligheid. 2e inhoudelijke analyse van bescherming vitale infrastructuur. http://www.infopuntveiligheid.nl/Publicatie/DossierItem/10/712/2e-inhoudelijke-analyse-van-bescherming-vitale-infrastructuur.html, November 2009.

[34] Instituut Fysieke Veiligheid. Vitale infrastructuur. http://www.infopuntveiligheid.nl/Publicatie/Dossier/10/vitale-infrastructuur.html, June 2014.

[35] International Organization for Standardization. ISO/IEC 27002:2013. 2013.

[36] International Telecommunications Union. Definition of cybersecurity. http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx, June 2014.

[37] S. Jayson. 2013 Cost of Cyber Crime Study: Global Report. Technical Report October, Ponemon Institute, 2013.

[38] C. Jeffries. Threat modeling and agile development practices. http://technet.microsoft.com/en-us/security/hh855044.aspx, February 2012.

[39] W. Jiang. Survey of Network and Computer Attack Taxonomy. In *Robotics and Applications (ISRA), 2012 IEEE Symposium on*, pages 294–297, Kuala Lumpur, Malaysia, 2012. IEEE. ISBN 9781467322072.

[40] X. Jiang, Wei; Tian, Zhi-hong; Cui. DMAT: A New Network and Computer Attack Classification. *Journal of Engineering Science and Technology Review*, 6(5):101–106, 2013.

[41] Kaspersky lab. Global corporate it security risks: 2013. http://media.kaspersky.com/en/business-security/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf, May 2013.

[42] Kaspersky Lab. Global Corporate IT Security Risks: 2013. Technical Report May, 2013.

[43] R. Klump and M. Kwiatkowski. Distributed IP watchlist generation for intrusion detection in the electrical smart grid. In *Critical Infrastructure Protection IV*, pages 113–126. Springer, 2010.

[44] B. Krebs. Dairy Queen Confirms Breach at 395 Stores. http://krebsonsecurity.com/2014/10/dairy-queen-confirms-breach-at-395-stores/, October 2014.

[45] B. Krebs. Home Depot: 56M Cards Impacted, Malware Contained. http://krebsonsecurity.com/2014/09/home-depot-56m-cards-impacted-malware-contained/, September 2014.

[46] B. Krebs. Email attack on vendor set up breach at target. http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/, Feb 2014.

[47] C. Kuligowski. *Comparison of IT Security Standards*. PhD thesis, 2009.

[48] P. Lincoln, P. Porras, and V. Shmatikov. Privacy-preserving sharing and correlation of security alerts. In *Proceedings of the 13th conference on USENIX Security Symposium*, pages 239–254, San Diego, CA; United States, 2004. USENIX Association.

[49] D. Liu, Y. Ji, and V. Mookerjee. Knowledge sharing and investment decisions in information security. *Decision Support Systems*, 52(1):95–107, 2011.

[50] Lockton. Cyber risks decoded. Technical Report February, 2012.

[51] G. Lodi, L. Aniello, G. a. Di Luna, and R. Baldoni. An event-based platform for collaborative threats detection and monitoring. *Information Systems*, 39(January):175–195, Jan. 2014. ISSN 03064379. doi: 10.1016/j.is.2013.07.005.

[52] McAfee. Net Losses: Estimating the Global Cost of Cybercrime. Technical Report June, 2014.

[53] NATO Communications and Information Agency. NCI Agency Malware Information Sharing Platform.

[54] NCSC. Cyber Security Assessment - Netherlands. Technical report, 2012.

[55] NCSC. Welke ISAC's zijn er? https://www.ncsc.nl/organisatie/publiek-private-samenwerking/isacs/welke-isacs-zijn-er.html, n.d. n.d.

[56] M. Nieuwenhuis. Explosieve stijging van cyberaanvallen. http://www.ad.nl/ad/nl/5595/Digitaal/article/detail/3534364/2013/10/28/Explosieve-stijging-van-cyberaanvallen.dhtml, October 2013.

[57] NIST. Framework for Improving Critical Infrastructure Cybersecurity. page 39, 2014. URL http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[58] D. Ochel. Comparing NIST's Cybersecurity Framework with ISO/IEC 27001. http://www.secuilibrium.com/news/comparing-isoiec-27001-with-nists-cybersecurity-framework, February 2014.

[59] S. Oda, H. Fu, and Y. Zhu. Enterprise information security architecture a review of frameworks, methodology, and case studies. In *Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on*, pages 333–337, Beijing, China, 2009. IEEE. ISBN 9781424445202.

[60] K. Papadaki and D. Polemi. Collaboration and Knowledge Sharing Platform for supporting a Risk Management Network of Practice. In A. Mellouk, J. Bi, G. Ortiz, D. K. W. Chiu, and M. Popescu, editors, *Internet and Web Applications and Services, 2008. ICIW '08. Third International Conference on*, pages 239–244, Athens, Greece, 2008. IEEE. ISBN 978-1-4244-4238-6.

[61] C. E. Phillips, T. Ting, and S. a. Demurjian. Information sharing and security in dynamic coalitions. In *Proceedings of the seventh ACM symposium on Access control models and technologies - SACMAT '02*, pages –96, Monterey, CA; United States, 2002. ACM Press. ISBN 1581134967.

[62] Retail Industry Leaders Association. Retailers launch comprehensive cyber intelligence sharing center. http://www.rila.org/news/topnews/Pages/RetailersLaunchComprehensiveCyberIntelligenceSharingCenter.aspx, May 2014.

[63] N. Robinson and E. Disley. Incentives and Challenges for Information Sharing in the Context of Network and Information Security. *Resilient e-Communications Networks*, 10:52, 2010.

[64] R. S. Ross. Security and Privacy Controls for Federal Information Systems and Organizations. Technical report, NIST, 2014.

[65] A. Schaad and M. Borozdin. TAM 2: Automated Threat Analysis. In *Proceedings of the 27th Annual ACM Symposium on Applied Computing*, pages 1103–1108, Riva del Garda, Italy, 2012. ACM Press. ISBN 9781450308571.

[66] J. Schellevis. Gegevens deel bol.com-klanten waren toegankelijk via sql-injectie. http://tweakers.net/nieuws/82873/gegevens-deel-bol-punt-com-klanten-waren-.toegankelijk-via-sql-injectie.html, July 2012.

[67] Security.nl. Skimmers slaan keihard toe bij Albert Heijn. https://www.security.nl/posting/27380/Skimmers+slaan+keihard+toe+bij+Albert+Heijn, January 2010.

[68] Security.nl. Meeste AH-klanten willen privacy niet ruilen voor bonus. https://www.security.nl/posting/384743/Meeste+AH-klanten+willen+privacy+niet+ruilen+voor+bonus, April 2014.

[69] M. Shariati, F. Bahmani, and F. Shams. Enterprise information security, a review of architectures and frameworks from interoperability perspective. *Procedia Computer Science*, 3:537–543, Jan. 2011. ISSN 18770509.

[70] A. Slagell and W. Yurcik. Sharing computer network logs for security and privacy: A motivation for new methodologies of anonymization. In *Workshop of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks, 2005*, volume 2005, pages 82–91, Athens, Greece, 2005. IEEE. ISBN 0780394690.

[71] G. E. Smith, K. J. Watson, W. H. Baker, and J. a. Pokorski II. A critical balance: collaboration and security in the IT-enabled supply chain. *International Journal of Production Research*, 45(11): 2595–2613, June 2007. ISSN 0020-7543.

[72] J. Steven. Threat Modeling-Perhaps It's Time. *Security & Privacy, IEEE*, 8(3):83–86, 2010.

[73] T. Takahashi and Y. Kadobayashi. Cybersecurity Information Exchange Techniques: Cybersecurity Information Ontology and CYBEX. *Journal of the National Institute of Information and Communications Technology*, 58(3/4):127–136, 2010.

[74] E. Todeva and D. Knoke. Strategic alliances and models of collaboration. *Management Decision*, 43(1988):1–22, 2005.

[75] Trustwave. 2013 Global Security Report. Technical report, 2013.

[76] D. Tsai, W. Chen, Y. Lu, and C. Wu. A trusted security information sharing mechanism. In *Security Technology, 2009. 43rd Annual 2009 International Carnahan Conference on*, pages 257–260, Zurich, Switzerland, 2009. IEEE.

[77] Verizon. 2014 Data Breach Investigations Report. Technical report, 2014.

[78] J. Wagenaar. Collaboration in Cyber Security Defence, 2014. URL http://www.wagenaar.info/thesis/Collaboration_in_cyber_security_defence.pdf.

[79] M. Waller, M. E. Johnson, and T. Davis. Vendor-managed inventory in the retail supply chain. *Journal of Business Logistics*, (20): 183–204, 1999. ISSN 07353766.

[80] Y.-G. Wang, X. Li, and W. Hu. Distributed Detection of Network Intrusions Based on a Parametric Model. In *2008 IEEE International Conference on Systems, Man and Cybernetics*, pages 2068–2073, Singapore, 2008. IEEE. ISBN 1062-922X 978-1-4244-2383-5.

[81] E. T. Welsh, C. R. Wanberg, K. G. Brown, and M. J. Simmering. E-learning: emerging uses, empirical results and future directions. *International Journal of Training and Development*, 7(4): 245–258, 2003.

[82] Whitehat Security. Website Security Statistics Report, 2013. URL https://www.whitehatsec.com/resource/stats.html.

[83] Willis. Willis special report: 10k disclosures, 2014.

[84] B. d. Winter. Lek 18: 715.000 klanten van cheaptickets.nl. http://webwereld.nl/beveiliging/55080-lek-18-715-000-klanten-van-cheaptickets-nl---update, October 2011.

[85] S. Xu. Collaborative attack vs. collaborative defense. In *Collaborative Computing: Networking, Applications and Worksharing*, pages 217–228. Springer Berlin Heidelberg, 2009.

[86] W. Yu, G. Xu, Z. Chen, and P. Moulema. A cloud computing based architecture for cyber security situation awareness. In *Communications and Network Security (CNS), 2013 IEEE Conference on*, pages 488–492, National Harbor, MD; United States, 2013.

[87] R. Zenger. Datalek: klantgegevens sportwinkel op straat. https://www.bof.nl/2012/05/28/datalek-klantgegevens-sportwinkel-op-straat/, May 2012.

[88] J. Zhang, N. Borisov, and W. Yurcik. Outsourcing security analysis with anonymized logs. In *Securecomm and Workshops, 2006*, pages 1–9, Baltimore, MD; United States, 2006. IEEE.

[89] W. Zhao and G. White. A Collaborative Information Sharing Framework for Community Cyber Security. In *Homeland Security (HST), 2012 IEEE Conference on Technologies for*, pages 457–462, Waltham, MA; United States, 2012. IEEE.

[90] C. V. Zhou, C. Leckie, and S. Karunasekera. A survey of coordinated attacks and collaborative intrusion detection. *Computers & Security*, 29(1):124–140, Feb. 2010. ISSN 01674048.

A

NIST FRAMEWORK

A.1 SHORTLIST

The extensive list of 98 subcategories is narrowed down to a shortlist of 23 subcategories, each describing cyber security activities. Subcategories were left out of the shortlist based on the following criteria:

- The activity is not organization-specific
- The activity could benefit from additional knowledge
- The activity could benefit from additional information

The following subcategories remain:

1. **ID.RA-2:** Threat and vulnerability information is received from information sharing forums and sources.
2. **ID.RA-3:** Threats, both internal and external, are identified and documented.
3. **PR.AT-1:** All users are informed and trained.
4. **PR.AT-3:** Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities.
5. **PR.DS-4:** Adequate capacity to ensure availability is maintained.
6. **PR.IP-7:** Protection processes are continuously improved.
7. **PR.IP-8:** Effectiveness of protection technologies is shared with appropriate parties.
8. **DE.AE-2:** Detected events are analyzed to understand attack targets and methods.
9. **DE.AE-3:** Event data are aggregated and correlated from multiple sources and sensors.
10. **DE.CM-1:** The network is monitored to detect potential cyber security events.

11. **DE.CM-2:** The physical environment is monitored to detect potential cyber security events.
12. **DE.CM-4:** Malicious code is detected.
13. **DE.CM-6:** External service provider activity is monitored to detect potential cyber security events.
14. **DE.DP-4:** Event detection information is communicated to appropriate parties.
15. **DE.DP-5:** Detection processes are continuously improved.
16. **RS.CO-3:** Information is shared consistent with response plans.
17. **RS.CO-4:** Coordination with stakeholders occurs consistent with response plans.
18. **RS.CO-5:** Voluntary information sharing occurs with external stakeholders to achieve broader cyber security situational awareness.
19. **RC.CO-3:** Recovery activities are communicated to internal stakeholders and executive and management teams.

A.2 LITERATURE

The activities listed for each of the subcategories of the NIST Cyber Security Framework are compared with literature related to that subject. Every subcategory is listed below, followed by findings in the literature.

ID.RA-2	Threat and vulnerability information is received from information sharing forums and sources.
Literature	ID.RA-2 states that additional information should be *retrieved* from external sources. Zhou et al. [90] suggest that organizations should collaborate by correlating information from intrusion detection systems. Some attacks are extremely difficult to detect because they occur in multiple networks simultaneously. This collaborative approach has the potential to detect intrusions that occur across the whole internet simultaneously, by correlating attack signatures among different subnetworks of the internet. Zhao and White [89] confirm this and adds that potential risks could be detected earlier and the correlation has a positive effect on the effectiveness of detection and prevention.
Practice	The interviewees all agree that obtaining information from sharing forums and sources is useful if this information is reliable. Yet, *sharing* threat and vulnerability to such platforms is something that brings difficulties. For sharing information to such platforms, there should be an exchange platform such as an ISAC [1, 5]. The success of such a platform depends on the maturity: a more mature platform allows the exchange of more detailed and sensitive information, which is more useful [5].

ID.RA-3	Threats, both internal and external, are identified and documented.
Literature	This subcategory refers to RA-3 of the NIST SP-800-53rev4 [64]: risk assessment. RA-3 requires identification and documentation of risk assessment results. The exchange of threat identification information could assist in detecting early indications of potential threats, as Zhao and White [89] identify in the Prevent & Protect stage of their framework. The literature studied does not mention the exchange of documented risks specifically. On a more abstract level, exchange of information is explained such that it could also include the exchange of documentation. The exchange of information is mentioned by Feledi et al. [20, 21] and states that the exchange of information could lead to solutions of higher quality and saves valuable resources.
Practice	The interviewees think sharing documentation is beneficial [4, 1]. The sharing of documentation should only be limited to external threats, as they only contain information from the external environment which is useful for others [1]. Exposing threats and vulnerabilities of the internal environment could expose weaknesses. In one case an interviewee lets know that threats aren't documented, so there's no documentation to be shared [5].

PR.AT-1	All users are informed and trained.
Literature	Collaborating in this area could bring economies of scale in the case of e-learning: this technology can be used to reduce training costs if there are a large number of learners, if the learners are geographically dispersed and if the course will be repeated several times [81].
Practice	In general, collaboratively organizing user trainings is considered useful. Costs could be reduced if staff from multiple retailers were trained [1]. The trainings could also be developed in collaboration, but the trainings itself require a specific part for every retailer [4].

PR.AT-3	Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities.
Literature	In line with PR.AT-1, organizations could benefit of economies of scale when collaborating, by using e-learnings to make third-party stakeholders understand roles & responsibilities [81]. §13.2.2 of ISO27002:2013 [35] describes information transfer agreements between the organization and external parties.
Practice	In general this is considered to be the responsibility of the third-party stakeholders to have their roles & responsibilities in place [4, 5]. Organizing trainings for third-party stakeholders is considered difficult: third-party organizations differ a lot in size and core business, requiring different needs for training [5]. Additionally, contact with third-party stakeholders is often organized outside the risk management department [1]. A translation would be necessary.

PR.DS-4	Adequate capacity to ensure availability is maintained.
Literature	Zhou et al. [90] discuss Collaborative Intrusion Detection Systems (CIDS) which could reduce computational costs by sharing intrusion detection resources between networks. The resources that are saved could be used to improve the availability.
Practice	To share capacity means IT infrastructure is used for multiple organizations. This is considered rather a risk than an advantage [4, 5]. Using a (private) cloud environment could be beneficial, but does not necessarily require collaboration with retail organizations: any organization could be a partner [1].

PR.IP-7	Protection processes are continuously improved.
Literature	As mentioned at ID.RA-2, Zhao and White [89], Zhou et al. [90], Zhang et al. [88] and Slagell and Yurcik [70] state that correlation of information from multiple sources will lead to better detection of sophisticated attacks that are occurring in multiple networks. Feledi et al. [21] confirm this: "An exchange of knowledge between experts would be desirable in order to prevent developing always the same solutions by independent persons. Such an exchange could also lead to solutions of higher quality, as existing approaches could be advanced, instead of always reinventing the security wheel".
Practice	The interviewees think this could be interesting, although it is not done in practice yet [4, 1]. There should be a platform to facilitate confidential sharing of information, yet the sector and its organizations are not mature enough [4, 5]. Additionally, the information shared should not contain competitively sensitive information [1].

PR.IP-8	Effectiveness of protection technologies is shared with appropriate parties.
Literature	The NIST Cyber Security Framework already suggests sharing effectiveness with the appropriate parties. Zhao and White [89] confirm this, but considers the appropriate parties to be the organizations collaborating in the same community.
Practice	There is no consensus amongst the interviewees. One of the interviewees thinks collaboration in this area is not really necessary: when a specific technology doesn't work this is known quite fast already; sharing how technologies are applied and what the added value is would be more interesting [4]. Another interviewee thinks it can be of added value, as long as no sensitive information is shared [1]. This in accordance with a third interviewee, who says to use sources such as forums to obtain a variety of information, but not specifically about the effectiveness of protection technologies [5].

DE.AE-2	Detected events are analyzed to understand attack targets and methods.
Literature	Slagell and Yurcik [70] suggest sharing event data (logs) in order to make more refined tools for computer forensics and log analysis. This is supported by Zhang et al. [88]: correlating logs across organizations, contributes to a more effective response.
Practice	In general, the interviewees are positive about collaborating in this area, but an organization should in the first place be able to detect and analyze events on its own [4]. An important requirement is that sensitive information shouldn't be shared, and only external events (events from outside the organization) should be shared [1]. In one interview it is mentioned that tools used for event detection and analysis often report back to the manufacturer in order to improve protection [5].

DE.AE-3	Event data are aggregated and correlated from multiple sources and sensors.
Literature	Although event data is aggregated and correlated from multiple sources and sensors, Slagell and Yurcik [70] suggest sharing event data (logs) in order to make more refined tools for computer forensics and log analysis.
Practice	This is considered to be useful by the interviewees, although the need for such an approach would require more serious cyber threats [1]. In line with DE.AE-2, organizations should be able to do this activity within the organization in the first place before other organizations are consulted [4]. Sharing a filtered set of data, and obtaining data in return is considered to be useful though [5].

DE.CM-1	The network is monitored to detect potential cyber security events.
Literature	In line with DE.AE-2 and DE.AE-3, Slagell and Yurcik [70] & Zhao and White [89] state that events can be better detected by sharing logs. This is also of potential value for this activity.
Practice	This is considered to be effective. External events can be shared through this way [1] and it is mentioned by [5] that the tools they use already exchange information with the manufacturer in order to improve protection.

DE.CM-2	The physical environment is monitored to detect potential cyber security events.
Literature	Phillips et al. [61] state that physical security is always a consideration for information sharing. When physical assets are federated in a coalition, controlling physical access is dramatically complicated.
Practice	Not much support for collaboration in DE.CM-2 can be found. The interviewees consider data about the physical environment too specific to make sharing useful [1, 5]. On top of that, sharing data about staff members could cause privacy-related issues [5].

DE.CM-4	Malicious code is detected.
Literature	Different types of malicious code exist. The NATO has been using a platform to exchange information and knowledge about malware and marks the elimination of duplication of analytical work and faster threat detection amongst their benefits. [53] Additionally, Zhao and White [89] mention collaboration could aid in the detection of malicious or unauthorized activities.
Practice	From the practice the exchange of information on this subject gains a lot of interest, and one organization even indicates that they are already doing this. The exchange could be beneficial in general [4] but mostly for system software such as database systems and middleware [1]. In the last case, collaboration with other retail organizations is not strictly necessary as the use of these software products is not limited to retail organizations.

DE.CM-6	External service provider activity is monitored to detect potential cyber security events.
Literature	Cyber attacks often can come through compromised networks with a trust relationship. Bruce and Fink [10] state that in such cases collaboration is important for sound security, clues for a solution are spread across many networks and systems with many owners.
Practice	Initially this could provide retail organizations with a lot of advantages. A standard framework for security agreements could be created, of which the compliance is checked by a third party on behalf of the collaborating organizations [4]. Especially the cloud trend makes compliance important: often retailers are using the same cloud-based products [1]. Barriers to sharing information about external service providers include the legal aspects and responsibilities. Disclosing information about certain aspects of an external service provider could cause legal disputes, if i.e. this is unproven negative information [5]. Responsibilities for the previously mentioned compliancy check should arranged: an interviewed organization is reluctant to let peer-organizations sign for a compliancy check that would also apply for (amongst others) his organization.

DE.DP-4	Event detection information is communicated to appropriate parties.
Literature	Zhao and White [89] state in line with PR.IP-8 that event detection information should be shared within the organizations collaborating in the same community.
Practice	Although there are different opinions between the interviewees, in practice exchanging event detection information is considered to be useful. Event detection information can be shared right away or it can be analyzed first. Sharing information right away is already taking place at one organization through the use of software that reports back to the manufacturer [5]. Event detection information can be filtered first and shared afterwards as well. Events are filtered first and only information that is considered to be useful after analysis [4].

DE.DP-5	Detection processes are continuously improved.
Literature	In line with ID.RA-2 and PR.IP-7, the correlation of multiple sources will lead to better detection of sophisticated attacks [89, 90, 88, 70, 21]
Practice	Collaborating in DE.DP-5 could be beneficial according to [4, 1]. [5] states that their organization is not mature enough: before adopting a collaborative approach they have to streamline their internal processes first. The exchange of signatures and anomalies could be useful for the continuous improvement of detection processes [4].

RS.CO-3	Information is shared consistent with response plans.
Literature	Zhao and White [89] state that the design of response plans can be assisted by using relevant information from external sources.
Practice	The practice is interested in incorporating information sharing in their response plans. It is suggested that this is done at the evaluation phase as one of the final steps [4]. The possibility of outbreak to other companies also plays a role [5]

RS.CO-4	Coordination with stakeholders occurs consistent with response plans.
Literature	Zhao and White [89] state that a centralized coordination group is required to participate in sharing response and recovery recommendations as well as mitigation strategies.
Practice	The idea collaborating with stakeholders by exchanging knowledge and information gains support from all the interviewed people. Often attacks that reach or affect multiple stakeholders are captured by IT service providers. These attacks are often generic and not sector-specific as can be seen in some other sectors. If this will be the case in the future, a collaborative approach is desirable [4]. ISACs are a suitable forum for coordination with peer organizations in case they are involved or affected, given the participants trust each other and confidentiality is guaranteed [5].

RS.CO-5	Voluntary information sharing occurs with external stakeholders to achieve broader cyber security situational awareness.
Literature	Zhao and White [89] describe that during response phase both routine information and incident-specific information should be shared.
Practice	Exchanging current information about threats, vulnerabilities and incidents with collaborating organizations is a type of collaboration all interviewees are interested in. An important requirement is confidentiality and trust. Confidentiality and trust are also important to reach a higher maturity in an exchange forum, which allows to share more confident and more useful information [5].

RC.CO-3	Recovery activities are communicated to internal stakeholders and executive and management teams.
Literature	Zhao and White [89] state that information relevant to the evaluation of response effectiveness is required to be shared in the resolve stage of the cyber incident response cycle of a community.
Practice	Communicating recovery activities to collaborating organizations is not considered to be useful by all stakeholders. Supporters of collaboration on this topic state sharing successful processes and procedures can be of good use [4]. Adversaries state that the added value will be low [1] and that it's not necessary to report recovery activities as long as the effects remain invisible to the outside world and things turn back to normal [5].

B

INTERVIEWS

B.1 QUESTIONS FOR VALIDATION OF THE THREAT MODEL

1. Can you describe the cyber threats that influence your organization the most?
2. Which of the following threats do you recognize?
    - *Spoofing*: An attacker tries to be something or someone he/she isn't.
    - *Tampering*: An attacker attempts to modify data that's exchanged between your application and a legitimate user.
    - *Repudiation*: An attacker or actor can perform an action with your application that is not attributable.
    - *Information disclosure*: An attacker can read the private data that your application is transmitting or storing.
    - *Denial of service*: An attacker can prevent your legitimate users from accessing your application or service.
    - *Elevation of privilege*: An attacker is able to gain elevated access rights through unauthorized means.
3. Are you aware of any threats that are not in this model?

B.2 DESCRIPTION OF THE INTERVIEWEES

The interviewees that participated in the validation of the threat model can be found in table 11, the interviewees that participated in the practice assessment can be found in table 12.

Table 11: Description of the interviewees used for the validation of the threat model

Interview reference	Country	Description
[1]	The Netherlands	Chief information security officer of a retail organization in the Netherlands
[2]	The Netherlands	Independent cyber security consultant in the retail sector
[4]	The Netherlands	Global chief information security officer of an international retail organization
[5]	The Netherlands	Chief information security officer of an international retail organization with significant activities in the Netherlands.

Table 12: Description of the interviewees used for the practice assessment

Interview reference	Country	Description
[1]	The Netherlands	Chief information security officer of a retail organization in the Netherlands
[4]	The Netherlands	Global chief information security officer of an international retail organization
[5]	The Netherlands	Chief information security officer of an international retail organization with significant activities in the Netherlands.