UTRECHT UNIVERSITY

MASTER THESIS

MCP: The risk modelling framework for the banking sector

A MULTI-CHANNEL CYBER-ATTACK PATTERN-BASED APPROACH TO MODELLING RISK

Author:
Oka Jacob ARNTZEN

University Supervisor:
Dr. Gerard TEL
Dr. Fabiano DALPIAZ

Daily Supervisor:
Ir. Geert-Jan WACKERS

A thesis submitted for the MSc Business Informatics
in the
Department of Information and Computing Sciences
Utrecht University

May 20, 2019

Universiteit Utrecht

"Our deepest fear is not that we are inadequate. Our deepest fear is that we are powerful beyond measure."

Marianne Willamson

UTRECHT UNIVERSITY

Abstract

Faculty of Science
Department of Information and Computing Sciences

MSc Business Informatics

MCP: The risk modelling framework for the banking sector

by Oka Jacob ARNTZEN

Context: The world is changing rapidly, driven by an increased focus of integrating Information Technology (IT) into everyday life. Organisations integrate IT into their products and services to provide increased convenience and efficiency, as well as to reduce costs. Banks are no exception to this trend. This increase in IT use has in turn introduced new security challenges and risks that have to be taken into account and mitigated. **Objective:** The goal of this research is to develop a risk modelling framework for cyber-attacks that expands on existing security concepts by including the impact and likelihood associated with these threats to determine risk. This research focuses on cyber-attacks that target banking institutions. **Method:** This thesis was conducted based on theory from the Design Science methodology. A thorough literature review was carried out to understand the problem context and existing theory available. This was supported by consultations with experts from the banking sector and outsiders to gain a better understanding of the practical aspects of risk and cyber-attacks, and their alignment with theory. A framework was then designed based on this information, which was validated by expert reviews. This led to modifications aimed to improve the correctness and usefulness of the framework. **Results:** This research produced a single artefact, a risk modelling framework. Information that was used as input for the framework was analysed and resulted in a number of findings regarding IT risk perceptions. **Conclusion:** The cyber-attacks analysed in this research context were not classified as high risk for a banking institution, however differs per institution. This research revealed that IT risk is difficult to model accurately due to the varying nature and complexity of factors that contribute to determining risk. More research needs to be conducted to improve risk estimation techniques and perception amongst experts.

Keywords: risk, IT risk, risk modelling, risk banking sector, cyber-attacks, risk modelling, risk framework

Acknowledgements

I would like to thank a couple of people for their help and support throughout this thesis.

First and foremost, I would like to show my appreciation to my Utrecht University supervisors, Gerard and Fabiano. Gerard in particular, as he stepped in when my initial first supervisor left the university. He calmed my uncertainty during the handover phase, and supported me greatly in the thesis content and process that followed.

I would also like to extend thanks to my supervisor at my work placement company. Geert-Jan was always welcoming and interested in assisting me throughout the process. As my daily supervisor he was always available, providing me with valuable insights and often an alternative perspective on the various aspects of conducting a sound thesis. He often challenged me to broaden my horizon and try new things, giving my advice on an professional and personal level.

Special thanks to all my friends that have supported me during and before my thesis journey started. Forcing me to take breaks, occasionally reading bits and pieces of my thesis but most importantly encouraging me to be social when I wasn't exactly open to it. Additional thanks to my fellow graduate interns at the work placement company for the many brainstorming moments during social coffee and lunch breaks.

Lastly, I would like to give the biggest thanks and love to my parents and brother for their continuous support throughout my life and it's many endeavours. They have always believed in me and stood behind me, regardless of the situation and circumstances, challenging me to greater things.

Contents

List of Figures

List of Tables

List of Abbreviations

APT	**A**dvanced **P**ersistent **T**hreat
ATM	**A**utomatic **T**eller **M**achine
DDoS	**D**istributed **D**enial **o**f **S**ervice
DMZ	**D**emilitarized **Z**one
EMS	**E**mergency **M**edical **S**ystems
EU	**E**uropean **U**nion
ISMS	**I**nformation **S**ecurity **M**anagement **S**ystem
IT	**I**nformation **T**echnology
MCP	**M**ulti **C**hannel **P**atterns
OSI	**O**pen **S**ystems **I**nterconnection
POS	**P**oint-**O**f-**S**ale
RM	**R**isk **M**anagement
RQ	**R**esearch **Q**uestion
SWIFT	**S**ociety for **W**orldwide **I**nterbank **F**inancial **T**elecommunication
VM	**V**irtual **M**achine
2FA	**T**wo **F**actor **A**uthentication

Chapter 1

Introduction

This chapter provides an elaborate, yet specific introduction to this thesis that will research cyber-attack patterns in the banking sector. It will discuss the scientific gap and motivation of the research, as well as the scope that the research will be restricted to. Finally, the structure of this thesis will be explained.

1.1 Problem statement

The world is changing constantly, faster than ever. The amount of information technology (IT) people are shown or interact with, directly or indirectly, is increasing and taking a much more prominent role in their daily lives. This occurs on both a personal and professional level. IT has, over time, evolved to be more complex and inter-dependent, taking responsibility for more vital processes and functions that were previously carried out by people.

An example of such a responsibility is explained by Khurana et al., 2010 where power supply grids are made 'smart' by augmenting existing physical infrastructure with IT. Examples of other fields in which IT continues to take a more prominent role are illustrated in Table 1.1 below.

TABLE 1.1: Examples of IT in different fields

Field	Examples
Utility sector	Power utilities use IT to regulate and distribute power efficiently to autonomously to reduce load on the electricity grid.
Defence/Security	Companies use IT to remotely monitor assets and resources against physical or digital threats.
Manufacturing	IT and robotics are used in factories to automate processes, production and improve logistical/distribution efficiency.
Public health	IT is used in EMS systems to support medical procedures in healthcare facilities.
Economics	Financial institutions use IT in the trading floor to carry out automated market trading.

As the capabilities, availability and inter-dependency of IT systems grew, so did the risks and threats associated with them (Khurana et al., 2010). Ben-Asher and Gonzalez, 2015 point out that new weaknesses in IT systems emerge constantly and that new, complex attack strategies (Choo, 2011) are employed to misuse them. A non-banking incident illustrating how an intruder abuses a weakness in an IT system is presented by Case, 2016, a case in which a cyber-attack on an electrical power grid caused severe electricity disruptions. A study conducted by Accenture (Accenture, 2017) in 2017 revealed that the number of successful cyber-attacks on organisations increases by 27% each year; Ransomware attacks increasing the most, doubling every year for the past 5 years.

The banking sector is no different. The increasing complexity of IT has led to the emergence of new and evolving challenges that pose a risk to the stability of institutions. These threats have in turn led to stricter regulatory requirements that banks have to adhere to. IT is used to perform functions in a more accurate and often more efficient manner than people do.

Examples of such functions include:

- Handling as well as processing transactions and payments.
- Application and services monitoring.
- Fraud and attack detection.
- Loan and mortgage management.

By offering more products and services online and in real-time across various platforms and media, institutions in the banking sector are susceptible to abuse due to cyber-attacks. Cyber-attacks refer to malicious attempts to gain unauthorised access to an IT system through the internet. An illustration of such is the number of cyber-attacks targeting the SWIFT[1] banking network in 2018 tripled compared to the year before, and of those attacks, 9 were successful in breaching systems (*The Hi-Tech Crime Trends* 2018).

In addition, Camillo, 2017 states that the number of attacks directed at institutions in the financial sector in 2015 increased by 80% compared to the previous year. That, together with a Kaspersky Lab report from 2017 (Kaspersky, 2017) pointing out that the average cost per cyber-attack on a banking institution is estimated at $1.8 million, further emphasises the need for increased security awareness.

By increasing their online presence, bank customers have the ability to carry out more services independently, without contacting a bank employee. Whether a customer is changing their personal information, checking their balance or conducting a transaction, an institution's online presence and expanding range of services will likely have consequences for its security. In reality, a cyber-attack often consists of a combination of different attacks that together form a cyber-attack pattern.

1.2 Motivation

Regardless of their size, organisations worldwide are investing money and resources into measures to prevent and combat the threats posed by cyber-attacks. Successful cyber-attacks have financial implications that run into millions of dollars per year, often leading to reputational damage and severe service disruptions (Julisch, 2013). Therefore, organisations are under strain to maintain a satisfactory level of security (Julisch, 2013).

In an IT context, security refers to the implementation of controls to prevent the of abuse of IT assets and systems. In doing so, providing security aims to maintain availability and integrity.

Several initiatives by organisations and governments worldwide aim to standardise and provide best practice guidelines for cyber-security risks such as the NIST cybersecurity framework (Sedgewick, 2014) and ISO27001 (Disterer, 2013). These types of initiatives are commonly known as control frameworks due to their 'validating' nature; verifying an organisation's existing security standards and policies using objectives and measures provided by the control framework.

Control frameworks are therefore security-oriented standards and policies where the objectives and measures that an organisation has to adhere to are fixed. However exceptions are often

[1]SWIFT: The global provider of secure financial messaging services used by banks worldwide to send and receive information (www.swift.com)

made to suit a particular organisational situation which, in terms of protection, are not in an organisation's best interest as they affect their level of security compliance. Control frameworks also do not take the impact and implications of a security breach into account.

As the complexity of IT in organisations grew, so did the number of exceptions in security controls. In many cases, this leads to an increase in the finances and resources necessary to maintain compliance, but also complicates matters as each exception will differ from the other.

There is however no comprehensive, holistic model that encompasses IT risk, taking both technical and non-technical aspects such as business objectives, budget and general risk into account. In this context risk refers to the threats, vulnerability and the accompanying impact, that may occur should a risk materialise.

Organisations use control frameworks to adhere to security regulations and standards, ensuring the security of critical data. As mentioned, control frameworks do not take risks, along with their impact and likelihood into account. The use of risk management frameworks has increased in recent years, with organisations switching from the traditional control frameworks to account for risk when dealing with security threats. Basic risk analysis concepts point to different controls that can be implemented.

This thesis aims to fill a void by developing a risk modelling framework that incorporates IT, business objectives and risk to counteract cyber-attacks for banking institutions. In essence it will combine strategic, IT security and operational targets with risk management principles and findings from other fields to define a domain-specific IT risk framework for the banking sector.

By developing a risk modelling framework, this thesis analyses the threats that target institutions in the banking sector. Risk management concepts in other fields will be, where applicable, applied to determine the risk of these threats.

Figure 1.1 illustrates the gap that the developed risk modelling framework will fill. Information will be obtained from IT security principles as well as risk management in other fields, which will be used to determine the impact and risk of cyber-attacks.

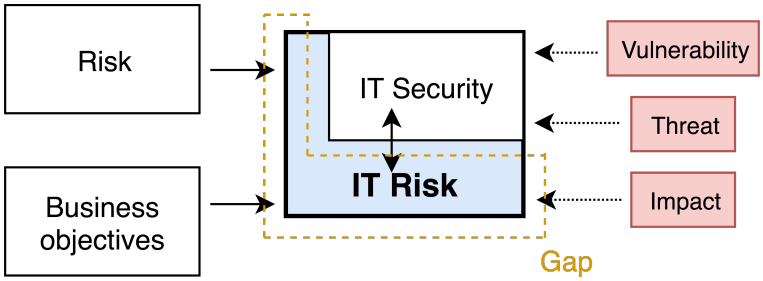

FIGURE 1.1: Illustration of the gap in literature and motivation

1.3 Scope

The scope of this research thesis titled 'MCP: The risk modelling framework for the banking sector' is bound to designing a multi-channel cyber-attack patterns-based risk modelling framework specifically for the banking sector.

The term *multi-channel* is used to denote that various points of information exchange with a banking institution (to use a service for example) such as their website or mobile application will be looked into during this thesis. The channels that will be explored are elaborated on in Section 3.1.5. A cyber-attack *pattern* refers to the combination of a number of different forms of intrusion, also known as attack vectors (See section 3.1.5).

For clarification purposes, decisions made in the interest of conducting a sound research with regards to scoping (and their motivation) are mentioned and discussed below. The four main scoping concepts are visualised in Figure 1.2.

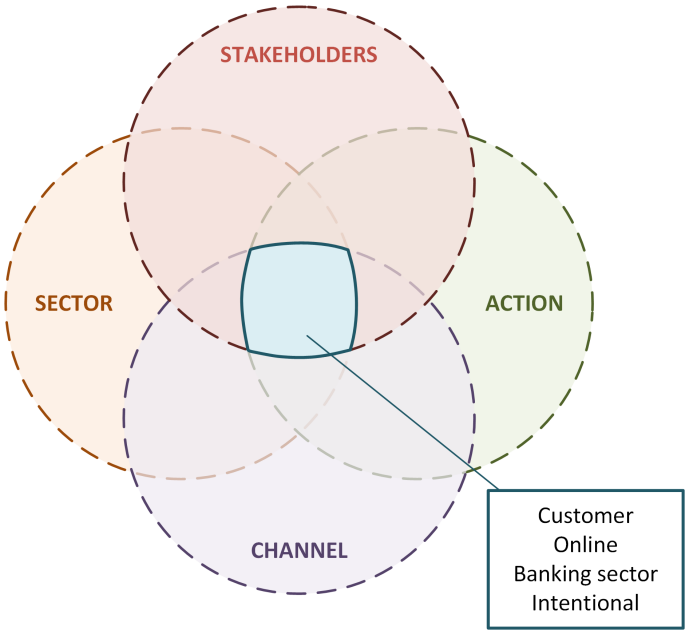

FIGURE 1.2: Visual representation of the thesis scope

Customers
As with most service providers, numerous stakeholders exist; from customers to employees and shareholders. With regards to commercial banks providing financial services, a customer is often in contact with an (administrative) employee of the bank.

The decision has been made to focus on investigating cyber-attacks that come through external channels. These are channels that *customers* typically use. Therefore this scoping boundary will ensure that cases of (internal) financial fraud, amongst other attacking threats that are considered to be coming from within the organisation, are excluded.

Online
In this day and age, customers and organisations can do almost anything *online*, hence the logical decision was made to scope the research to attacks being conducted in an online context. By using this term, this research refers to online as a medium for the transfer of information, or communication through the digital channel. This facilitating digital medium is often referred to as the internet.

When used alongside the term multi-channel, online therefore refers to different media facilitating information transfer with a bank through the internet.

Hence attacks that are carried out online and target commercial banks will, regardless of which channel through which they take place, be explored for this thesis. This includes attacks such as social engineering which are often initiated offline, but eventually lead to online threats.

Banking sector
This research will focus on IT risk management in the *banking sector*, thus focusing on cyber-attacks targeting commercial banks that provide services to both private and business customers. Therefore this thesis will exclude all other types of financial institutions such as insurance companies, funds providers, brokerages and investment companies.

As with all industries, each institution in the banking sector is different. This thesis will look at the generic banking products and services that all banks generally tend to offer. In this case

BankY, a large bank in The Netherlands has been selected for the validation. This is explained in Section 2.3.

The decision has been taken to scope the research to commercial banks so as to conduct a more in-depth research focused on one entity, rather than a brief overview of the whole spectrum of different types of financial institutions.

Intentional
Two types of actions exist; intentional and unintentional. This research will focus on *intentional* actions; activities that occur on a deliberate and purposeful basis. Depending on the scenario, intentional actions may have a collateral (unintentional) effect on assets or resources that surround the intended target.

The thesis was scoped to intentional actions as it focuses primarily on attacks directly targeting institutions in the banking sector. Therefore, it will not take the collateral effect that actions directed at other assets or resources into account.

1.4 Thesis outline

This chapter introduced the topic of this thesis by means of a problem statement, accompanied by the research's motivation and scope. Chapter 2 will elaborate on the research approach that was followed, which includes the research questions that will support the main goal of this thesis. Chapter 3 will present the findings of the review of literature and scientific theory that forms the foundation of this thesis.

Chapter 4 explains the decisions, design principles and steps taken to design the framework. Chapter 5 presents the designed framework, while Chapter 6 explains how the usefulness and correctness of the framework was validated. Chapter 7 presents the findings of the framework's validation. Chapter 8 reflects on the research by discussing a number of findings, answering the research questions, as well as mentioning the limitations encountered and possible future work that can expand or improve on this thesis.

Chapter 2

Research approach

This chapter introduces the main goal of this research. The research questions that have been formulated to support the main goal will be explained. Finally, the research method and approach taken to conduct the literature review will be described.

2.1 Research Questions

The main goal of this thesis is to develop a risk-based reference framework for cyber-attack patterns in the banking sector. The motivation for this thesis is explained in Section 1.2. The main goal is therefore formally defined as follows:

MAIN GOAL:
To design a multi-channel cyber-attack patterns-based risk modelling framework for the banking sector.

The main goal is in line with the motivation of this thesis which is to take risk factors such as impact and likelihood into account when determining the threat a cyber-attack poses.

A number of research questions have been defined to steer and guide this research to a satisfactory conclusion. The research questions have been formulated so as to, when combined together, achieve the main research goal (as shown in Figure 2.1).

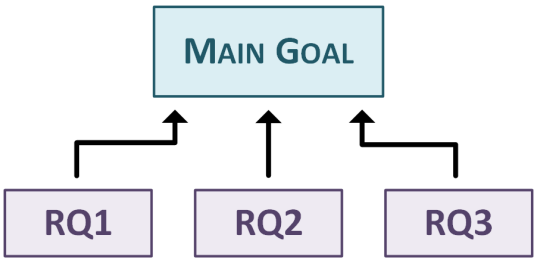

FIGURE 2.1: Relationship between the main goal and research questions

Each research question presented below includes a brief motivation and explanation of how the question will be satisfied.

RQ1: What aspects of generic risk management are relevant in an IT context?

This question will introduce and elaborate on the concept of risk management in general by looking at its purpose, components and application in various industries. This question will be answered by applying this knowledge to risk management in an IT context, having extracted relevant and useful concepts from other industries.

Normally, IT security forms the basis to define a risk management strategy for an organisation, this thesis will therefore deviate from the usual approach.

RQ2: What defines and characterises a cyber-attack in the banking sector?
The answer to this question should provide a clear definition of what the term 'cyber-attack' entails. It will further elaborate on the types of cyber-attacks, their requirements and capabilities as well as mention their possible impact.

This will be done by researching and analysing cyber-attacks in the banking sector, complemented with knowledge obtained how cyber-attacks affect other industries. The relevance and importance of detecting cyber-attack patterns will be discussed and justified.

RQ3: How can multi-channel cyber-attack patterns be optimally represented?
This question will answer how the cyber-attack patterns can be represented in a manner that best illustrates their components and impact they have. The representation will involve combining a number of factors, impact and likelihood for example, to give a complete view of the framework.

2.2 Research Method

A number of choices and decisions have been made in the best interest of this research. This section will elaborate on the research paradigm chosen, the Design Science Methodology (Wieringa, 2014), as well as the decisions and steps taken to conduct a clear, sound and thorough literature review.

2.2.1 Research Paradigm

As mentioned, this research follows the guidelines that are stipulated in the Design Science Methodology (Wieringa, 2014), which consists of three distinct phases shown in Figure 2.2; Problem Investigation, Treatment Design and Treatment Validation.

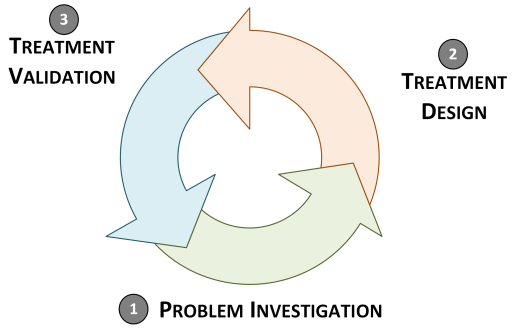

FIGURE 2.2: The Design Science Methodology's design cycle

Problem Investigation
The design process starts with the Problem Investigation phase. It is used to gather information about the context, to learn more about the problem to be treated, in doing so improving the knowledge and understanding of the *current* problem situation (Wieringa, 2014).

A detailed literature review will be conducted to collect and document information that will be used in the Treatment Design phase. The literature review will be used to identify relevant information in the context of this research, which will in turn provide a better understanding and insight with respect to how cyber-attacks are dealt with in the banking sector. Additionally, the literature review will study the application of risk management in other fields to determine

if certain elements can be applied to, or are of relevance, to this thesis' approach.

Treatment Design
The second phase, Treatment Design, uses knowledge from the Problem Investigation phase to develop a clear and well-defined list of requirements for the research's risk management framework. The requirements will be assessed, based on the initial goals discovered during the problem investigation to determine if the specified requirements will sufficiently fulfil the main goal of this research. Should the requirements insufficiently address the goals, the literature review will be expanded.

Using the requirements as guidelines, a new framework will be designed and developed that makes use of the knowledge and principles obtained regarding cyber-attacks, IT risk management in other fields and the banking sector from the first phase of the design cycle. This risk-based framework should fulfil the goals of this research, by including elements IT risk management from other sectors that are applicable to the banking sector with regards to cyber-attack patterns.

Treatment Validation
The Treatment Validation is the third and final phase of the design cycle, the goal is to "evaluate a treatment after it has been applied in the original problem context" (Wieringa, 2014).

During this phase, the designed framework will be validated through expert reviews at BankY (described in Section 2.3). To ensure the designed framework sufficiently fulfils the initial goals of this research, the questions formulated to determine the research goal and requirements for the framework's design will be revisited.

2.2.2 Literature Review

A comprehensive literature review was conducted to gain knowledge on the various topics this research thesis involves, as well as to understand the definitions and concepts that come into play. The literature review took place in the first phase of the thesis, the Problem Investigation Phase.

A systematic literature review technique was selected as it provides a means to identify, analyse and interpret all available research that is relevant to the topics of interest for this research (Kitchenham, 2004). A systematic literature review puts the current state of research regarding cyber-attacks and the banking sector into perspective, whilst also showing gaps in literature that form the motivation for this thesis.

The main requirement for the systematic literature review is that it be exhaustive and transparent to ensure the research's scientific contribution and value cannot be doubted. The process of collecting scientific literature involved querying numerous online databases using a predetermined set of search queries.

The search engine Google Scholar (GScholar) was consulted for scientific theory. GScholar presented results from the following online databases:

- Worldcat
- ScienceDirect
- ACM - Association for Computing Machinery: Digital Library
- IEEE - Institute of Electrical and Electronic Engineers
- DBLP - Computer Science bibliography

GScholar was consulted using search queries. Each query was defined using the research topic, questions and objective as motivators. A standard format was used to build up the search queries to ensure that most of the available papers about the topics of interest were found.

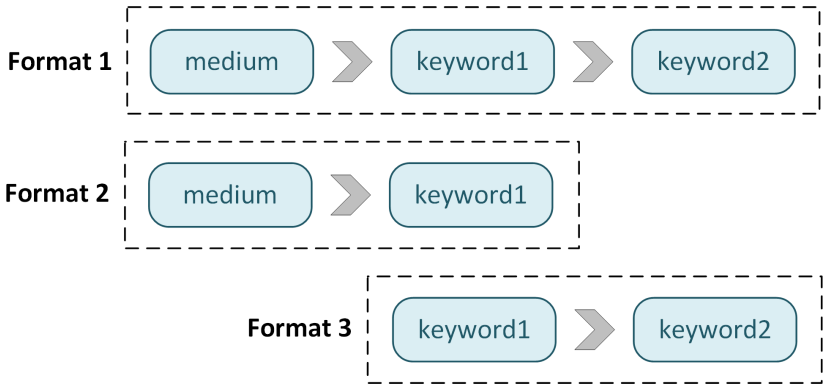

FIGURE 2.3: Format for generating database search queries

Figure 2.3 shows the procedure for building queries, which can have 3 formats. An example of a search query built using the first format would contain a string consisting of the variables *medium*, *keyword1* and *keyword2*. Replacing the variable names with keywords from Table 2.1 would produce, for example, the following search query:

medium + keyword1 + keyword2 = "cyber attack patterns"

Table 2.1 shows the different terms used to build up the search queries for the online databases and search engines. The semi-colon (;) between keywords in the *keyword2* column in Table 2.1 is an indication of separates keywords that can be used for building a query.

TABLE 2.1: Search query build-up

medium	**keyword1**	**keyword2**
Online	attacks	banks; banking institutions; insurance
	attack	patterns; vectors; reports; statistics; vectors; risk; banks; finance; implications; components
	threat	banks; reports; statistics; mitigation; components
	security	patterns; bank
	bank	security
Cyber	attack	history; banks; channels; patterns; components
	risk	history; banks; channels; patterns; management
	security	risks; patterns
IT	risk	statistics; reports; management
	security	banks; reports; risk
Bank	attack	vectors; risks; history; patterns; security; statistics
	attacks	
	security	incidents; attack patterns; vulnerabilities; banks
	risk management	insurance; IT; weather; economics; politics; gambling; banking; medicine
	risk	prevention; mitigation; statistics

Considering the positive reputation of the online databases listed and availability of articles, scientific literature from the online databases mentioned was considered exhaustive and

comprehensive enough for this research. Scientific literature such as books, journal articles and conference proceedings were collected as well.

The Snowball method (Wohlin et al., 2012) was employed to find additional papers. This refers to the process of using references to or from a paper to discover other relevant scientific papers (Wohlin et al., 2012). This thesis conducted backward snowballing, a process where the reference list of a paper is examined in order to discover other scientific papers that may be of interest.

Due to the relatively new nature of the IT risk management field, various trusted websites and whitepapers produced by internationally-renowned, industry-leading organisations were also used. This thesis will refer to these sources as *grey literature*, information obtained through other sources than traditional academic literature. This was done in order to obtain an alternative perspective that would supplement the scientific literature.

Information was obtained from the following organisations:

- ICT market-analysis company Gartner.
- Consultancy companies: Accenture, CapGemini, McKinsey.
- Accountancy companies: Deloitte, PWC, EY, KPMG.
- Cyber-security companies: Symantec, McAfee, Bitdefender, Avast, Kaspersky.

Once filtered based on relevance, the literature review resulted in 157 useful papers on the topics of interest. Further selection based on direct relevance and usefulness to this research resulted in a reduction of the number of papers for this thesis.

2.2.3 Expert Opinions

Expert opinions will be used in this thesis to obtain information in an informal and conversational manner from experts. This feedback will be used to gain knowledge as well as verify and validate information collected through other sources.

The expert opinions can be seen as a form of semi-structured interview in which an open discussion takes place. When carried out correctly, an expert opinion is a valuable data collection technique (Wieringa, 2014).

Experts from various departments and domains in BankY (see Section 2.3) will be consulted in order to obtain as much relevant information as possible about the topics this thesis touches on. Experts from outside BankY will also be consulted to gather a wider and more varying perspective of the topics at hand, improving the objectivity of information.

2.3 BankY

This research will be carried out at a bank in The Netherlands. The institution is an international bank that services approximately 8 million clients worldwide, providing customers with services ranging from banking to insurance, capital management and real estate. The types of customers vary from families or individuals to large-scale companies. For purposes of anonymity, the bank will be named BankY.

As with most institutions in the banking sector, BankY is working on bringing more reliable and robust services to their online platforms. The services mentioned are offered through traditional banking channels (physical offices), a dedicated telephone line as well as online through websites and other innovative channels (e.g. smart devices). The majority of the channels mentioned are facilitated online, therefore cyber-attacks are a real threat.

Staff members at BankY have made themselves available to, when necessary, give interviews and expert opinions throughout the course of this research. For the validation phase of this research, the developed framework will be validated using expert reviews of the framework, and a mapping of past and present cyber-attacks to the attack patterns this thesis discovers.

Chapter 3

Theoretical background

This chapter elaborates on the topics and themes that were researched during the literature review. The findings and conclusions of the literature review will be presented. Finally, the professions of experts that were consulted for additional information to supplement the literature review will be shown.

3.1 Literature Review

This section presents the research and findings of the review of a variety of concepts in literature for this thesis. The motivation for the decisions made for this literature review have been explained in Section 2.2.

Firstly, the general concept of Risk Management (RM) will be introduced followed by an analysis of RM in both a non-IT (Section 3.1.2) and IT (Section 3.1.3) context. Conclusions of knowledge obtained both perspectives is presented and discussed in Section 3.1.4.

Thereafter, cyber-attacks and their characteristics will be discussed. The literature review section will conclude with an analysis of other topics deemed relevant to this thesis.

3.1.1 Risk Management

Over the years, the world has evolved digitally to become faster, more dynamic and complex. This evolution has welcomed numerous opportunities and benefits, but has come coupled with weaknesses.

These very weaknesses have made risk important to take into account as it becomes more prevalent and prominent, in both a personal and professional context. Risk refers to the potential damage to, or possible loss of, a tangible or intangible asset without any direct gains in return (Wolke, 2017).

Several definitions of risk exist, differing slightly depending on the context in which it is being applied. A universal definition of risk that will be used in this thesis is presented in this section.

RM is a process that attempts to identify and best prepare to counteract *risks*. Boehm, 1991 describes RM as the process of identifying and analysing risk prior to it becoming a realistic threat to the 'normal' situation. Gartner on the other hand defines RM as the strategic discipline of assessing, prioritising, monitoring and controlling the impact of uncertainty on objectives.

Risk Management can be described from a non-technical perspective as the complete process of "identifying, quantifying and prioritising the risks organisations face" (Impe, 2017). Technical definitions of Risk Management introduce statistical concepts into the definition.

The following definition of Risk Management will be used throughout this thesis:

DEFINITION: Risk Management is the process of identifying, monitoring and prioritising risk by analysing the likelihood a threat will occur and the impact it will have.

Associated concepts

Three fundamental concepts of Risk Management were discovered during this review: likelihood (probability), impact (consequence) and risk. Further analysis revealed that these concepts are related to each other and often used interchangeably.

In literature, the concepts have different definitions. The exact definitions differed depending on the field and nature of their use.

For clarification purposes the following definitions of these associated concepts are explained.

DEFINITIONS:

- **Likelihood:** Describes the probability that an incident will occur, and what the consequence of that incident is. Likelihood can be formulated as:

$$likelihood = f(threat, vulnerability) \tag{3.1}$$

  Example - The likelihood that a high-value device will be stolen within months of purchase is medium to high.

- **Impact:** Describes the (negative) effect an occurrence will have on an individual or organisation should the incident take place. In IT, the type of impact can be split into two categories;
  - Technical impact: Impact on data confidentiality, integrity, availability and accountability.
  - Business impact: Effect on reputation, financial damage, privacy, non-compliance and legal implications.

  Example - Poorly produced (defective) laptops will lead to a decrease in revenue, affecting annual profit.

- **Risk:** Describes the potential of an incident in which a threat exploits a vulnerability and the corresponding impact on the individual or organisation (Dahbur, Mohammad, and Tarakji, 2011). Risk is a concept that cannot be completely eliminated, but risk should be kept as low as possible. Cases in which there are threats but no vulnerabilities, or there are no threats but vulnerabilities exist lead to minimal risks. Risk is defined as:

$$risk = impact \times likelihood \tag{3.2}$$

  The formula provided for risk differs per scientific paper. It should not be seen as the actual product of impact and likelihood, rather that there is a relationship between the two. Numerous papers mention risk to be the product of impact and likelihood, whereas others define risk as a logarithmic function of impact and likelihood. The common feature throughout the scientific literature is that risk is affected by the relationship between impact and likelihood.
  Example - Intellectual property collected by thieves or competitors from a stolen device can affect a company's annual results.

As Formula 3.1 shows, likelihood is based on a relationship between a threat and vulnerability. Risk on the other hand is shown in Formula 3.2 and determined by the likelihood an event will occur and its corresponding impact.

Risk management is applied to organisational situations and challenges across numerous fields. Section 3.1.2 presents the findings of the research and analysis of RM in a number of fields to gain a better understanding of its implementation in a non-IT perspective. Risk Management from an IT perspective is elaborated on in Section 3.1.3.

3.1.2 Non-IT

This section presents the findings of the literature reviews with respect to the application of RM in a number of non-IT fields. The chosen fields are: insurance, healthcare, game theory, economics, politics and weather forecasting.

These fields have been selected based on their assumed applicability and added-value to this research of cyber-attacks. The fields vary greatly in their goal, but share a common theme in that effective and accurate Risk Management is of great importance. Each field is presented briefly below, with Table 3.2 summarising the findings.

Insurance

Insurance refers to an agreement an individual or organisation undertakes with an insuring entity that guarantees compensation for the eventuality of damage or loss. Organisations and individuals use insurance to safeguard against business, natural and political risks (Gordon, Loeb, and Sohail, 2003).

Insurance policies are a form of Risk Management (MacMinn, 1987) in the sense that they are used to provide cover against threats on both a private and professional level.

This review of insurance models focused primarily on car insurance. Other insurance models operate in a similar way in the sense that likelihood and impact is quantified using historical data. For example, the number of accidents in past years is used to determine the likelihood of a car accident over a certain period. The impact of a car accident is also quantifiable, with the maximum impact being the monetary value of the car, should it be written-off.

The different ways in which insurance companies handle risk by attempting to quantify the likelihood and impact of occurrences showed that insurance models are mostly simple, direct models. This characterises the insurance industry as it is relatively easy to calculate likelihood and impact estimates using hard data.

Healthcare

Healthcare refers to the maintenance or improvement of health through preventative, diagnostic or treatment techniques. The healthcare sector is often deemed as critical infrastructure due to the importance and high-risks of the work associated with it. Risk Management in healthcare is therefore aimed at analysing and reducing the *risk* of adverse events.

The likelihood that an adverse event occurs depends on the exact situation, but should be kept to a minimum due to the possible grave consequences. Impact is of even greater importance due to it's extreme forms in healthcare. It is difficult to quantify, but impact can result in the ultimate human sacrifice, death. Other forms of impact can be permanent medical conditions, financial costs or damage to the reputation of a healthcare facility.

An example of impact in healthcare would be a study by Vincent, Taylor-Adams, and Stanhope, 1998 in which "45% of patients experienced some medical mismanagement and 17% suffered events that led to a longer hospital stay or more serious problems" in hospitals in the United States.

The importance of minimising impact and likelihood, and how it is handled in healthcare was motivation to research the field. Although Risk Management in healthcare is improving, no concrete findings were deemed useful for the design of the framework

Game theory

Game theory refers to the study of models of strategic interaction between different parties. This literature review focused on the rational and logic between competing parties (decision makers) in chess game theory.

Game theory in chess involves two interacting parties, each with the goal of obtaining the best possible outcome from every move given a particular strategy. The likelihood that an event will occur is computable, but depends on many variables. These variables include the opposing party's current state and strategy.

Likelihood is based on computation and analysis, rather than historical data as other fields do. Impact in game theory is computable and is determined by a couple of variables; whether it is checkmate, or the value of the opponents piece taken. Analysing game theory provided extra insight into how impact and likelihood are determined by not simply using historical data (experience), but using patterns that are based on the strategy being followed.

Economics

Economics is the field concerned with the production, distribution and consumption of goods and services. Accounting for risk in economics is essential due to the importance and responsibility these organisations have in maintaining world order by providing a sound global financial environment.

Currently, financial organisations are exposed more to risk than in the past (Hellwig, 1995). Banks for example have the risk of having insufficient equity if income is low whilst they still have "obligations to its depositors are mostly independent of the returns which the bank earns" (Hellwig, 1995).

The negative impact in economics should be kept to a minimum and can be measured by a number of variables, the GDP growth for example, which is calculated based on a number of factors. The consequences of a banking crisis on an economy can be lasting, with Lehar, 2005 stating that "output falls by an average of 15–20% of GDP during banking crisis periods".

The likelihood of an event occurring in economics is complex to quantify due to the large number of factors that affect it. Cebenoyan and Strahan, 2004 mentions that banking is one of the only sectors in economics where such a large amount of risk is managed simultaneously.

Economics was researched the field lies close to the banking field, and that the incorrect estimation of risk and likelihood will have an impact on the world that spans beyond the banking and economic sectors. After analysis it was decided that economic RM concepts would not assist in reaching the goal of this thesis.

(geo)Political

Political risk describes the risk to an organisation's business strategy, objectives and finances (Kennedy Jr, 1988) that are affected by political decisions and changes. The definition of political risk varies across scientific literature, not necessarily limiting political risks to government entities, but to governance within an organisation as well (Kobrin, 1979).

An article by Deloitte (Deloitte, 2016) regarding the United Kingdom leaving the EU (Brexit) provides a clear example of how changes in the political landscape will come coupled with political risks that may be out of ones control. This example shows the difficulty in correctly determining impact and likelihood.

In order to account for political risk, an organisation (or government) needs to understand how political risk will impact business operations and profit, as well as strategy and business processes. Likelihood is extremely difficult to calculate due to the many variables that affect it. Both likelihood and impact are therefore difficult to calculate.

Weather forecasts

Weather forecasting refers to the application of science and technology in predicting weather conditions for particular locations and times. The field of weather forecasting involves the continuous calculation of likelihoods that a particular event will occur, and if necessary what the impact thereof will be.

Weather forecasting can therefore be seen as a continuous process of Risk Management. RM in weather forecasting is a highly uncertain and unpredictable field, with risks emphasised by the range of possibilities for any given weather forecast. To calculate impact and likelihood, weather forecasts use historical data of weather occurrences and incidents, as well as variables obtained from measurements of atmospheric conditions.

Risk Management in weather forecasting is therefore a "procedure for handling risks due to natural, environmental or man made hazards" (Plate, 2002). When determining risk in weather forecasting, the prediction itself, types of hazards (threats), impact and likelihood of the prediction occurring vary greatly. These are determined by the context in which they are applied. The impact caused by a hurricane for example may be more predictable and severe than that of a thunderstorm.

3.1.3 IT

The adoption of IT and reliance on digitisation, coupled with valuable data stored on these systems is incentive for intruders to execute an attack on IT systems. The inter-connected nature of computer systems that rely on each other for information-exchanges often introduces unintentional weaknesses and vulnerabilities that, until patched, form an additional risk of being exploited by a threat.

Managing this risk is an important activity due to the increasing value of information stored, as well as the reliance on processes that are conducted autonomously using computer systems. Risk Management is therefore an essential process to minimise "the probability and impact of IT project threats and capture the opportunities" (Alhawari et al., 2012).

Risk management in IT highlights the operational and economic implications of protective measures (Stoneburner, Goguen, and Feringa, 2002) to ensure the availability and integrity of IT systems and data. Illegal activity is often aimed at vital online systems and critical infrastructure, increasing the importance of correct risk estimation.

IT Risk management adopts a different approach to existing IT security and risk-handling protocols by enabling more efficient and effective sets of controls. Risk management can be seen as an alternative approach to handling risk that accounts for both IT and business aspects such as strategy and operational objectives without 'simply' implementing controlling policies.

It "allows IT managers to balance the operational and economic costs of protective measures and achieve gains ... by protecting the IT systems and data" (Stoneburner, Goguen, and Feringa, 2002).

Three RM concepts were introduced in Section 3.1.1. IT Risk Management supplements the three concepts from RM with two additional concepts. These are introduced below:

DEFINITIONS:

- **Threat:** Refers to an imminent danger for information or computer systems in which a a specific un(known) vulnerability is exploited (Dahbur, Mohammad, and Tarakji, 2011), whether it be intentionally or accidentally.
  Example - Intruders execute increasingly complex and targeted cyber-attacks worldwide which are difficult to prevent.

- **Vulnerability:** "Refers to a software, hardware, or procedural weakness that may provide an attacker ... [the opportunity] to enter a computer or network and have unauthorised

access to resources" (Dahbur, Mohammad, and Tarakji, 2011). A vulnerability describes a weakness or gap that can be exploited to gain access.
Example - A banking customer writes their access details for online banking on a piece of paper next to their shared computer.

Risk Management in IT was researched and analysed to obtain knowledge about how it is currently implemented in an IT context. This, together with knowledge from Section 3.1.2 will contribute to the design of the framework in Section 4.

3.1.4 Conclusion

Summary

In order to compare RM from the different fields effectively, a number of variables that are relevant for this thesis were identified. The table with the comparable results is shown in Table 3.2. The variables that are compared are described in Table 3.1.

Table 3.2 was populated using information from the literature review and experts. Multiple sources were used in order to ensure the accuracy and objectivity of the information collected.

Precautions were taken to minimise bias and subjectivity in the results, such as not mentioning the goal and approach of this research prior to hearing an expert's opinion(s). Furthermore the experts were explicitly requested to provide an objective opinion based on their theoretical knowledge and experience.

The literature review revealed that risk models vary greatly in nature, complexity and maturity. This variation comes down to their application in various fields, with a number of fields being significantly different to others in character but also their handling of risk.

All risk models, regardless of the field in which they are applied in, have impact (consequence) and likelihood (probability) components. These components are computed and evaluated separately, but are combined together to form a standard approach to analysing risk.

As was evident, the risk models differ greatly in complexity. This literature review concluded that weather forecasting and game theory, together with economic and (geo)political fields were most similar in nature to the IT risk modelling environment. Insurance applies a simple, direct approach to risk modelling, which differed the most from IT risk modelling.

In fields similar to (geo)political and economics, the occurrence of black swan (Taleb, 2007) phenomena are not well understood nor integrated into risk modelling. IT risk modelling experiences the same challenges in the sense that it is nearly impossible to take an unexpected event with its accompanying (significant) impact into account when calculating risk. 'Black swan' events primarily affect the impact component.

When determining total impact, the impact in weather forecasting is built up from several factors and managed in a structured and orderly manner. This is not the case in IT risk models, however impact in IT risk models would best be expressed in multiple components that together describe the full impact of an occurrence.

In general, quantitative likelihoods are difficult to calculate and can only be done when sufficient and reliable factual data is available. Taking car insurance as an example, the likelihood for a customer to be involved in a car accident is calculated based on the historical data available of the number of car accidents yearly for the total population of cars.

Deriving likelihoods for indirect concepts is more complex as likelihood variables tend to interact and depend on each other to give a full 'likelihood picture'. For the weather forecasting, game theory and economics fields, the relevance of likelihood variables and their contribution to the overall likelihood is the key differentiating factor that determines the quality of the entire risk model.

These likelihood variables and the total contribution to the likelihood has been developed over a number of years and is based on research and experience. The concept of patterns have

been introduced in risk models to integrate and work likelihood variables more effectively and accurately.

Conclusion

A lot can be learnt from the analysed models. A simple direct model (such as car insurance) can be seen as taking a flat approach to risk modelling in the sense that the likelihood is computed based on hard, factual data or derived from fixed threat-vulnerability components. This approach will not yield satisfactory nor desired results if applied to IT risk models.

When looking at quantifying likelihood, the absence or lack of sufficient incidents that are adequately analysed or categorised leads to the conclusion that likelihood quantification for IT risk models cannot be done yet. Merely deriving likelihood from categorised variables in the threat-vulnerability areas is too simplistic to achieve a reliable and robust IT risk framework.

The concept of introducing patterns as a way to group likelihood variables is therefore logical for IT risk models, similar to the application of patterns in weather forecasting and game theory. However, nuances in patterns are challenging to identify and map. Due to a lack of reliable input data, a coarse-grained approach must be used to map patterns, an approach that can be refined and improved over a period of time to achieve better mapping results.

Unexpected, black swan occurrences need to be addressed in order to accommodate, to some extent, the impact such occurrences will have on the overall risk determination. This research suggests introducing an impact concept that takes the variance of impact into account, in doing so producing a more accurate impact estimate per occurrence. Section 4.3.2 will introduce this concept, termed the O-factor.

Based on this research and analysis, the researcher determined the most applicable concepts came from risk management in the weather forecasting and game theory fields. The manner in which likelihood was determined by using patterns, or impact variance was handled by identifying a number of influential variables is of added value in working towards achieving the goal of this research.

TABLE 3.1: Description of variables for analysing risk in other fields

	Measure	Description
Computational complexity	High/Med/Low	The computing power needed to calculate variables and build the model.
Chaos leniency	High/Med/Low	How complex, fuzzy and complicated the field is.
Ability to quantify impact	Easy/Med/ Difficult	The ease at which impact can be calculated.
Nr. impact variables		The number of variables that are taken into account in calculating the impact.
Impact variables complementary	Yes/No	Whether a relationship exists between the impact variables.
Likelihood computable	Yes/No	Is it possible to calculate/quantify likelihood in this field.
Nr. likelihood variables		The number of variables that are taken into account in calculating the likelihood.
Pattern concept relevancy	Yes/No	Do patterns exist or emerge in this field.
Theory available	Yes/No	Is there an abundance of sufficient, reliable theory available.
Maturity	High/Med/Low	How mature or advanced is the field.

TABLE 3.2: Results of the analysis of risk in other fields

	(car)Insurance	Weather Forecasting	Healthcare	Game theory	Economic	(geo)Political	IT Risk
Computational complexity	Low	High	Medium	Medium	Medium	Medium	Medium
Chaos leniency	Low	High	Medium	High	High	High	High
Ability to quantify impact	Easy	Difficult	Easy	Medium	Difficult	Difficult	Difficult
Nr. impact variables	2	Many	1	2	1	2	Many
Impact variables complementary	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Likelihood computable	Yes	Yes, difficult	Yes, difficult	Yes	Yes, difficult	Yes, difficult	Yes, difficult
Nr. likelihood variables	2	Many	2	Many	Many	Many	Many
Pattern concept relevancy	No	Yes	No	Yes	Yes	No	Yes
Theory available	Yes	Yes	Little	Yes	Yes	Yes	Little
Maturity	High	High	Medium	High	High	Medium	Low/Medium

3.1.5 Cyber-attacks

Introduction

As mentioned in section 1, the world is changing at an incredible pace. More tasks, processes and the exchange of information are carried out online, with interactions taking place between systems running on inter-connected devices. This very inter-connectivity leads to more channels and directions in which cyber-attacks can manifest (Choo, 2011), in doing so making it harder to predict them. A criminal activity carried out online and directed to an IT system will be referred to as a cyber-attack.

Inter-connectivity and relationships between devices, combined with the increased importance, availability and value of information on systems located on these devices offers added incentive for intruders to carry out criminal activities. Creating uncertainty and chaos, coupled with the hunger for increased fame and acknowledgement are other motivations for intruders. To complicate matters further, the manner in which intruders execute cyber-attacks continues to become more invasive, complex and targeted (Choo, 2011), with their effectiveness and reach increasing.

In the past, criminal activities would be of a physical nature. However a shift has taken place as many organisations and governments now see cyber-attacks as credible threats; the United States has labelled cybersecurity as a major security concern (Choo, 2011). An example of critical infrastructure succumbing to intruders, and the effects of the cyber-attack, are well elaborated on in Case, 2016. Intruders gained unauthorised access to the Ukranian power grid and shut down substations which led to a 3 hour loss of electricity for 225,000 residences.

One of the most far-reaching cyber-attacks in recent times was an attack that took place in 2017, affecting 230,000 computers in 150 countries (Ehrenfeld, 2017). The cyber-attack, named WannaCry, was a form of malware that encrypted all files on a computer system till a ransom payment had been completed.

In the banking sector, banks that carry out international banking transactions using the SWIFT network are regular victims of cyber-attacks. The Bangladesh Central Bank lost $101 million in a cyber-attack using their SWIFT information in 2016 (Camillo, 2017); the attackers initially aimed to transfer $1 billion. The different types of cyber-attacks, when they occurred and attack vectors will be discussed later in this section.

Definition

Various definitions of cyber-attacks exist in different fields, with applications ranging from ICT to law environments. Three contrasting, yet comprehensive definitions of cyber-attacks are:

- 'A hostile act using computer or related networks or systems, and intended to disrupt and/or destroy ... cyber systems, assets, or functions' (Hathaway et al., 2012)
- 'An act in cyber space that could reasonably be expected to cause harm,' with harm defined as, amongst others, economic, physical and reputational implications (Robinson, Jones, and Janicke, 2015)
- 'Deliberate actions against data, software, or hardware in computer systems or networks. The actions may destroy, disrupt, degrade, or deny access' (Denning and Denning, 2010)

In the interest of this research, the formal definition of a cyber-attack that will be applicable throughout this research is:

Definition: A *cyber-attack* is an action executed by an (unauthorised) individual or group with a clear intention of modifying, disrupting or disabling the operations of computer systems or networked devices in an illegal manner.

This thesis will refer to unauthorised individuals or groups carrying out illegal activities with harmful intent as *intruders*. Figure 3.1 provides a high-level illustration of interactions between individuals and computer systems through various channels that exchange information through the internet.

An analysis of the types of attacks revealed that cyber-attacks can have different origins, namely internal or external. Internal attacks, better known as insider attacks, are instigated by an individual that has (authorised) access to the system or resource being attacked. The attack therefore comes from within a trusted network of individuals.

External attacks on the other hand are initiated by individuals that do not have access to the system, therefore from outside the trusted network of individuals. Due to the limited time frame and scope, this research thesis will exclude insider (cyber) attacks.

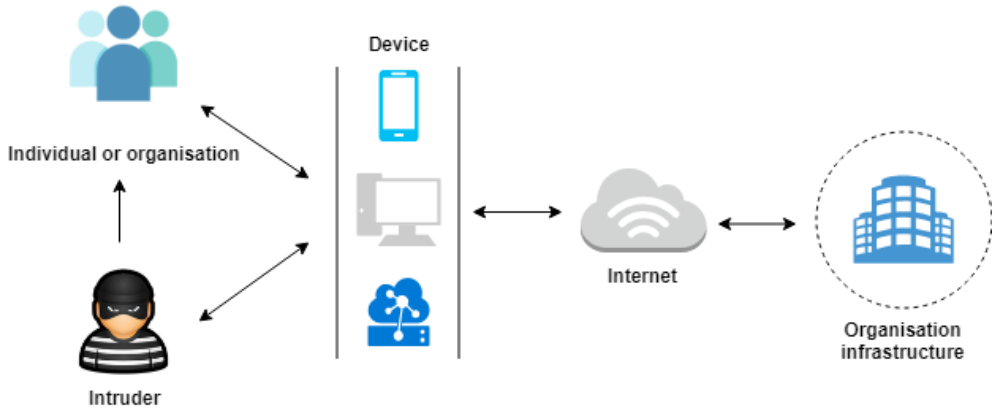

FIGURE 3.1: Basic view of the components of a cyber-attack

Attack form

When carried out, cyber attacks can take two forms, namely; targeted or un-targeted attacks. NCSC, 2016 states that a targeted attack occurs when the attacking entity has 'a specific interest' in an individual or organisation or has received a monetary reward to do so.

The victim of a targeted attack has therefore been specifically selected by the attacker and is often the subject of an attack tailored (Laszka, Johnson, and Grossklags, 2013) to their computer systems or processes. An attack directed at a Russian bank in 2017 by the hacker group Cobalt through the SWIFT system is an example of a successful targeted attack (*The Hi-Tech Crime Trends* 2018).

An un-targeted attack is the occurrence of a coordinated and planned, yet un-directed attack. The individuals carrying out the cyber-attack use a range of techniques that abuse the freedom provided by the internet to 'indiscriminately target as many devices, services or users as possible' (NCSC, 2016).

An example of the abuse of internet freedom is whereby attackers (randomly) scan the ports of accessible servers on the internet (or an internal network) for vulnerabilities in a protocol or an implementation thereof (Khurana et al., 2010). Singh and Tomar, 2015 observe that 50% of attacks that take place are initiated in an un-targeted manner through scanning activity with malicious intent.

This research will focus on attacks that *target* organisations, or customers therefore, in the banking sector.

Attack method

Cyber attacks can be described by the way in which they operate and exist, described by Kong, Hong, and Gerla, 2003 as having very different goals; passive or active.

A passive attack describes an attempt by an intruder to gain access or intercept data in a stealthy manner (Pawar and Anuradha, 2015), by doing so being 'as invisible as possible' (Kong, Hong, and Gerla, 2003). An active attack is described by Padmavathi and Shanmugapriya, 2009 as an intruder's repeated efforts to actively gather information or gain unauthorised access.

Passive and active attacks can therefore lead to similar results. Literature revealed that recent attacks often make use of active methods as opposed to passive methods. Passive methods were more prevalent in the past. This research will focus on both active and passive attacks on institutions in the banking sector.

Attack motivators

To carry out a cyber-attack, an intruder generally tends to have a reward as motivation to execute it. The types of rewards vary greatly, but the end-goal is similar; to cause some form of harm to the victim's credibility.

This literature review uncovered the motivations that are presented and described briefly in Table 3.3.

TABLE 3.3: Possible motivation for an intruder to execute a cyber-attack

Motivation	Sub-motivation	Reason
Fame		Gain recognition for the achievement.
Uncertainty	Credibility	Damage or raise doubt in an entity's reputation.
	Chaos	Cause confusion, de-stability or disruptions.
Retribution		Retaliation for an attack or other reason.
Redistribution		To sell or distribute information collected.
Financial reward		Financial incentives from another entity.
Theft	Monetary	Steal funds, directly or indirectly.
	Information	Collect, alter or destroy valuable information.
	Intellectual property	Gather secret (non-public), valuable information.
Ethical		Discover vulnerabilities with good intentions.
Political		Retribution for a political occurrence, or gaining knowledge.

The OSI Model

As explained in Briscoe, 2000, the Open Systems Interconnection (OSI) model is an abstract representation that describes how applications can communicate, standardising (tele)communication between networked computer systems.

It is a 7-layer model that assists in information exchange by splitting "complex networks into manageable pieces that can be easily understood" (Handel and Sandford, 1996) through a generic set of protocols.

Data packets "descend and then re-ascend the layers" (Briscoe, 2000) of the OSI model during communication between systems, each layer carries out distinct functions. Figure 3.2 shows movement between layers and Table 3.4 describes the corresponding layers.

The OSI model was analysed to establish which layers cyber-attacks take place in, or target, and how they affect the layers. Cyber-attacks go through all 7 layers of the OSI model, but primarily target and affect the Application layer as it has the most interaction with users.

The decision was made not to use the OSI model layers as vulnerable areas that threats may target in the channel between a user and a bank. This was based on the finding that attack threats merely move through the 7 layers of the OSI model, rather than target a layer.

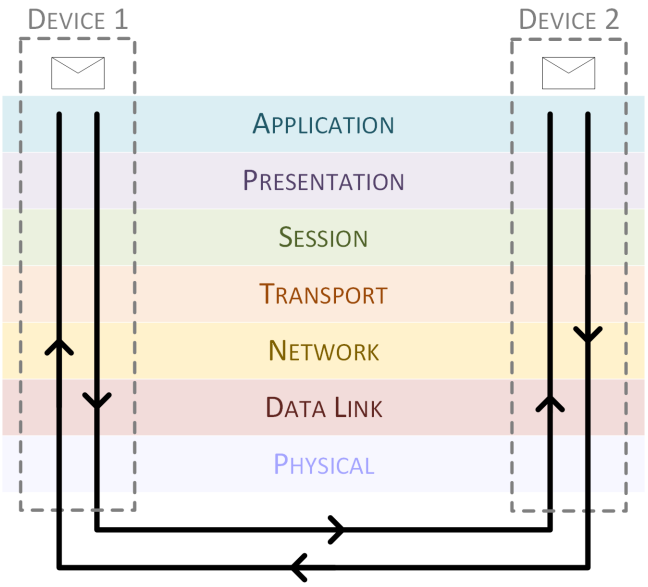

FIGURE 3.2: Data flow between two communicating devices by means of the OSI model

TABLE 3.4: Description of layers of OSI Model

Layer		Description
Nr.	Name	
7	Application	Together with users, interacts with software applications. Implements a communication component determining resource availability and synchronisation.
6	Presentation	Translates network and application formats by mapping different syntax and semantics. Transforms data into a form that an application accepts.
5	Session	Controls connections between computers by establishing, managing and terminating connections. Closes sessions when transfers are complete.
4	Transport	Controls and ensures the reliability of a data flow from source to host by tracking data and re-transmitting data that was transferred unsuccessfully.
3	Network	A medium that allows for many nodes to connect and transfer messages, providing the functional procedural means of transferring data sequences.
2	Data link	Provides direct data transfer between two nodes by defining the protocol to establish and terminate connections. Detects and corrects errors that occur in the physical layer.
1	Physical	Responsible for the transmission and reception of unstructured raw data. Converts data bits into signals (electrical, radio or optical).

Control frameworks

A framework is an underlying structure that supports and guides an individual through the steps of a concept/system. This literature review focused on three of the most relevant and applicable (control) frameworks available in the cyber-security sector.

NIST

Table 3.5 illustrates the core functionality of the NIST framework[1], with each function describing a collection of tasks and activities to accomplish an organisation's cyber-security goals (Cybersecurity, 2014).

TABLE 3.5: Core functions of the NIST Framework

Function	Description
Identify	Develop an understanding to manage cyber-security risk to people, systems, processes data. Used to understand the business context and related cyber-security risks, enabling task prioritization.
Protect	To develop and implement appropriate precautionary measures aimed at limiting (mitigate) the impact of a potential cyber-security incident.
Detect	This function aims to develop and implement tasks to identify a cyber-security incident, allowing for their timely discovery.
Respond	Develop and implement tasks aimed at taking action when an incident is detected. This function assists in limiting the impact of a cyber-security incident
Recover	Develop and implement appropriate tasks to restore services or functions that were affected by an incident. It supports timely recovery to normal operations after a cyber-security incident.

Each functional group consists of tasks split into categories and subcategories, complimented with informative references to standards, guidelines and common practices that assist in achieving their goal. In addition, NIST introduces a 4-tier scale that describes the sophistication in cyber-security risk management practices, assisting in determining to which extent risk management is informed by business needs (Cybersecurity, 2014).

The framework makes use of a standard notation to collect, analyse and present "cybersecurity risk to internal and external stakeholders" (Cybersecurity, 2014). It is aimed at providing a flexible and cost-effective approach (Cybersecurity, 2014) to improve infrastructure security and protection through various measures and controls.

ISO 27001

The ISO 27001 is an internationally-recognised security standard that aims to increase control and oversight in an Information Security Management System (ISMS) by listing a set of requirements which an organisation can use to devise or validate their security protocols (Disterer, 2013). The current version of the standard was last updated in 2013.

According to Gartner[2], the standard is a legal framework for aligning information technology and operational technology, providing guidance for new and existing cyber-security programs.

[1]NIST website: `www.nist.gov/cyberframework`

[2]A market analysis and advisory company: `www.gartner.com/en`

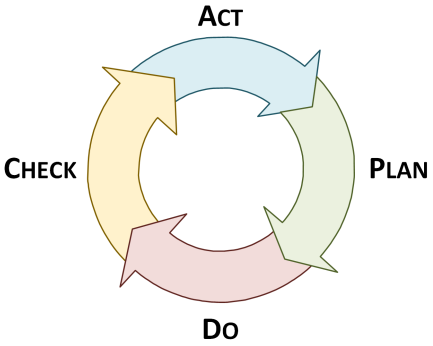

FIGURE 3.3: The PDCA model: Cycle used by ISO 27001

Disterer, 2013 further explains that ISO 27001 follows the PDCA (**P**lan, **D**o, **C**heck, **A**ct) cycle as shown in Figure 3.3 and described in the context of the ISO 27001 in Table 3.6. An essential step in the process is that "risks should be identified ... and control objectives should be defined". Process performance is reviewed and audited relative to the pre-defined set of ISMS controls and policies, which should allow for further improvements in terms of compliance with security objectives.

The ISO 27001 framework consists of 39 control goals and 134 measures that need to be implemented for sufficient security management (Disterer, 2013). The measures should be adjusted and improved continuously, whilst ensuring that the procedures and policies in place are constantly monitored and satisfied.

TABLE 3.6: The PDCA cycle described in the context of ISO 27001

Step	Description
Plan	Establish the ISMS objectives, policies, controls processes relevant to managing risk and improving information security.
Do	Implement and operate the policies, controls, processes of the ISMS.
Check	Monitor and assess process performance against the ISMS controls, objectives and policies. Report results to management.
Act	Bases on the ISMS, management audit and review, maintain and improve the ISMS by taking corrective and preventative actions where necessary.

This research analysed both the NIST and ISO 27001 control frameworks to learn about their implementations and what they entail. Concepts from both frameworks, the functional groups from NIST and the PDCA cycle from ISO 27001, and their attributing functions will be taken forward in the design of this thesis' risk modelling framework.

COBIT

Another framework that was researched during this thesis was the COBIT framework. COBIT is the "most renowned framework for support of IT governance concerns" (Simonsson and Johnson, 2006) that "helps businesses develop, organise and implement strategies around information management and governance" (White, 2019).

COBIT is a control framework that addresses governance, technology and security needs. The COBIT Core Model consists of 40 governance goals (Simonsson and Johnson, 2006) that uses provides metrics and maturity models to measure an organisation's capabilities and performance in reaching their goal.

The COBIT framework has 5 principles that are applicable to organisations of all sizes, these principles are illustrated in Figure 3.4.

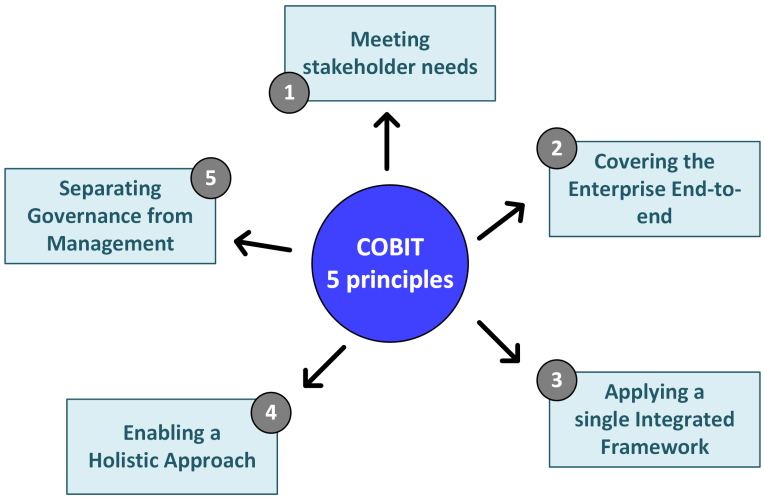

FIGURE 3.4: 5 principles of the COBIT model

Although COBIT offered additional insights for this thesis, the framework will not be used moving forward due to the emphasis on governance and security, without looking specifically at the risk component of the security challenges.

Channels

Businesses, governments and organisations are expanding the services provided on their online platforms. Technological advances and innovations broaden the possibilities with regards to ways through which these platforms can be accessed; these possibilities will are often referred to as channels. Channels can also be interpreted as lines of communication to the bank.

However advantageous the large choice of channels at our disposal are, without adequate security measures, they become vulnerable and susceptible to cyber-attacks. These channels in the banking sector are of no exception and therefore need to be well protected and monitored to ensure the integrity of banking systems and availability to all stakeholders involved. Table 3.7 presents the channels identified.

TABLE 3.7: Channels through which banks can be accessed

Channel	Description
ATM	Devices providing cash and transaction services (Adeoti, 2011).
POS	Payment devices in places of business.
Website	Banking portals that provide online services.
Mobile application	A portal developed specifically for mobile devices.
Smart devices	Banking services through alternative (ICT) devices.

The POS and ATMs channels are susceptible to various types of security breaches, ranging from social engineering techniques to infecting the software designed to run on the devices (Choo, 2011). Attacks on POS and ATM devices are mainly for fraud purposes (Adeoti, 2011), to steal money, or collect valuable card information (Choo, 2011). Choo, 2011 dives further into smart devices as an emerging attack channels; applications running on mobile devices such as tablets, and (voice-enabled) virtual assistants. The ability to access a Rabobank account through Google assistant is an example of a virtual assistant.

Dimensions

During the literature review phase, the possible dimensions of cyber-attacks were collected and analysed. The dimensions were filtered and cross-checked with experts who were able to verify the relevance of the dimension within the context of a bank. The dimensions deemed relevant to cyber-attacks on banking institutions are described in Table 3.8.

TABLE 3.8: Cyber-attack dimensions for banking institutions

Dimension		Description
Impact	Operational disruption	The amount of, and severity of interruption the cyber-attack has caused.
	Damage to reputation	The damage done to the bank's credibility due to the cyber-attack in the eyes of the community.
	Financial implications	The monetary cost the attack inflicts in terms of getting back to normal operations.
	Economic cost	The financial cost caused due to, amongst other reasons, the downtime or reduced performance.
	Legal consequences	The legal, regulatory and compliance impact an attack will have.
Threat		The danger of a vulnerability being exploited.
Mitigation costs		The cost of implementing measures to reduce the severity of weaknesses and attacks.
MTTR		The average time taken to recover from a cyber-attack.
Likelihood		The probability that an attack will occur.
Geopolitical		Tension and conflict in the geo-political climate can influence/motivate cyber-attacks.
Risk		The potential of an incident in which a threat exploits a vulnerability.
Journey		The path an attack takes from attacker to the intended goal.
Attack complexity		The level of intricacy and complication of a cyber-attack.
Cost to execute		The financial cost to carry the attack out.

The majority of the dimensions discovered turned out to be various forms of impact on a banking institution. This research will analyse how dimensions and attack vectors (explained in Section 3.1.5) affect each other.

Attack vectors

During the literature review, attack vectors were analysed and filtered according to relevance to banking institutions. An *attack vector* is a way in which an intruder can gain access to a IT system in order to carry out a malicious activity.

Table 3.9 lists the attack vectors that have have been classified as relevant for this thesis. A brief description of each attack vector is also included.

TABLE 3.9: Overview of attack vectors a banking institution is susceptible to

Attack vector	Sub-attack vector	Description
DDoS		A cyber attack whereby the objective is to disrupt the operation of a system to a point that it is unable to function normally, or be completely unavailable. This form of attack often uses computers infected with malware to send disruptive traffic to the computer hosting a system being attacked.
Ransomware		A form of malware that encrypts all information on a computer, or locks the victim out, till a ransom payment has been made.
Malware	Viruses	Malicious software that, when activated, replicates itself by modifying applications (adding its own code) in order to gather information or cause harm.
	Worms	Self-replicating malicious software that exploits vulnerabilities in applications and operating systems to severely affect performance and reliability.
	Trojans	An attack form in which malware nests itself in a normal application, in time installing other applications, collecting, modifying, destroying or stealing information.
	Hybrids	A combination of malicious applications that, once activated, spreads through a network to other computers.
	Adware	Delivers advertisements (often in the form of pop-ups) that exposes the victim to unwanted, malicious advertisements.
	Spyware	An application that stores and collects information such as keystrokes, screen captures and data from the victim without their knowledge. Information collected is often of a personal nature.
	Rootkit	A malicious application that is installed without the knowledge of the victim, allowing the intruder to remotely access or take control of a computer system.
Social engineering	Human error	An attack whereby an individual accidentally creates an opportunity, or introduces a weakness, in a system that is susceptible to exploitation by an intruder.

	Credential misuse	The reuse (accidental or intentional) of credentials for multiple websites, storing credentials in shared locations, or the continued use of standard passwords (e.g. admin, admin). Once obtained, the credentials can be misused by intruders.
	Phishing	A cyber-attack whereby an intruder acts like a trustworthy entity in an attempt to gain the trust of the victim in order to steal personal data. The intruder often acts getting the user to (unknowingly) visit a particular website or open a file containing malicious code.
	Spoofing	An attack whereby an intruder or automated program (successfully) acts as another individual to gain unauthorised access to a system in order to alter or destroy information.
	Baiting	An intruder entices the victim to pay money or give up personal information by offering a product or service in return.
Fabrication		The intruder inserts forged objects into the systemwithout the victim's knowledge or involvement.
Sniffing		An attack using a specific application to monitor and intercept network packets as they are transferred over a network. Intercepted packets are analysed by intruders to detect if there is unencrypted information.
Stealing		A cyber-attack that is aimed at stealing valuable information or funds from the victims' system without their knowledge. Stealing generally involves using social engineering or malware as a form to gain access.
Hacking		Refers to a cyber-attack whereby an intruder finds a weakness in a computer system and gains access to alter or destroy an application or steal information.
Man-in-the-middle		An attack where an intruder intentionally monitors, intercepts and (often) alters information transferred between communicating entities. This action is done without the communicating entities having knowledge about it.
Access	Unauthorised	An attack in which an intruder attempts to gain access to a system or service that they do are not entitled to.
	Unauthenticated	An attack whereby vulnerabilities are sought for in networked systems that can be accessed without logging in as an authorised individual.
Vulnerability exploit		A weakness or vulnerability in an application or system that has been introduced intentionally or accidentally that allows for abuse by an intruder.
Zero-day		An attack on a software vulnerability found at the core of an application or system in which malware is installed. A zero-day is a critical weakness in a system that requires immediate fixing by developers before a zero-day cyber-attack can be launched.

3.1.6 Other

CORAS

CORAS is a method for carrying out security risk assessments and analyses using a customised language for threat and risk modelling.

The framework consists of guidelines that explain how the language should be used to identify and analyse risk by using a framework-specific tool to document and report the risk analysis results.

The CORAS method consists of five sub-processes to determine and account for risk (Fredriksen et al., 2002). The sub-processes are described in Table 3.10 (Fredriksen et al., 2002). The sub-processes are carried out in a sequential manner, with each sub-process building on the results of the previous one, as shown in Figure 3.5.

TABLE 3.10: CORAS sub-processes described

Sub-process	Name	Description
1	Context Identification	Identify the domain-specific context the analysis will be carried out in, in doing so identifying the usage scenarios.
2	Risk Identification	Identify the threats and vulnerabilities of assets.
3	Risk Analysis	Determine the impact and likelihood that a threat on an asset will cause.
4	Risk Evaluation	Identify the risk associated with threats that have been identified.
5	Risk Treatment	Address the treatment of the identified risks.

The method of risk analysis by the CORAS framework proved useful for this research. The steps taken for identifying risk (sub-processes 1 to 3) were inspiration for this research thesis' design principles and decisions.

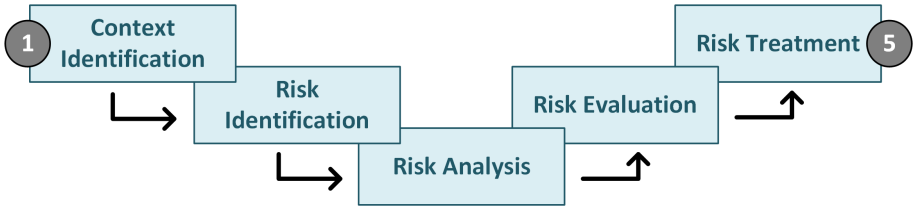

FIGURE 3.5: The flow of CORAS sub-processes

3.2 Practical Review

The literature review in Section 3.1 was the main source of information and theory for the Problem Investigation phase of this thesis. However, experts were consulted to gain additional insight into various concepts from literature, to hear an expert's practical experience and opinion about the concepts from theory.

Experts at BankY were spoken to, as well as external experts from outside the banking sector. This was in order to increase the objectivity of the framework and therefore reduce possible bias introduced by information from experts from BankY. External experts included independent experts, as well as experts that work at other companies.

Table 3.11 shows the different functions of experts that were consulted.

TABLE 3.11: Professions of experts that were consulted

Function	
Information Security Officer	Lead for Digital ID fraud prevention
(lead) Business Architects	Product Owners
Risk Experts	Solution Architects
Red Team head	Threat-incident Analyst
Security Specialists	Cyber-security Analysts
Lead Architects	Meteorologists
Developer	Cryptography expert

3.3 Conclusion

The literature and practical review revealed important concepts and insights, as well as verified existing knowledge. Scientific articles, grey literature and talks with experts proved to be invaluable sources of information.

The review into risk management concepts produced interesting insights and concepts from other fields that this research uses moving forward. The use of patterns in weather forecasting and game theory to model likelihood, as well as the concept of accounting for variance to determine impact were the most interesting findings that were obtained from other fields and used in this research.

A comparison between 6 other fields where risk management is applied indicated that not all models are reliable enough to use for risk management in IT. Insurance models for example have a simple, direct approach to modelling likelihood and impact that would not be sufficient for modelling risks in IT in a accurate manner. The literature review illustrated that different definitions for risk management concepts exist, with the definitions of *threat*, *vulnerability*, *likelihood*, *impact* and *risk* depending on the field within which it is applied.

The literature review into cyber-attacks and their characteristics led to valuable information. It showed that cyber-attacks existed in various forms, with some attacks taking place in a passive and unsuspecting manner whilst others took a more (pro)active approach. Cyber-attacks can have specific targets (victims), which is often influenced by the attacker's motivation or rewards.

Further research showed that various attack types and vectors exist, which when looking at their intended target, affect the attack's impact (consequence). The general channels that customers can use to access banking services, channels, were identified analysed.

Various control frameworks were researched such as NIST, ISO27001, COBIT and IS031000, as well as the risk analysis framework CORAS. These frameworks complemented existing knowledge about cyber-attacks, security and risk concepts, and influenced the design principles of the research's framework.

Chapter 4

Framework design

This chapter elaborates on The Treatment Design (Wieringa, 2014) phase of this master thesis by incrementally describing the procedure and steps taken in designing the framework. The design decisions made, and their motivation, will be explained in this chapter.

4.1 Introduction

Treatment Design is the second of three phases in the Design Cycle (Wieringa, 2014). The Treatment Design builds on knowledge obtained from the Problem Investigation phase, where a literature and practical review was carried out.

The knowledge is then used in conjunction with the research's main goal to design an effective, useful and reliable artefact. Therefore the Treatment Design phase involves specifying the requirements of the artefact that will be designed, as well as how these requirements will contribute to the main goal of the research.

The validation of these requirements is explained in Section 6. Expert reviews is an effective validation method (Wieringa, 2014) and will be used as the principle validation method.

Existing treatments and artefacts are observed and noted during the Problem Investigation phase. Depending on the specified requirements, existing treatments and/or artefacts may contribute to the design of a new artefact. A simple illustration of the explained procedure is shown in Figure 4.1.

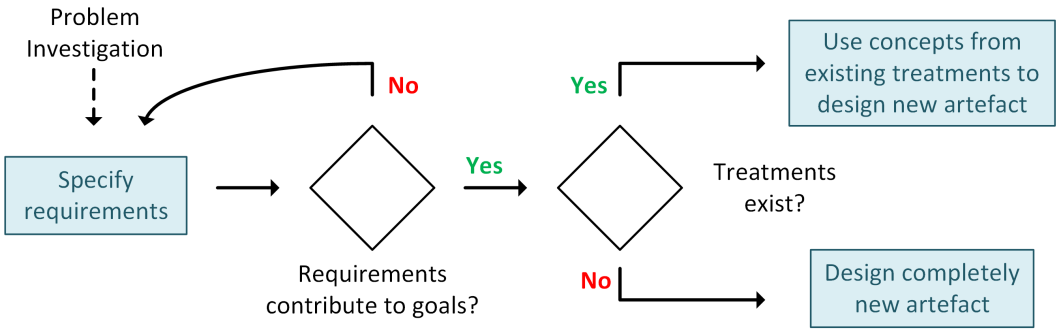

FIGURE 4.1: Procedure to determine treatment

4.2 Goal

The main goal of this research is introduced and explained in Section 2.1 along with the research questions that contribute to the goal. A reminder of the goal is:

MAIN GOAL:
To design a multi-channel cyber-attack patterns-based risk modelling framework for the banking sector.

A framework is therefore the type of artefact that will be designed in this thesis. The requirements for to-be-designed artefact are based on information from the literature review and expert opinions.

These requirements are as follows:

- Design a comprehensive and self-explanatory framework for the banking sector that takes threats, vulnerabilities, likelihood and impact into account when determining the risk of cyber-attacks.
- Introduce the concept of patterns as a way to model and categorise the likelihood of cyber-attacks targeting banking institutions.
- Determine essential impacts types and values to take into account per cyber-attack pattern.
- Identify the factors that affect the level of impact (impact variance) cyber-attacks have on banking institutions.

The framework design will consist of three matrices: a likelihood matrix, impact matrix and risk matrix. The order in which each matrix was designed is illustrated in Figure 4.2.

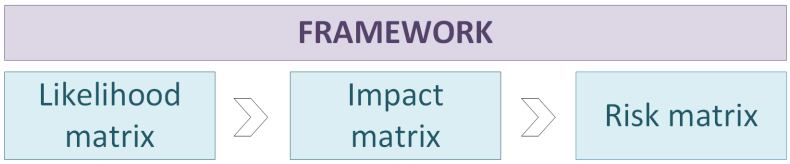

FIGURE 4.2: Steps followed for designing the framework.

4.3 Design Principles

This section will explain the components of the framework along with the reasoning, based on the literature and practical review, behind component design decisions.

The literature review in Section 3.1 illustrated five concepts that are of great importance in IT Risk Management: threat, vulnerability, likelihood, impact and risk. These were described and elaborated on in Section 3.1.1.

The concepts mentioned from risk management are related and expressed in the two formulae listed below. Formula 4.1 expresses risk, whereas formula 4.2 describes how likelihood is calculated.

$$risk = likelihood \times impact \tag{4.1}$$

$$likelihood = f(threat, vulnerability) \tag{4.2}$$

In literature, the likelihood formula (Formula 4.2) is commonly denoted as $likelihood = threat \times vulnerability$. This is done purely for simplicity purposes. This thesis defines likelihood

slightly differently. Based on literature, a relationship was found to exist between threat and vulnerability. This was however not simply the product of both concepts, but rather a function of the two as shown in Formula 4.2.

With the main goal of this thesis set to design a risk modelling framework, a logical decision was made to use the risk and likelihood formulae as a basis for designing this framework. The different variables in both formulae are obtained and analysed separately, but together contribute to determining total risk.

Therefore this thesis researched and analysed the various concepts of both formulae in order to obtain a valid and comprehensive perception of risk for cyber-attacks in the banking sector. The steps taken to design the framework are explained per step in this section.

Figure 4.3 provides a visual illustration of the aforementioned procedure that is derived from Formula 4.1 and Formula 4.2.

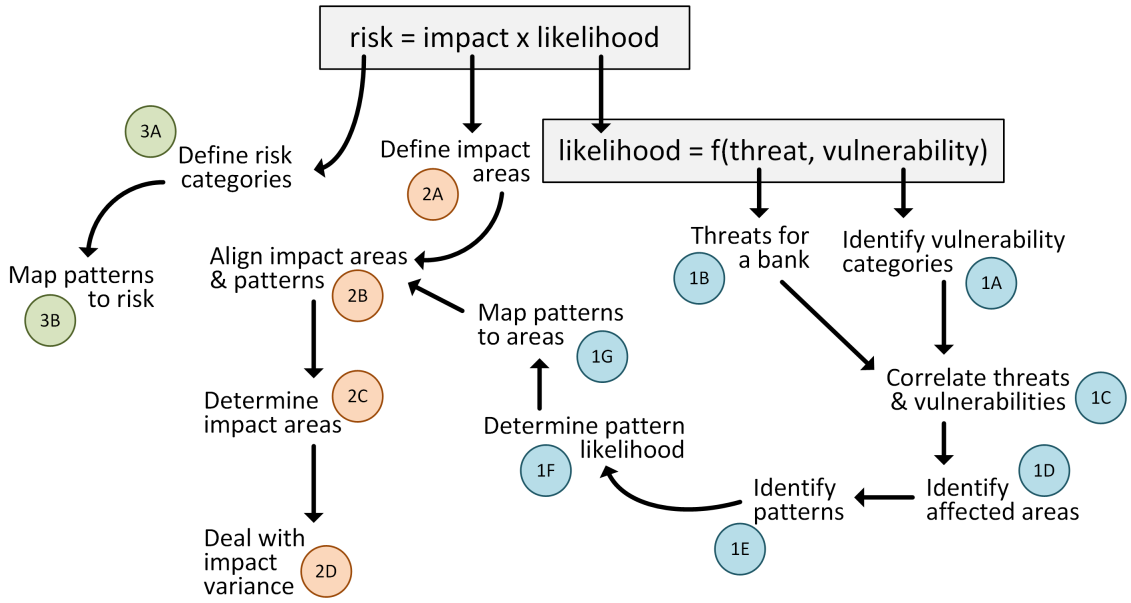

FIGURE 4.3: Outline of steps taken to design the framework.

4.3.1 Likelihood

This section will elaborate on the procedures shown as 1[*] from Figure 4.3 to determine the likelihood component of the framework.

1A: Identify vulnerability categories

As Formula 4.2 shows, vulnerability is a component used to determine the likelihood. Therefore it is of great importance to identify areas within the scope of the research that are vulnerable to cyber-attacks. This represents the goal of step 1A in the design.

The literature review analysed areas in which communication takes place between the user and a bank, which typically involved some form of data transfer. Whitepapers and publications by security companies were a vital source of information as they have a similar, generic approach to modelling the architecture channel of external-facing organisations. This resulted in the design of a channel between the user and a bank.

This approach was further validated with experts during the practical review and, although each organisation's architecture differs, a generic, high-level architectural channel was defined and is shown in Figure 4.4.

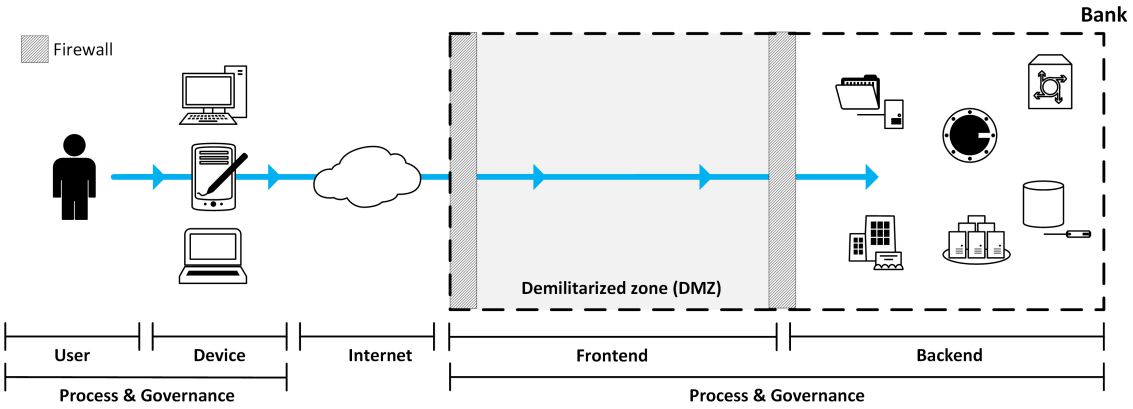

FIGURE 4.4: View of the channel between the customer and a bank.

The components in Figure 4.4 are described in Table 4.1. As Figure 4.4 shows, the channel contains seven components; three of which (*user*, *device* & *internet*) a bank has no direct control over. The *frontend* typically contains a Demilitarized zone (DMZ) which is used as a location to provide non data-critical application services to external entities, forming a 'buffer' between the external entities and critical banking infrastructure found in the *backend*.

A DMZ is a term used throughout the IT industry to describe an architectural concept whereby a network (sub network) is created within an organisation's IT infrastructure that logically separates an internal network from other (untrusted) networks, such as the internet. This is definition is based on Stoddard, 2012 and expert opinions.

TABLE 4.1: Definition of components between a customer and a bank

Name	Description
User	An individual attempting to access a banks systems.
	E.g. Alice, Bob, John Doe
Device	The object with which the **user** is attempting to access banking systems.
	E.g. Laptop, desktop, tablet, smartphone
Internet	The media through which the customer's **device** is connected with a bank.
	E.g. Internet exchanges, routers, cable-infrastructure
Process	The predefined (by**governance**) procedure to carry out tasks and activities.
	E.g. A verification code is sent to the customer's phone for a password reset
Governance	Policies and decisions by management about infrastructure and **processes**.
	E.g. A user needs to be verified before the password reset process can start
Frontend	Applications for preventative measures and non-data-critical functions.
	E.g. Firewall, load balancer, honeypot, web server
Backend	Critical data and core banking applications and infrastructure.
	E.g. Databases, virtual machines

Once identified, the vital components in the channel were mapped as categories of vulnerabilities for the framework, vulnerable areas. Vulnerable areas refer to targets of cyber-attacks that are susceptible to compromise. The identified categories are therefore derived from components in the channel between the user and a bank. The categories form an axis in the likelihood matrix, which will be explained in due course. This axis is shown in Figure 4.5.

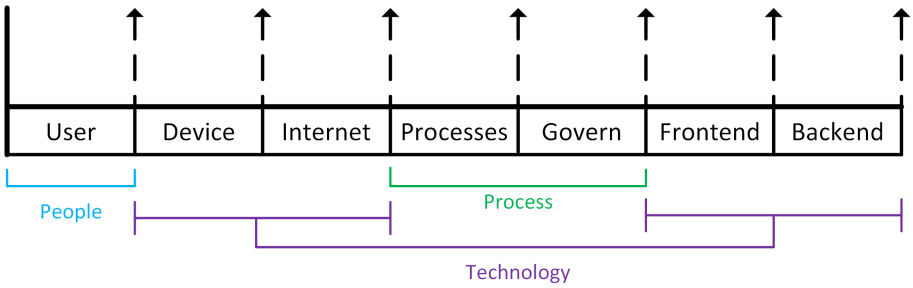

FIGURE 4.5: Vulnerabilities in channel between the user and a bank

Figure 4.5 shows the identified categories of vulnerabilities on an axis, as well as a mapping of these to the 'People, Process and Technology' theory. This theory emphasises the importance of correctly accommodating for the user's needs, business goals and processes, as well as the IT capabilities (Chen and Popovich, 2003) in an organisation's set up.

1B: Threats for a bank

The threat component in the likelihood formula (Formula 4.2) involves identifying attack vectors by which a vulnerability can be exploited. This step in the design process explains the identification of threats that target banking institutions.

The literature and practical review formed the basis for the identification of these threats. Initially, threats targeting banking institutions were analysed, however this was later widened to include threats that indirectly affect banks. For example, threats that target internet communication infrastructure (AFP, 2019) indirectly affect a bank. The findings of the literature review into attack vectors were presented in Section 3.1.5.

Both reviews resulted in the identification of threats with different levels of complexity; this varied from detailed, implementation-level threats to more general, abstract threats. In order to correctly analyse and compare them, the threats were grouped and categorised by type.

Table 4.2 contains explanations of each threat category, which is based on the attack vectors from Section 3.1.5. The various threats were categorised together based on their behaviour/journey as well as their goal/motivation. For example, social engineering from Table 4.2 covers a wide variety of attack vectors that have the common goal of manipulating an individual by creating a false sense of trust in order to obtain information from them.

TABLE 4.2: Descriptions of threat categories

Threat	Description
Theft	The criminal activity of obtaining information or funds illegally.
	E.g. Stealing log in information for a customer or employees account
Vulnerability exploits	The threat of a (un)known weakness in an application or system that is abused by an intruder to gain access.
	E.g. zero-day, SQL injection, cross-site scripting (XSS), buffer overflow
Unauthorised access	The threat that an intruder gains access to an application or system that they are not entitled or allowed to view or use.
	E.g. Accessing a system by obtaining an individuals login credentials
Social engineering	A threat of manipulating individuals, by creating a false perception of trust to divulge confidential information for fraudulent purposes.
	E.g. Baiting, phishing, piggybacking, pretexting, spoofing
Destruction	The threat whereby data or infrastructure is destroyed
	E.g. Data is destroyed when an intruder gains access to a system
Malware	Software that is designed to disrupt, damage or gain unauthorised access to a (computer) system for malicious purposes.
	E.g. Ransomware, spyware, adware, virus, trojan horse
Deception	Threats where a user assumes to be interacting and communication with a bank, but is unknowingly interacting with an individual with malicious intent.
	E.g. Man-in-the-middle attack
Eavesdropping	The threat of communication and data being stealthily recorded or listened to without their knowledge or consent.
	E.g. Sniffing traffic over a network (sniffer), keylogger
Brute-force	The persistent threat of an individual (or automated process) attempting to gain (unauthorised) access to an account or system by force means of forceful entry.
	E.g. Dictionary attack, commonly-used passwords
DDoS	A threat whereby banking systems receive an exceptionally large amount of data requests that the system becomes overloaded to an extent that it does not function normally, or goes offline.
	E.g. DDoS attack on a company's front-facing log in page.

1C: Correlate threats & vulnerabilities
In order to determine likelihood, the relationship between threats and vulnerabilities needs to be analysed. The vulnerability component was determined through a mapping in step 1A, whilst step 1B presented the threat classification. The goal of this step is to create a visualisation in which the likelihood relationship can be determined.

The decision was made to model the threat and vulnerability in a likelihood matrix, which is a common manner to express the likelihood Formula (4.2). The basic, unpopulated likelihood matrix is shown in Figure 4.6.

The reason for the chosen visualisation of the model (a matrix) is due to the relatively straightforward manner in which it can be populated and understood. Understanding relationships between the two axis' can be done in a visual manner. This is a common approach used in industry and academic literature to assess and identify the relationship between threats and vulnerabilities.

1D: Identify affected areas
Having analysed the vulnerabilities and threats separately, the relationship between the two

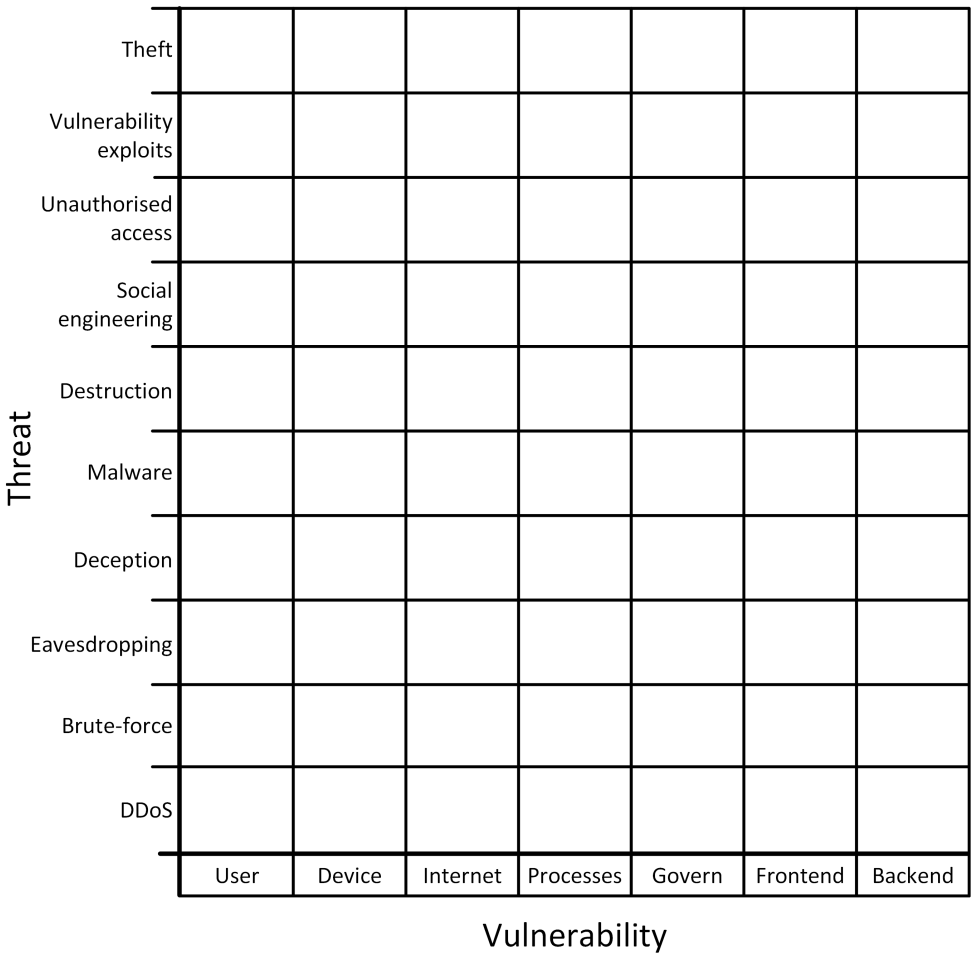

FIGURE 4.6: Empty likelihood matrix

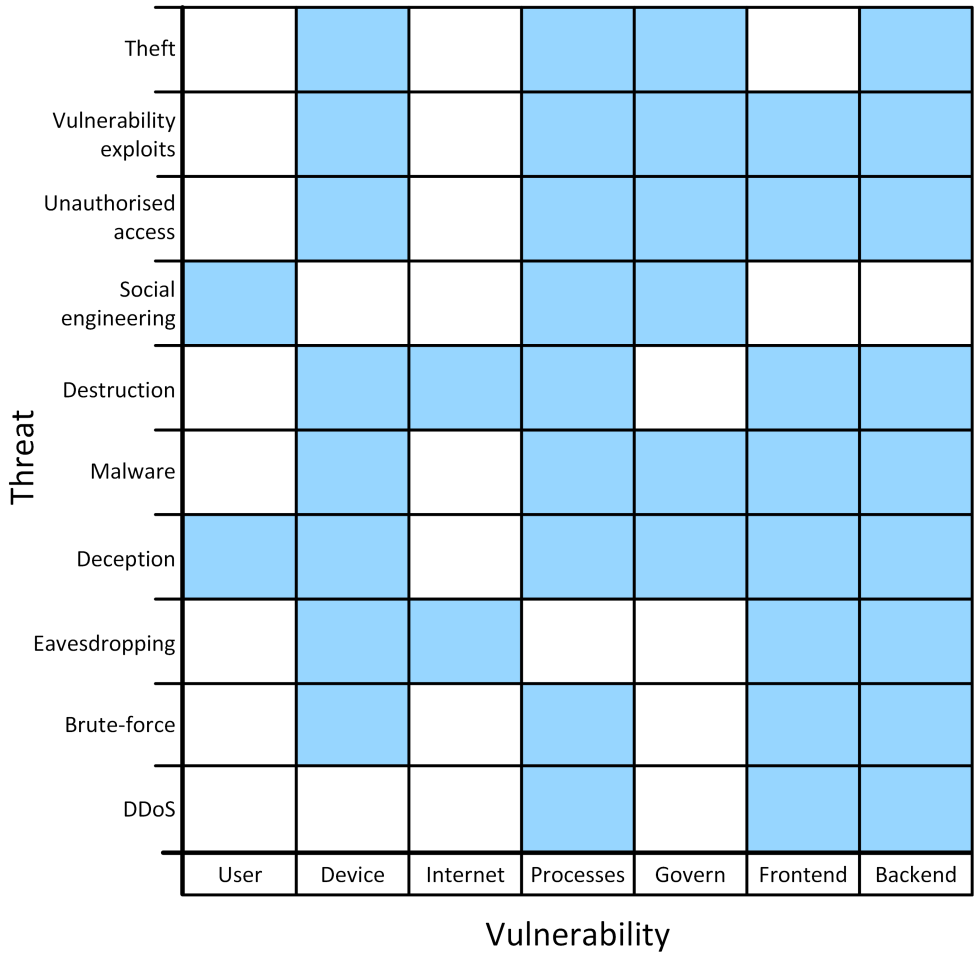

FIGURE 4.7: Vulnerable areas affected by the identified threats

components needs to be evaluated. The aim of this step was to determine which threats affect which vulnerabilities.

The literature review provided the foundation for this step. Scientific literature improved knowledge on well-documented and theoretical threats, whilst grey literature was used to identify the effect public threats have on vulnerabilities.

This knowledge was verified by experts to obtain an accurate and correct interpretation of the affected areas. In some cases, the expert added additional areas where vulnerabilities are affected by threats.

Figure 4.7 illustrates the vulnerable areas that threats affect, shown by the blue highlight. As an example, the vulnerable areas *device*, *process*, *governance* and *backend* are affected by the threat of *theft*.

1E: Identify patterns

Section 3.1.1 showed the findings of the literature review into risk management, including risk management in other fields. The findings showed that calculating quantitative likelihood is possible when sufficient reliable data exists, however calculating likelihood for indirect concepts is extremely complex due to likelihood variables interacting with each other.

The concept of patterns was therefore suggested as a means to model the likelihood variables. These patterns will provide a more reliable and effective way to determine the likelihood of cyber-attacks targeting banking institutions.

Knowledge from the literature review and discussions with experts was analysed to define cyber-attack patterns. This analysis resulted in the identification of 27 patterns.

The literature review was also used to research the occurrences of cyber-attacks primarily targeting banking institutions, but also indirectly affecting them. The cyber-attack occurrences were analysed, resulting in a number of similarities:

- Similar or identical motive.
- Identical attack, but targeting different organisations.
- Similar technique and technology used.
- Similar actions carried out during the attack.

Further analysis resulted in the grouping of cyber-attacks into categories based on these similarities, which revealed 27 pattern categories. The patterns are clearly distinguishable from each other. The identified patterns are described in Table 4.3.

1F: Determine pattern likelihood
Expert opinions and information from the literature review were used to determine the likelihood of an attack pattern. Experts determined the likelihood attack patterns would occur based on their experience and expertise, as well as how often the attacks have taken place. A 5-point Likert scale (Boone and Boone, 2012) was used by experts to determine likelihood, whereby 1 indicated *very-unlikely* and 5 *highly-likely* was used.

The average likelihood per pattern was calculated based on the expert opinions and used as final likelihood determinations. The likelihood estimations obtained per expert, and the average calculations are shown in Appendix A.1.

1G: Map patterns to areas
In order to obtain the pattern likelihood, the identified patterns (described in Table 4.3) are mapped onto the likelihood matrix. A mapping is done per pattern to determine which threat the pattern involves, as well as which vulnerable area(s) in the channel between the user and a bank are affected.

Figure 4.8 shows the visualisation to the pattern-mapping to vulnerable areas. The patterns on display in Figure 4.8 refer to the described patterns in Table 4.3.

The patterns displayed in Figure 4.8 show the patterns up to the point of compromise. Patterns are displayed as a combination of blue circles with directed-lines between them, indicating the pattern traverses more than one vulnerable area (or threat type). This illustrates and confirms a finding from the literature review that once an area is compromised, lateral movement is often observed; the attacks evolve in threat type or area targeted.

An example of a pattern mapping to the likelihood matrix can be that of P6, which is described in Table 4.3 as *a social engineering technique is used to get the user to unknowingly install malicious software*.

The mapping to the likelihood matrix in Figure 4.8 shows the pattern initialising in the *social engineering* (threat) and *user* (vulnerability) area. As the description of P6 describes, the user therefore unknowingly installs malware on their device, hence showing the mapped pattern moving to *malware* (threat) and *device* (vulnerability).

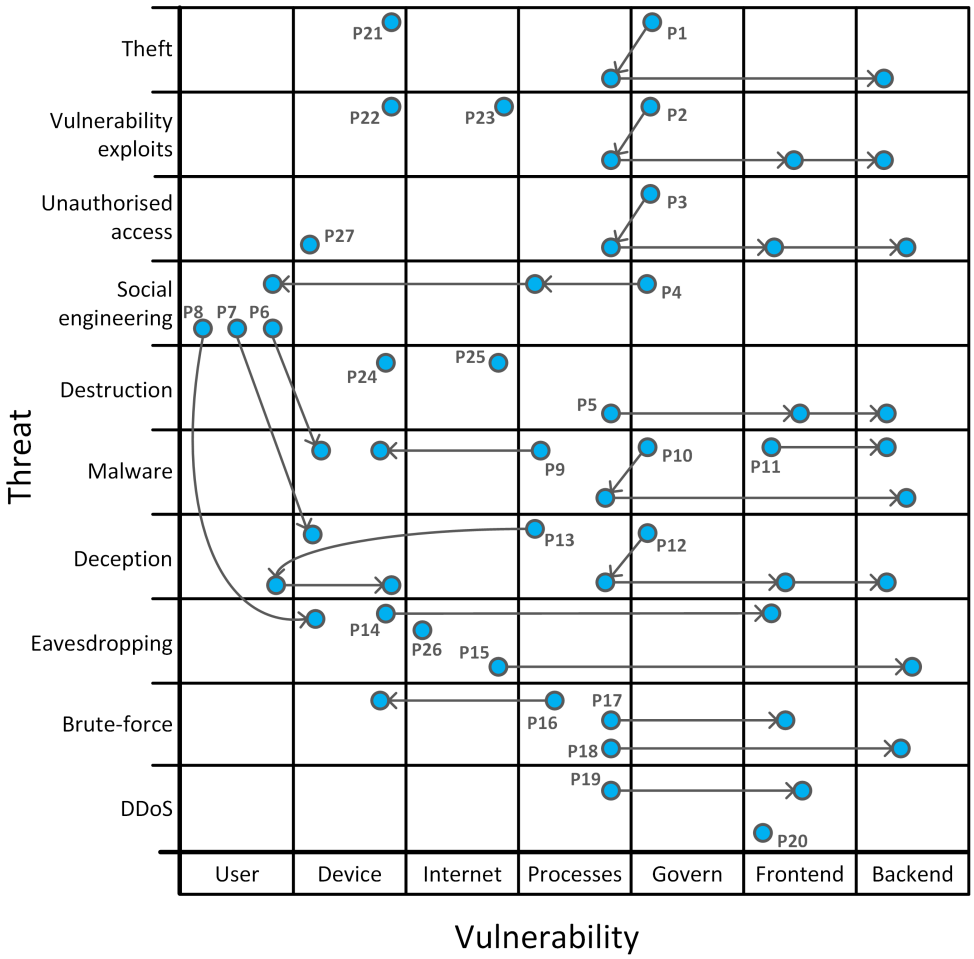

FIGURE 4.8: Attack patterns in relation to threats & vulnerabilities.

The complete likelihood matrix that incorporates all elements in determining the likelihood patterns for this thesis is a combination of Figures 4.7 and 4.8. This results in the Figure 4.9.

As Figure 4.9 shows, the patterns 'cover' all affected areas shown in blue. This is due to the blue areas indicating the threats vulnerable categories affect, which in turn are areas that are involve of targeted by cyber-attack patterns.

The types and number of patterns is not exhaustive due to their complex and overlapping nature. The discovered and defined patterns in this thesis are based on current and past cyber-attacks affecting banking institutions. These attacks are constantly evolving, changing their targets, methods and techniques in order to circumvent (preventative) measures to counteract them.

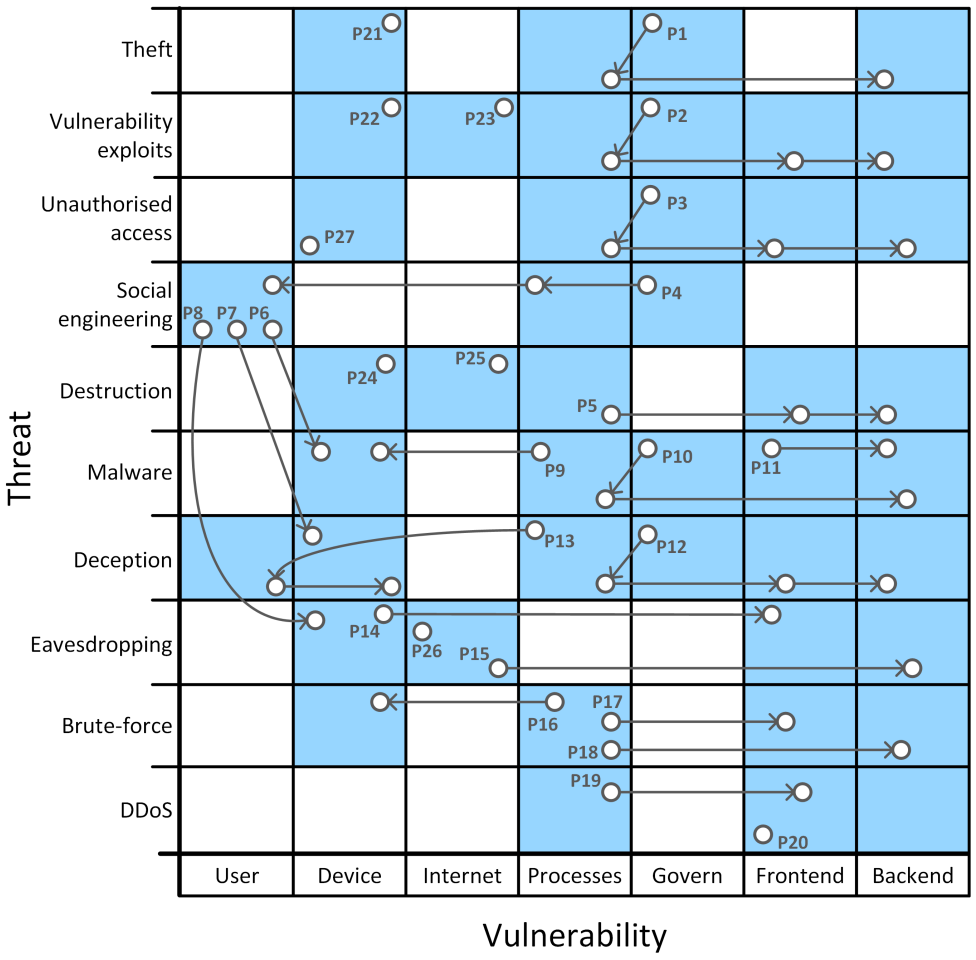

FIGURE 4.9: Populated likelihood matrix illustrating patterns and affected areas

TABLE 4.3: Descriptions of the identified attack patterns

Name	Description
P1	Governance decisions affect organisational processes that in turn may provide opportunities for data or monetary theft in backend systems.
	E.g. Decision that 2FA is not necessary allows easier access to vulnerable systems
P2	An intruder exploits vulnerabilities or loopholes in frontend and backend systems. Governance affects a bank's susceptibility to attacks as policies implemented affects internal processes.
	E.g. A policy that patches are not installed immediately when a vulnerability is signaled, checks first
P3	An intruder gains unauthorised access to the frontend and backend, carrying out illegal activities that should not be possible. Management decisions affect access-regulation.
	E.g. Login details to a system is not changed from the standard combination
P4	A social engineering technique is used to collect user information as the user is unaware that they are being tricked.Governance and processes have an effect on how easily a user is social engineered.
	E.g. An email sent to a bank's customer asking to send their information as the bank has lost it
P5	A loophole/error in a business process provides access to the backend of the bank, after which important data is destroyed/deleted.
	E.g. A competing business deletes confidential information
P6	A social engineering technique is used to get the user to unknowingly install malicious software.
	E.g. Accessing a fake website or clicking on a link that results in malicious software (malware) being installed
P7	A social engineering technique is used to lure the user (unknowingly) to a fake website. The user is then asked to enter their credentials or provide personal information which the attacker can sell for profit, or use to gain access to the banks computer systems on the users behalf.
	E.g. User enters their login details on a fake website that is hardly distinguishable from their banks
P8	A social engineering technique is used to confuse the user to install a sniffer or other eavesdropping software that logs and keeps track of traffic being sent between the user and the bank. The attacker can then sell information on, or use the collected information for illegal purposes.
	E.g. A user clicks on a link which installs an application that sends all data through to an interested party
P9	Malware is installed on a device due to shortcomings in business processes. These processes make it easier to unknowingly install malicious software that might seem like a legitimate application
	E.g. The process of installing a banking application leads to a malicious application being installed
P10	Governance and processes have an effect on the ease/difficult with which malware can be installed.
	E.g. Weak security protocols affect the susceptibility of backend systems to malware

P11	The frontend and backend systems of the bank are compromised by malware.
	E.g. Self-replicating malware that traverses through a banks internal network
P12	Governance decisions lead to policies and processes that affect the level of deception possible at the frontend and backend.
	E.g. The absence of policies enforcing 2FA mechanisms can allows backend access should the user be deceived
P13	Processes affect a user's susceptibility to deceptive techniques whereby the user's communication is altered without their knowledge.
	E.g. Communication between a user and bank, whereby an intruder changes the messages that are relayed
P14	Eavesdropping that takes place at a device-level leads to information being collected that will pose a risk to the frontend systems of the bank.
	E.g. An intruder collects login information from an high-privilege individual's smartphone.
P15	Eavesdropping at internet-level leads to information being collected that can pose a risk to backend systems.
	E.g. Confidential business information is listened to and transferred to an interested party
P16	Processes have an effect on the ease at which a device can be brute-force attacked.
	E.g. Allowing users to set weak passwords that are too short and not complex
P17	A process decision makes it easier to gain access to a banks frontend as information is easier to obtain.
	E.g. Individuals with access details to frontend applications do not need 2FA, making them more susceptible to brute-force attacks
P18	Processes affect the simplicity with which an organisation's backend can experience brute force attacks
	E.g. Short, simple passwords for individuals with important privileges and access is problematic
P19	Process decisions affect the effectiveness of a DDoS threat at the frontend, which if successful can cause severe disruptions.
	E.g. Configuration changes for the first, external-facing firewall may allow more malicious packets through filters
P20	A DDoS attack aimed to cause disruptions by reducing a banks availability, regardless of the processes or governance decisions made
	E.g. Attacks whereby individuals 'try their luck' at disrupting services
P21	Theft at a device level may lead to information being obtained that can be sold off for money or used to conduct other attacks in the future.
	E.g. An individual's personal and/or login information can be stolen from their device remotely or through other techniques
P22	Vulnerabilities at a device level do not directly affect the bank, but may lead to compromises in terms of information collection or remote access. Bank application hardening may need to be improved to ensure banking data is not compromised.
	E.g. Vulnerabilities in a smartphone's operating system may leave installed applications susceptible to particular vulnerabilities
P23	Vulnerabilities on the internet may form a point of weakness compromise for gaining access to a banks infrastructure.
	E.g. Login details can be obtained due to a vulnerability in a communication protocol

P24	Valuable information can be destroyed or altered on a device. This can involve valuable information that a user uses to login to their bank.
	E.g. Data that is used to run an application is deleted from the phone
P25	Data destruction or tampering takes place at the internet-level if an attacker is able to obtain data packets being communicated and/or sent between the user and the bank.
	E.g. Data losses or modification for personal benefit or to cause confusion
P26	Information is obtained through eavesdropping at internet level. This is a form of passive data collection. Data packets can be collected and inspected to collect information.
	E.g. Data and communication passing through an internet node is recorded and stored (illegally)
P27	An intruder gains unauthorised access to a device.
	E.g. An individual illegally accesses a customers‘ device and carries out activities

4.3.2 Impact

This section will elaborate on the impact component of the risk formula (Formula 4.1). This section will describe the 2[*] steps from Figure 4.3.

2A: Define impact areas
Impact refers to the (negative) effect an occurrence has, should it take place. Impact is explained in more detail in Section 3.1.1. In the context of this theses, impact refers to the negative repercussions for a banking institution caused by an occurrence of a cyber-attack.

Table 3.3 in Section 3.1.1 lists the results of the literature review into the dimensions of cyber attacks, which consisted of impacts and motivators. That, together with information from expert reviews culminated in a list of impacts that are applicable to the banking sector.

Further expert consultations to identify the most important impact areas resulted in the six impacts described in Table 4.4, namely; *financial*, *regulatory*, *reputation*, *availability*, *confidentiality* and *integrity*.

TABLE 4.4: Descriptions of identified impact types

Name	Description
Financial	The direct (money theft) or indirect (recovery, lost revenue) financial cost implications.
Regulatory	The direct compliance, regulatory and legal consequences, including the associated costs thereof.
Reputation	Damage or loss in trust and belief in a banking institution to customers or the wider community.
Availability	The system or application functioning normally and is accessible to users without disruptions or performance issues.
Confidentiality	The protection of information from being accessed by unauthorised parties, theft and data loss.
Integrity	The assurance of the accuracy and authenticity of information; that it has not been modified, altered or compromised.

The identified impacts have a clear differentiation and are classifiable into technical and business impacts as shown in Figure 4.10. These two types of impact have been classified in Section 3.1.1.

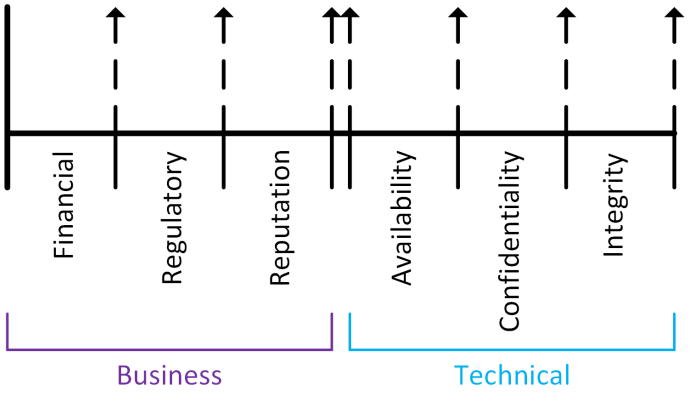

FIGURE 4.10: Relevant impact categories classified by type.

2B: Align impact areas & patterns
The impact per pattern is needed to calculate the total risk per pattern. Total impact can consist of different impact forms, hence the importance of impact type identification in the previous step.

The impact matrix will therefore contain the identified impact types on one axis and patterns on the other axis, as shown in the un-populated matrix in Figure 4.11. The goal of this matrix is to determine and analyse the relationship between the patterns and impact types.

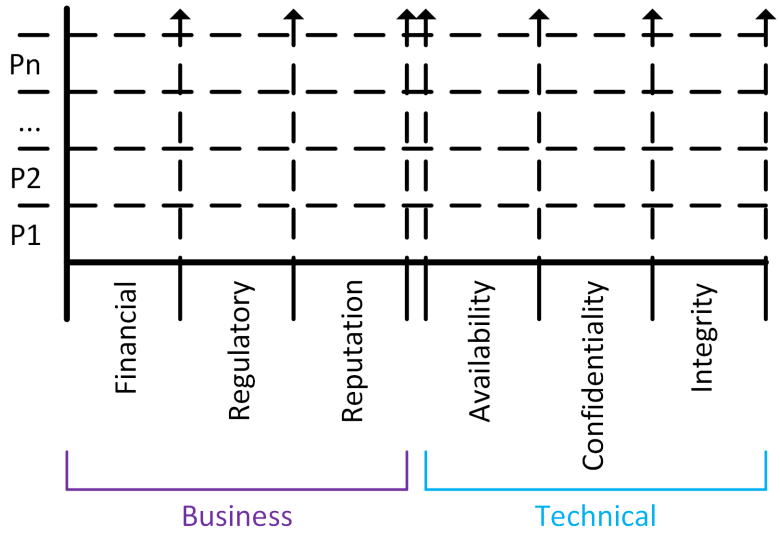

FIGURE 4.11: Impact matrix showing impact-pattern alignment

2C: Determine impact areas
The importance of estimating impact with minimal levels of uncertainty cannot be understated. The determined impacts are based on knowledge from the literature review, as well as incremental feedback from experts on their experience and perception of impact.

In order to determine impact, a quadratic scale was chosen as shown in Figure 4.12. The naming convention per impact level is self-explanatory, negligible refers to no or hardly measurable impact.

Score	Impact level	
0	Negligible	
1	Low	
4	Moderate	
9	Significant	
16	Severe	
25	Catastrophic	

FIGURE 4.12: Impact scale used for measuring pattern impact

A quadratic scale was chosen due to the non-linearity of impact; an impact occurrence classified as catastrophic is not likely to have exactly five times more impact (linear) than that of an impact classified as low.

Figure 4.13 shows the difference in impact level scores of linear or quadratic scales. The x-axis contains abbreviations for the impact level scale as described in Figure 4.12 whereas the y-axis represents impact values. Figure 4.13 therefore shows the difference in impact value per impact level should a linear or quadratic scale be used.

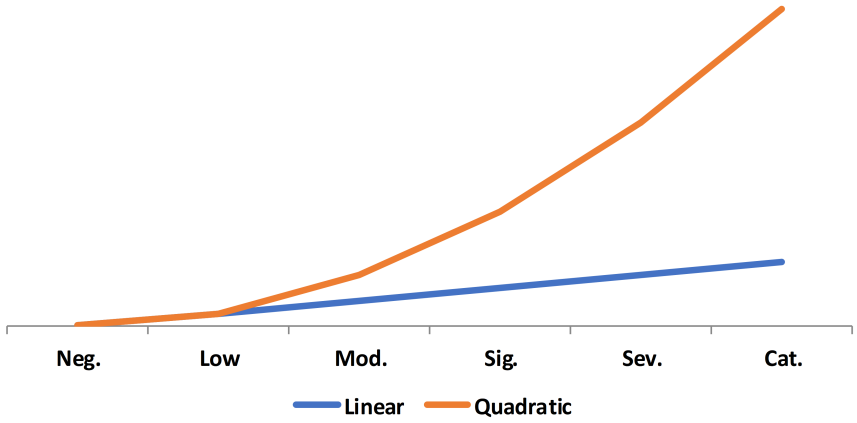

FIGURE 4.13: Graph illustrating the difference between linear and quadratic scales

The exact impact an occurrence has is complex to estimate, in particular when various factors and impact types exist that contribute to total impact. Hence, multiple experts were requested to provide their perceived or anticipated impact per pattern, based on their knowledge and experience. The objective is to get an accurate, objective estimation of impact per pattern.

The results of the impact estimation by experts are, after further analysis, presented in Figure 4.14. In order to show the highest-impact pattern, the patterns are ordered in descending order by their total impact.

2D: Deal with impact variance

Impact is defined and explained in earlier sections and steps in the design process. Although complex to calculate, impact estimations are determined through theory and experience. Impact estimates are used to calculate risk.

During the literature review, the cyber-attacks analysed and their accompanying impact showed that (total) impact is not constant. On the contrary, the level of impact was observed to vary greatly. Further research and expert opinions revealed that this variation was due to a number of variables.

To accommodate for varying impact, this thesis introduces the O-factor. The O-factor is an impact factor that provides a more accurate impact estimation for the effect an occurrence of a cyber-attack pattern has by taking a number of variables into account.

These variables collectively contribute to the circumstantial factor, Cf. The circumstantial factor consists of variables the literature review and expert opinions revealed affect the level of impact. The circumstantial factor can lead to a reduction or increase in the total impact of an occurrence.

The O-factor is therefore defined as the relationship between the circumstantial factor and the sum of the impact categories, the total impact, of an occurrence of a cyber-attack, $\sum_{y=1}^{n} I_y$.

A generalised expression of the O-factor can take the form of Formula 4.3 below:

$$f(\sum_{y=1}^{n} I_y, Cf) \tag{4.3}$$

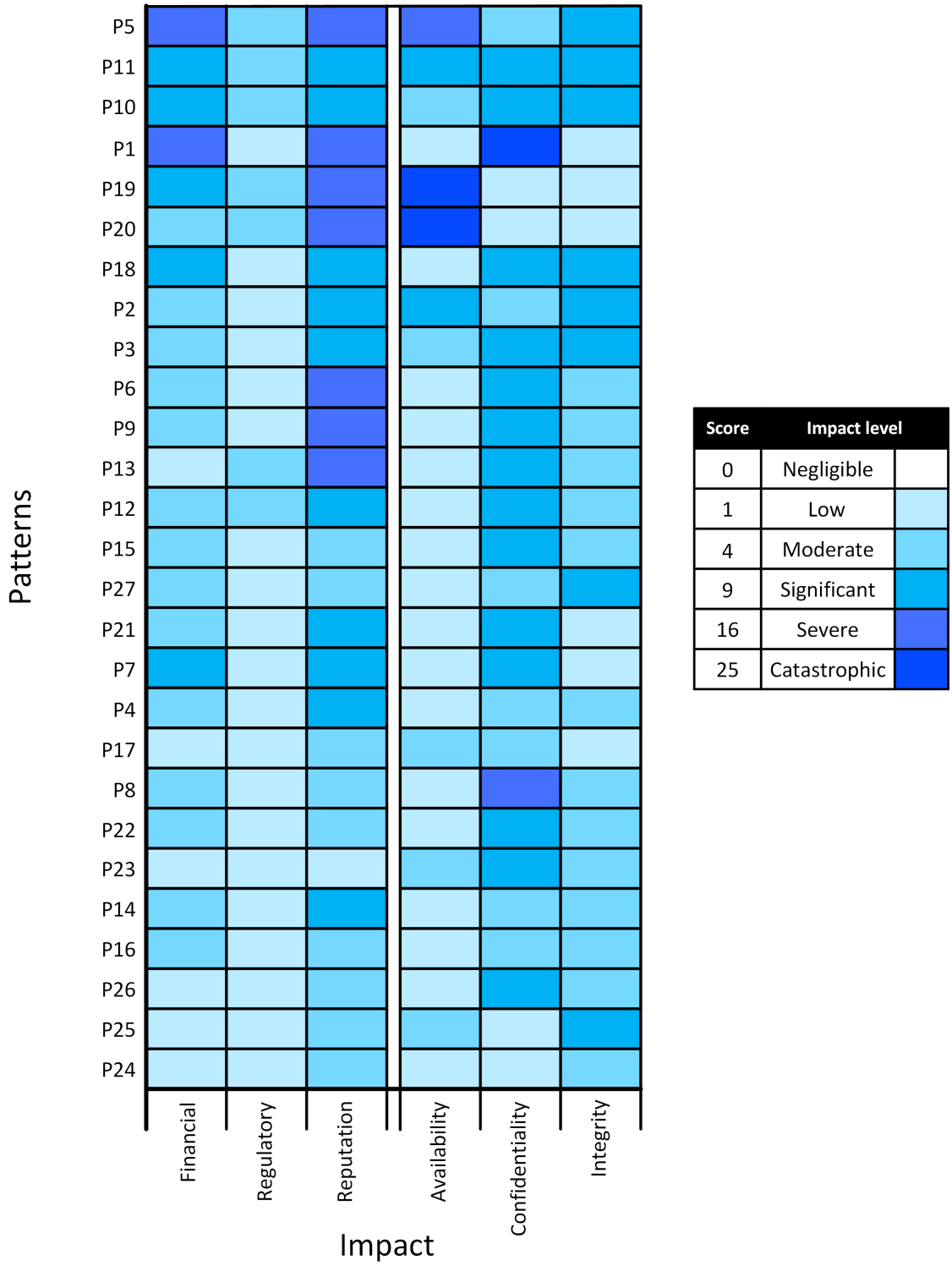

FIGURE 4.14: Impact matrix showing impact-pattern alignment

The circumstantial factor (Cf) is calculated by the product of the variables that affect impact. Cf is therefore represented as $Cf = x_1 \times x_2 \times ... \times x_n$, where the x_n's refer to the variables.

Variables that have an effect on the circumstantial factor are described in Table 4.5. The list of variables in Table 4.5 were obtained from literature and experts, however the list is not exhaustive.

TABLE 4.5: Descriptions of circumstantial factor variables

Name	Description
Size of bank	The size of the organisation.
	E.g. market value, customer base, assets, number of employees.
(current) Publicity	The current perception of the organisation to customers and the public at large (reputation).
	E.g. a bank's negative reputation due to investments in oil
Number of occurrences	Whether the attack is the first occurrence of its type. This affects an organisation's readiness to mitigate the cyber-attack.
	E.g. effective countermeasures nullify the impact of a repeated attack
Timing	A specific time can influence the level of impact that attack causes.
	E.g. Public holidays, attacks carried out from a specific timezone
Number of victims	The number of individuals affected by the cyber-attack.
	E.g. one-thousand instead of ten individuals are affected
Role of victim(s)	The role or job position of the targeted individual.
	E.g. Senior individuals likely have more critical private information

4.3.3 Risk

Risk is defined and explained in Section 3.1.1 as the potential for loss or damage when a vulnerability is exploited by a threat. Risk is expressed in Formula 4.1 as the product of *impact* and *likelihood*.

Literature on risk further showed that the most common and effective manner of modelling and visualising risk is by means of an impact-likelihood matrix. That combined with the definition of risk (which includes impact and likelihood) formed the motivation to use an impact-likelihood matrix to model and determine the risk of cyber-attacks in the banking sector.

This subsection will explain the creation of the Risk matrix.

3A: Define risk categories

The concept behind a impact-likelihood matrix is to determine risk by means of analysing the relationship between the likelihood an event will occur, and the impact that event will inflict. A basic, un-populated structure of an impact-likelihood matrix is shown in Figure 4.15.

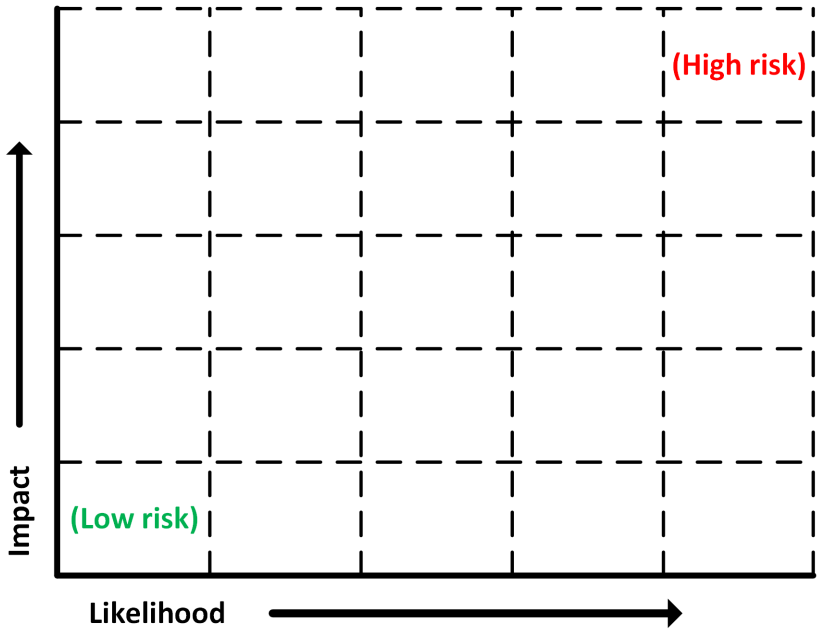

FIGURE 4.15: Empty risk matrix

The impact-axis on Figure 4.15 is designed to contain attack patterns that have been plotted based on their total impact, categorised from *very low* to *very high* impact. Likewise, the likelihood-axis is used to visualise the likelihood a cyber-attack will occur. Both approaches conform to procedures in literature in analysing risk using an impact-likelihood matrix.

Figure 4.16 illustrates the risk scale of the framework, linking colours to risk categories. A 5-point likert scale (Boone and Boone, 2012) was used to determine the risk categories. These risk categories are placed at predetermined locations in the impact-likelihood matrix as shown in Figure 4.17.

Risk scale	
	Low
	Low-Medium
	Medium
	Medium-High
	High

FIGURE 4.16: Scale used for indicating risk

Five impact categories were selected in order to provide an improved distinction of the various risk levels (severity). Literature on risk regarded 3-point (low, medium and high) and 5-point scales (low, low-medium, medium, medium-high and high) as viable, effective category options to model risk.

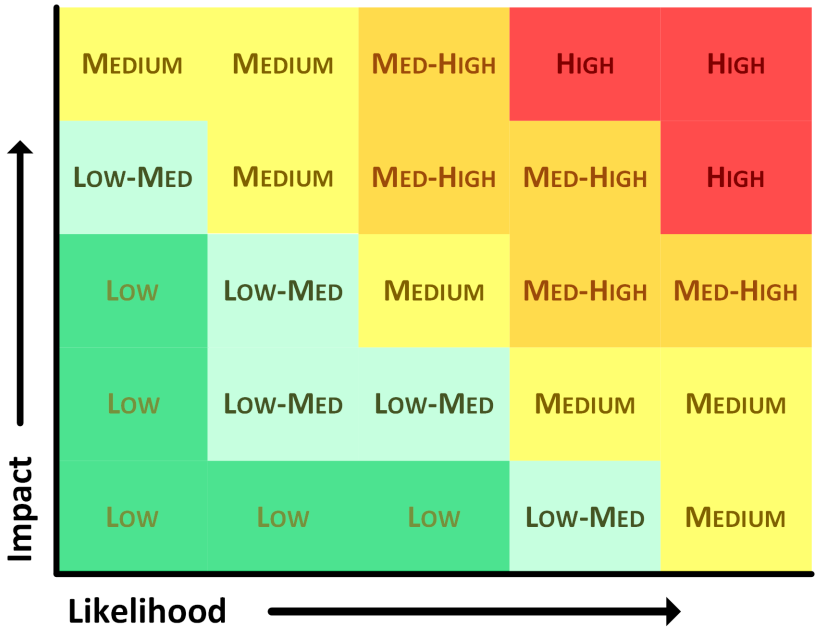

FIGURE 4.17: Risk values as per their location on the risk matrix

Figure 4.17 shows the risk categories plotted on an un-populated matrix from Figure 4.15. Attack patterns with both high impact and likelihood data are defined as high risk, whereas low impact and likelihood patterns are defined as low risk.

The location of each risk category in the Figure 4.17 is based on knowledge from the literature review, expert opinions and experience. This is the reason that the location of risk categories in Figure 4.17 does not resemble typical risk matrices.

3C: Map patterns to risk

Figure 4.18 shows a the populated risk matrix. The plotted attack patterns are based on the relationship between the total impact and the likelihood that the patterns will occur, as per risk literature.

The risk level per attack pattern is revealed in Figure 4.18 by the colour of the background at the location where the pattern is plotted.

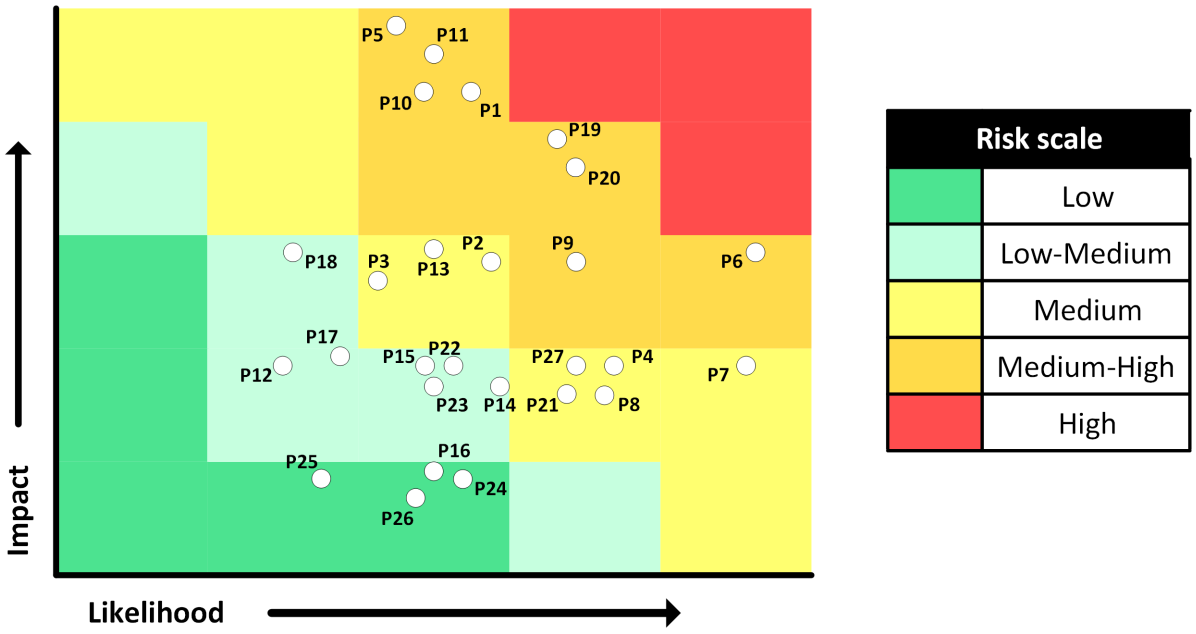

FIGURE 4.18: Risk matrix for cyber-attack patterns

Chapter 5

MCP Framework

5.1 Introduction

This chapter provides a full overview of the designed framework. The data flow and relationships between the different matrices in the designed framework are shown in Figure 5.1 on the following page. It shows which information was produced as output, and in turn contributed in the form of input to other matrices.

The design principles and steps have been explained in an iterative manner in Section 4.

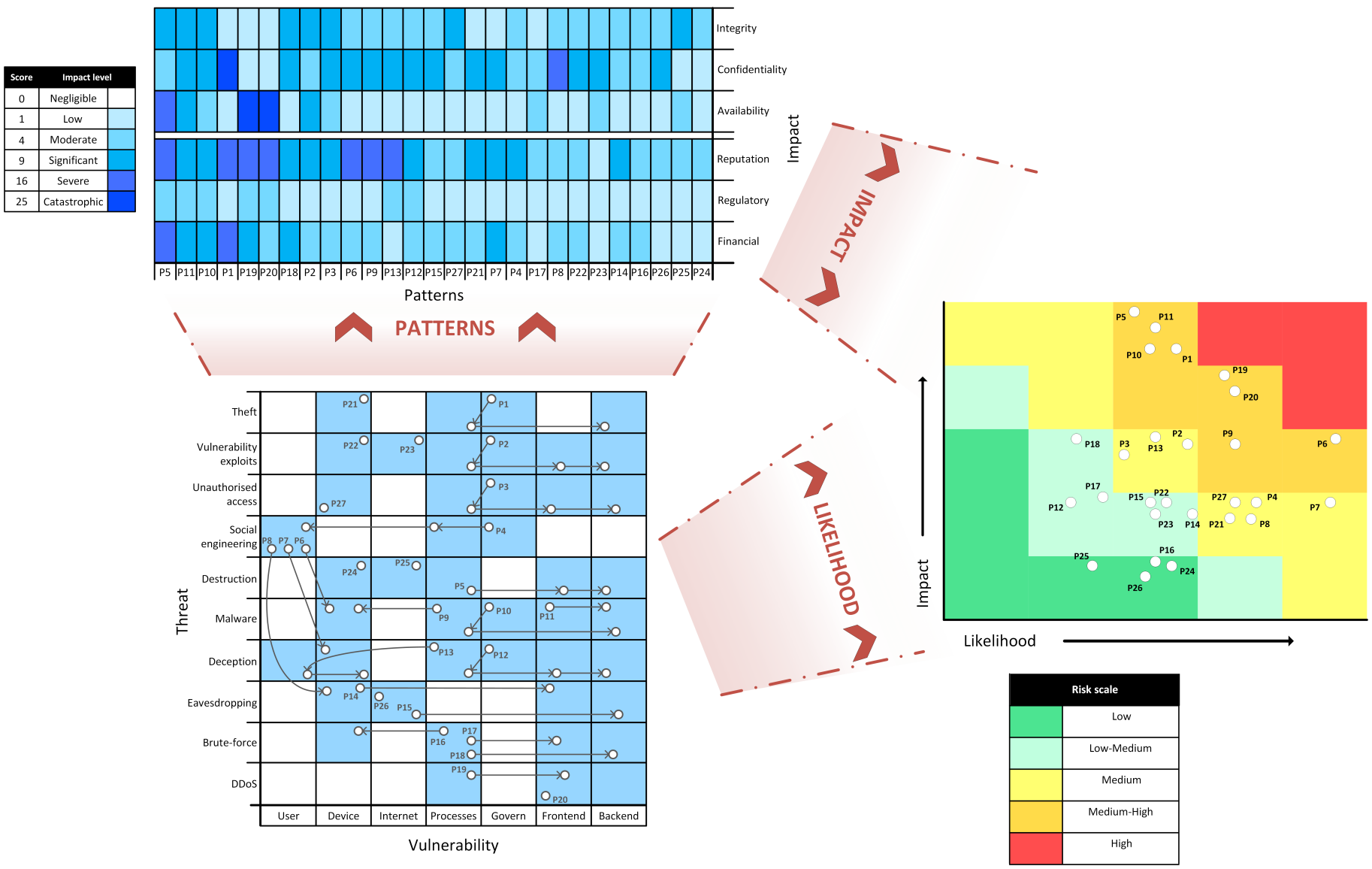

FIGURE 5.1: Full framework overview

Chapter 6

Framework validation

This chapter presents the objectives of the Treatment Validation phase by elaborating on what exactly will be validated. The designed framework will be referred to as an artefact in this section and Section 7. This chapter will also detail the techniques applied to validate the artefact.

6.1 Introduction

Treatment Validation is the third phase in the Design Cycle (Wieringa, 2014). The artefact developed during the Treatment Design is validated to ensure it satisfies specifically defined requirements, which contribute to the stakeholder goals.

Validation is an essential component during the design of an artefact as it provides a means to investigate and predict how the designed treatment will perform when implemented in the problem context.

The majority of this validation phase is based on standard techniques from Wieringa, 2014, however self-defined techniques based on validation theory from Wieringa, 2014 will be used to validate specific components of the artefact.

This section describes the various techniques in the validation phase. The designed framework will be referred to as the artefact.

6.2 Method

6.2.1 Objectives

The objective of this Treatment Validation is to determine whether, and to which extent the main goal of this thesis has been realised.

This phase aims to gain insight into the usefulness, completeness, validity and soundness of the designed artefact. Expert reviews will be used to obtain qualitative and quantitative information about the artefact.

As a reminder, the main goal of this thesis is:

To design a multi-channel cyber-attack patterns-based risk modelling framework for the banking sector.

Wieringa, 2014 states that the purpose of validation is to determine if the developed treatment contributes to stakeholder goals. The validation objectives were therefore defined based on this research's main goal, information obtained from risk expert opinions and scientific theory. General-purpose frameworks and existing risk frameworks were

The objectives are defined as follows:

- Evaluate the representation and understandability of the artefact.

- Gather information about the usefulness and effectiveness of the designed artefact.
- Determine the correctness and soundness of the artefact, and method of identifying risk.

6.2.2 Techniques

Four validation techniques will be used to validate the artefact. These techniques are shown in Figure 6.1 and described in this section.

The experts consulted during the validation phase are not the same experts that provided input and feedback in designing the framework in Section 4. This choice was made to improve the quality of the designed framework and validation results by maximising objectivity.

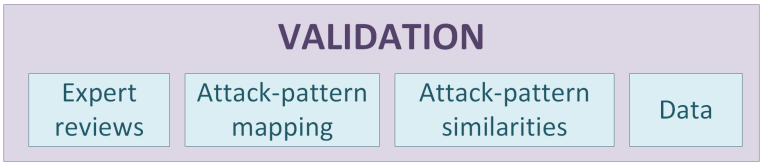

FIGURE 6.1: Techniques used to validate the artefact

The artefact will not be validated by aligning and comparing it to other risk frameworks. The completely different nature and approach of this framework made this form of validation less unsuitable.

The focus of control frameworks on controls and measures (without considering risk) makes validation by a comparison to control frameworks not a suitable, nor representative, form of validation.

As described in Section 3.1.5, control frameworks consist of guidelines and measures to increase security and protection. NIST describes functions to accomplish an organisation's goal, while ISO 27001 defined 134 measures that contribute to 39 control goals to improve security. COBIT is a control framework that lists 40 governance goals to assess the maturity of an organisation's security without considering risk.

The artefact from this research varied greatly from the FAIR, CORAS and ISO31000 risk frameworks. Although these frameworks had a common goal of identifying risk through a number of high-level steps, this research artefact's method of modelling the likelihood of cyber-attacks by means of patterns differs from traditional risk frameworks. This made it difficult to directly compare the frameworks as a form of validation.

Expert reviews

Expert reviews are "the simplest way to validate an artefact" (Wieringa, 2014) and are a good technique to discover bad designs (Wieringa, 2014).

Expert reviews will be used to validate the correctness and usefulness of the designed artefact, the framework. They are an effective validation technique to obtain (unbiased) information about expert perceptions and opinions of the artefact. Experts are able to elaborate on their expectations of such a framework, as well as provide feedback on their views on advantages and shortcomings of framework.

Environment

Each expert review will be conducted in a meeting room at BankY to ensure maximum focus and that there are minimal distractions and disturbances from others. The validation sessions were recorded (audio) to enable easier data collection and processing once the validation session

has been completed.

Procedure

The procedure for the expert reviews is shown in Figure 6.2. As illustrated in Figure 6.2 there are three phases in the expert reviews.

The pre-validation session tasks were once-off, followed by four separate validation sessions with experts. To conclude the process, post-validation session tasks involved processing and analysing the expert reviews.

Prior to the validation sessions, two artefacts were created:

- Presentation P1 describes the background, relevance and motivation of this master thesis. This introductory presentation is especially helpful for individuals that were unaware of what this research was about.
- Presentation P2 will elaborate on the framework. This shows the various components and matrices of the framework. The emphasis of P2 was to present the designed framework in an objective manner.

During the validation sessions, experts were encouraged and given complete freedom to express their opinions or ask questions at any time. Both positive and negative feedback was explicitly encouraged. The researcher was at all times objective regarding the artefact being validated.

Throughout the validation sessions, the researcher posed questions to the expert. These questions were based on a number of themes aimed at extracting information regarding the usefulness of the artefact.

Prior to each validation session, each expert was requested to give their objective opinion on all aspects of the framework during the validation session. The experts were therefore requested to not base their feedback solely on their experience and practices at BankY.

To further improve the accuracy and objectivity of results, multiple external experts were requested to take part in the validation sessions. However due to scheduling challenges, one of the four experts for validation were from outside of BankY.

The results of the four expert reviews are analysed and processed in the post-validation session. The results will be presented in Section 7. Table 6.1 shows the job description per expert in the expert review.

TABLE 6.1: Information about validation experts

Expert code	Job description	Motivation
E1	Solution Architect Security Specialist	Realises and translates business needs into technical solutions. A cryptography and security expert.
E2	Information Security Officer	Consults and advises various departments within a bank on issues pertaining to risk and security. Regularly does data security checks.
E3	Solution Architect	Realises and translates business needs into technical solutions.
E4	Security Tester	Has been working in the security field for over 10 years. His current position as a penetration tester underlines his expertise in security concepts.

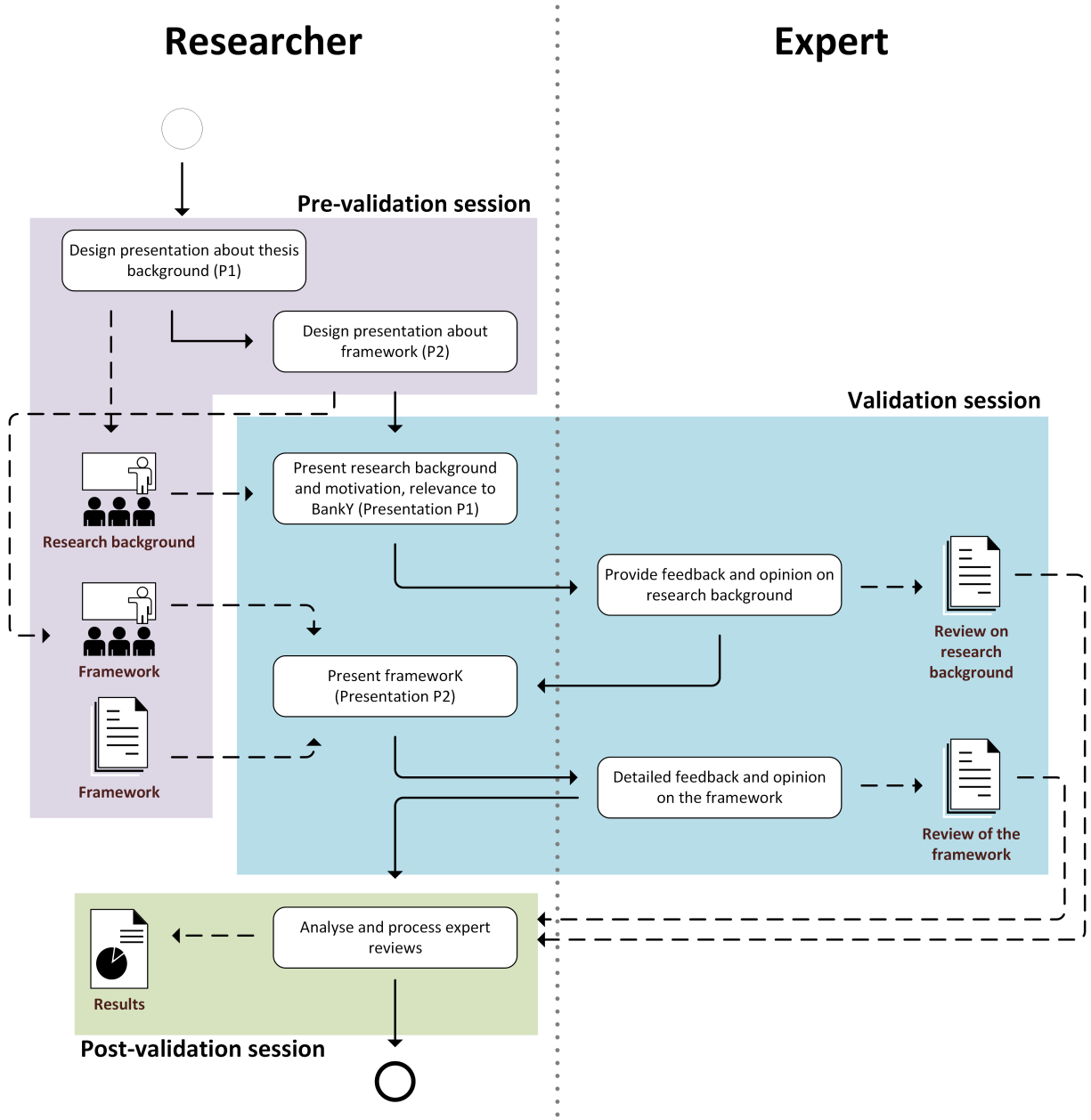

FIGURE 6.2: View of the expert validation session procedure

Attack-pattern mapping

The patterns presented in the artefact are as a result of the literature review. Further research of scientific and grey literature revealed various cyber-attacks that were directed at or affect banking institutions. To prove the validity of these patterns, a pattern-attack direct mapping will be done to demonstrate the validity of each pattern.

The pattern-attack mapping will consist of a direct mapping between patterns of cyber-attacks aimed directly at banks, as well as indirect attacks that may influence or have an impact on them. The aim of this mapping-validation is to verify the authenticity and correctness of the patterns.

Figure 6.3 shows an example of the attack-pattern mapping.

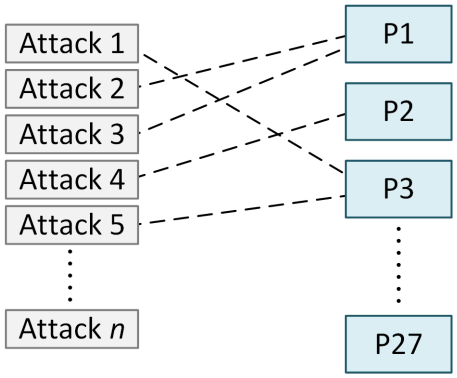

FIGURE 6.3: Illustration of attack-pattern mapping

Attack-pattern similarities

Attack-pattern similarities will be used to validate cyber-attacks that have been defined as forming the same pattern. The reasoning is to confirm that attacks sharing similar characteristics are indeed in the same pattern.

The attack-pattern mapping followed the same structured procedure. Validating four patterns should therefore be relatively representative for the remaining twenty-three patterns. These four patterns were selected at random.

Data validation

Qualitative and quantitative data was obtained from literature and experts during the review phase. Both formed input in the artefacts' design during the Treatment Design phase.

The goal of this is this technique is to show and elaborate on the findings that were used in designing the artefact.

Chapter 7

Validation results

This chapter presents the results of the Treatment Validation phase. The results will presented per validation method, which will be analysed and discussed in Section 8.1.

7.1 Expert reviews

The validation sessions for each expert was organised on a different day. Each validation session produced an audio recording, with all four recordings varying in length between 69 and 81 minutes. The audio recordings contained the full conversation and discussion with experts, hence producing qualitative data.

The qualitative data from the audio recordings was transcribed and processed to simplify the data analysis.

The expert reviews were analysed and the findings are presented below to illustrate the artefact's usefulness as per Wieringa, 2014. A brief conclusion of the expert review is in Section 7.1.

General

General comments and feedback about the framework.
All four experts found the framework to have a clear visualisation. E2 praised the simple but clear representation of information, stating that the framework was "well thought of, based on theory" and what he often sees in his role as security officer. E4, E2 and E1 explicitly mention that the framework looks good and is easy to understand. It must be noted that all four experts had significant experience in the security field therefore basic concepts of security and risk did not need detailed explanations.

There was consensus amongst the experts that the motivation and gap defined for the research was clear and justified, as well as that the representation of the designed artefact was in line to realise the intended goal. E1 was pleased with the research's risk modelling approach to combining IT and business stating that it links the practical (technical) and business aspects, something that isn't done enough when analysing risk and security.

Vulnerabilities

Comments about the identified vulnerable areas between a customer and bank.
The four experts all confirmed that the identified high-level channel architecture (Figure 4.4) is valid and relevant. The identified vulnerable areas are "good places to look at" according to E2, a statement supported by E3. Expert E1 added that it "is a correct view of the channel between a customer and the bank" with E3, E2 and E4 stating that the architecture shown is an effective and common, standardised architecture. E2 mentioned that the security course he follows (CISP certification) "has a similar architecture".

Three experts elaborated on the type of infrastructure in the DMZ, which confirmed the examples this research listed. The three experts stated that the applications in the DMZ are not data-critical, E1 explaining that if an application in the DMZ is compromised, the attacker will

not be able to "access or steal data".

Threats

Comments related to the threats or threat categories in the framework.
The most feedback and comments during the validation sessions came with regards to the threat categories that were used in the likelihood matrix. All four experts stated that the attacks that they could think of were covered by these categories, however E3 and E4 raised concerns of overlapping categories.

Expert E3 questioned the threat category *vulnerability exploits*, finding it "a bit of a strange threat because threats [ab]use vulnerabilities". The researcher concluded that naming convention was the main reason for this comment as the threat category *vulnerability exploits* merely encapsulates various concrete threats. E1 supports this reason that "a lot of attacks start with vulnerability exploits [unknown weaknesses]".

Expert E2 was pleased with the notion that patterns stop at the vulnerable area of compromise in the framework. Through his experience, he observed that attacks mutate, or open avenues for other threats to be executed once infrastructure or a system has been compromised. E2 likened this to the Anna Kournikova virus that spread in 2001.

Patterns approach

Comments about the method of using patterns to analyse the impact of cyber-attacks.
All four experts had positive comments about the approach of using patterns as a means to represent cyber-attacks. Expert E2 mentioned that "patterns give you a clear indication of [the] cause and consequence [of cyber-attacks]" as opposed to looking at the "consequences of the attacks separately, reactively". E2 further states that the concept of patterns is an effective manner in which the flow within attacks can be illustrated.

There was consensus amongst the experts regarding the formation of patterns. The four experts described the patterns as realistic and correctly based on attacks in the past, but were cautious about their validity in the future. E1 reasoned that "new attacks emerge everyday, current attacks are constantly changing", with E3 supporting this by stating that "predicting the future is difficult" and "in 10 years there may be 20% more attacks that are introduced by new technologies".

With respect to the effectiveness of the framework, E4 mentioned that there "will always be things [patterns] that don't fit in a model, but that does not say that it [the model] won't be useful". E1 further supported the notion that not all patterns will, nor can be covered by stating that "you will never get a complete set of patterns."

Impact

Feedback about the identified impact types and impact values.
In terms of impact, all four experts were in agreement that the six impact types identified were valid, as well as being the most important types for banking institutions. The impact types Confidentiality, Integrity and Availability were named by E2 as "very relevant ... technical impact" that are used in the security domain as a measure to describe data.

Experts E1 and E3 mentioned that relationships and dependencies exist amongst the impact types such as that "financial impact will most probably lead to a higher impact to reputation". There was consensus amongst the experts that impact to a bank's reputation was the most important factor to consider during an attack. Financial, Integrity and Confidentiality were also mentioned. However, E1 believes that banking institutions in The Netherlands are not phased by financial damage: Financial damage "in 2012 [stood at] €35 million and 2018 €3.8 million more".

Impact: O-factor

Feedback regarding the O-factor as a way to handle impact variance.
There was consensus amongst all four experts that impact is variable. The O-factor approach and formula was endorsed by all experts as an effective way to account for this impact variation, however E4 suggested that the relationship between the variables in the formula is more complex than 'simply' the product of them.

E1 and E3 on the other hand found the O-factor formula clear and correct, highlighting the differences and subjectivity in expert opinions. E4 continued at a later time to confirm that the variables in the O-factor formula are logical, but that he merely questioned the relationship amongst them. These comments led to a change in the O-factor formula's representation.

E2 explicitly mentioned that the O-factor concept shows that"you learnt from theory, [and] that you interpret this knowledge and show that these factors influence impact". The expert then issued a word of caution that regardless of how well impact is estimated "it will never be 100% certain".

The experts listed diverse reasons for varying impact, E1 and E4 explicitly saying that this was influenced by preventative measures. Preventative and mitigation measures were indirectly implied by E2 and E3. E1 is quoted that "the first time [an attack occurs] is shock, the fifth time [the shock-effect] is less". An interesting and valid comment by E1 and E4 is that the level of impact depends on the extent of which the attack is successful.

Comments regarding the suggested circumstantial factor (C_f) variables in O-factor were positive, all four experts concluded that these were very important ones. Two experts described them as "the most important" variables. E4 spoke about the timing variable from his experience in an instant response team that "we saw more activity on Friday afternoon, around [the] end-of-week drinks time" for example. The experts were however in consensus that the list of C_f variables is non-exhaustive, with E2 suggesting that "[it] may be an indefinite list"

As a parting comment, E4 described hearing about something similar in the news, that a recent cyclone would have had less impact had it occurred slightly south of the eventual area it hit. Checking news reports after the validation session showed that E4 was referring to Cyclone Idai in Mozambique, an interesting real-time example that impact varies.

Risk

Comment about the representation and areas of risk the framework identified.
All four experts agreed with the representation of risk in the Risk matrix, with E2 particularly pleased that there are no high-risk patterns. The choice of using a impact-likelihood matrix to model risk was valued by E2 as "it is the standard approach to determine risk", showing that a proven method was used to model and determine risk.

E1 found the method of risk representation in the matrix by means of a 5-point scale more interesting and insightful than the usual 3-point scale, and deemed it "good to not make it symmetric as is usually done". E4 added to the comment of the risk matrix not being symmetric as that it is a welcome change and shows that the impact and likelihood does not always lead to the same risk in an organisation.

Conclusion

Brief conclusion about the expert reviews.
All four experts were positive about the framework. The experts provided feedback supporting the completeness of the framework by repeatedly mentioning and implying that the framework is built on common and logical risk concepts and principles. In doing so, these comments can be read as supporting the correctness and validity of the framework as well.

E4 and E2 were, for example, in agreement with the steps taken to obtain risk of the attack patterns. E2 suggested that the framework's approach was "correct" and E4 that the framework

takes "logical steps for assessing risk". E4 in particular agreed with the use of "the standard risk formulas as a basis for the framework" as this was based on years of research and experience.

Although difficult, experts were cautiously optimistic about the use of patterns in determining risk. They fully acknowledge that the patterns will not always be applicable due to the continuously changing IT landscape, but that the patterns in their current form represent the current state of the cyber-attack landscape. Experts did see the use of patterns, one reason of them being a reliable manner to look at the flow of an attack as a way to observe the cause and consequence of the attacks.

To conclude, the experts were in agreement that the framework had an added value. They considered the framework itself, as well as the approach taken and concepts introduced, as a useful addition and a new way to look at and determine risk. This proves the framework's usefulness and contribution to this research thesis' main goal.

7.2 Attack-pattern mapping

Eighty-nine (89) cyber-attacks were analysed as part of this research thesis. As mentioned in Section 4, the cyber-attacks were classified into patterns that directly or indirectly affect banking institutions.

The attack patterns were defined and based on input from experts, literature and experience. Following this process, cyber-attacks were identified through research on news reports (grey literature) and scientific literature.

Each cyber-attack was then analysed and mapped (classified) to the correct attack pattern. The cyber-attacks and their corresponding pattern(s) are displayed in Appendix B.

Mapping the cyber-attacks showed that two attack patterns were missing, as cyber-attack incidents occurred where no suitable pattern existed. These patterns were added to the design.

A number of attack patterns obtained from expert reviews were not covered by the identified cyber-attacks. This can be due to bank secrecy on attack incidents (minimise public information about attacks), or that the attacks can occur in theory but have not been used in practice (yet).

The analysis of these attacks showed that a single occurrence often consists of lateral movement[1], whereby an attack has different threats and targets. As explained in Section 4, the patterns in this research stop at the point of compromise.

Both of these factors mean that the cyber-attacks may have one-to-many relationships with attack patterns.

7.3 Attack-pattern similarities

To show the validity of the attack patterns, 4 of the 27 attack patterns will be analysed to prove the similarities amongst cyber-attacks that have been mapped to these patterns. A simple mapping-technique was used to map the cyber-attacks to patterns, hence a sample of 4 patterns would give a good indication of the validity of the overall mapping.

Patterns P1, P4, P6 and P20 are analysed and explained below. The patterns and the cyber-attack's that fall into their categories are listed in Appendix B.

P1: Governance decisions affect organisational processes that in turn may provide opportunities for data or monetary theft in backend systems.

Sources: (McMillan, 2009), (Evans, 2018), (BBC, 2014)

[1]Technique used to systematically traverse a network to identify, search and gain access to sensitive information

- Theft card details (BBC, 2014): The lack of sufficient security measures allowed for a banks' contractor to (illegally) download data, which was unencrypted, to a USB-device. No logging mechanisms alerted the firm to the data breach.
- Personal data breach (Evans, 2018): Attackers used a common mathematical algorithm to generate account numbers that belonged to bank customers. This information was used by the attackers to 'verify' that the customer had forgotten their login password. Account data was then stolen. The process of verifying a user that requests a password change was therefore insufficient.
- Bankruptcy data breach (McMillan, 2009): An error/bug in the storage of data about bankruptcy claims, and the process of redacting[2] private information in these claims allowed for attackers to access personal data.

The three cyber-attacks described above shows the role governance and processes have on the ability of an attacker to commit data theft. Shortcomings in the governance stage affect processes which in turn influences how susceptible a bank is to cyber-attacks that take the form of pattern P1.

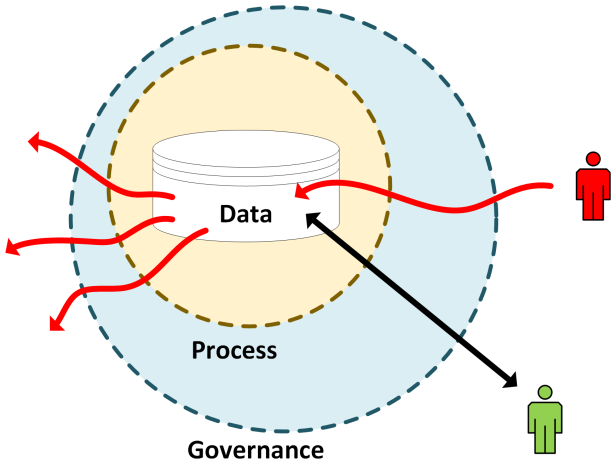

FIGURE 7.1: Illustration of the similar process amongst pattern P1 attacks

P4: A social engineering technique is used to collect user information as the user is unaware that they are being tricked. Governance and processes have an effect on how easily a user is social engineered.

Sources: (Zorz, 2012), (Schwartz, 2018), (Peter, 2017)

- SIM-swap (Peter, 2017): Bank customers receive their banking transaction tokens on their mobile phone. Criminals contact the customer's mobile provider impersonating the customer and requesting a new SIM card. The attackers then contact the customer impersonating the mobile provider and requesting the SIM card's unique code which 'gives' the criminals access the customer's phone number. Criminal transactions can then be authorised with the codes received on the mobile phone.
- CEO-Fraud (Schwartz, 2018): A company's financial director received a (fraudulent) email from the CEO's private email address requesting that funds be transferred for the secretive purchase of another company. Internal procedures did not protect against this.

[2]Redacting: The process of censoring (parts of) text for legal or security purposes.

- Theft (Zorz, 2012): A fraudster stole $2.1 million from a hospitals bank account by faxing a money transfer request with a copy-paste (false) signature. The bank employee authorised the request without sufficiently checking the legitimacy of the request.

All three of the cyber-attacks described above show that the incorrect, or the lack of sufficient verification in processes influenced the ability of attackers to carry out social engineering. Process decisions are often decided by management teams at a governance level. Figure 7.2 shows a simple high-level illustration of pattern P4 attacks.

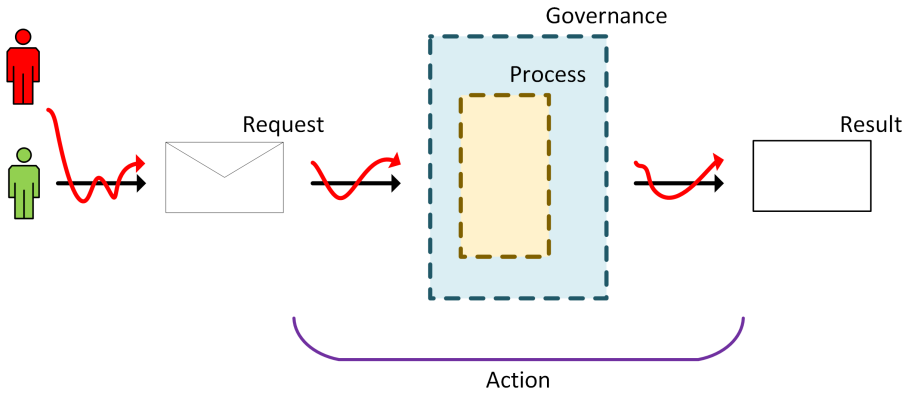

FIGURE 7.2: Illustration of the process of pattern P4 attacks

P6: A social engineering technique is used to get the user to unknowingly install malicious software.

Sources: (Vijayan, 2018), (Malwarebytes, 2018), (Kalashnikoff, 2018)

- CamuBot (Vijayan, 2018): Attackers phone victims and encourage them to visit a website which installs an application that silently captures banking login credentials when users access their bank.
- Fake App (Kalashnikoff, 2018): Users are tricked by a website link to download a malicious application that promises to show all their bank accounts in 1 view, instead stealing their information.
- Emotet (Malwarebytes, 2018): An email is sent to a targeted *user* with a script, macro or link in it that installs malicious software

As the described cyber-attacks show, attacks in pattern P6 start with a delivery mechanism that targets a *user* and results in the installation of malicious software. Figure 7.3 shows this pattern.

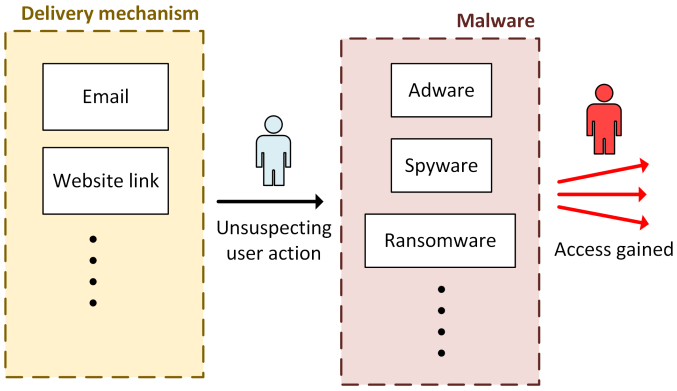

FIGURE 7.3: Similarity between cyber-attacks in pattern P6

P20: A DDoS attack aimed to cause disruptions by reducing a banks availability, regardless of the processes or governance decisions made.

Sources: (Brook, 2012), (Goldman, 2012), (McGuinness, 2017)

- Bank of America attack (Goldman, 2012): A politically-motivated hacking group conducted a DDoS attack on an American bank that affected the performance of their website for customers.
- HSBC DDoS attack (Brook, 2012): A DDoS cyber-attack targeting the British bank's global websites for a sustained period of time. The banks websites were unavailable during the attack.
- DDoS Estonian banks (McGuinness, 2017): A cyber-attack targeting online services of Estonian banks by flooding their servers with 'unprecedented levels of internet traffic' (McGuinness, 2017) from botnets.

The cyber-attacks described above show that DDoS attacks, that together form pattern P20, are carried out using similar techniques and with a common goal of disrupting systems, or making them unavailable. Figure 7.4 shows a simplified view of the goal of DDoS attacks, disrupting service.

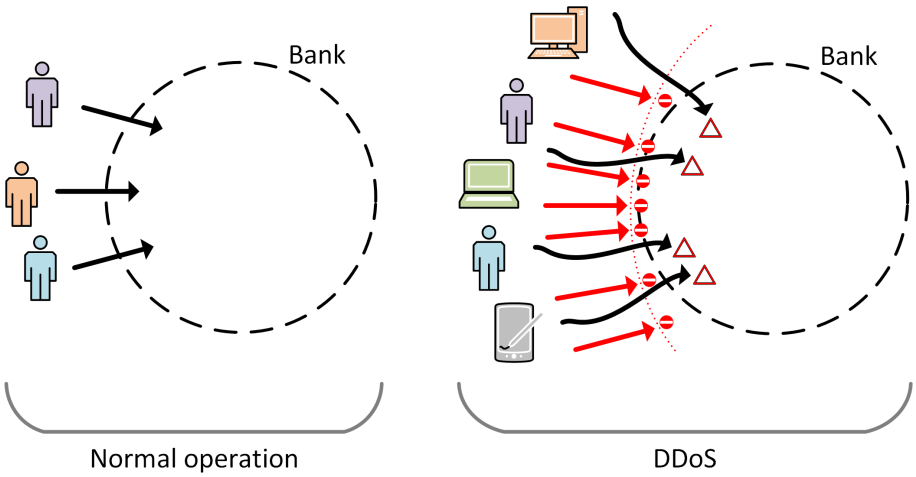

FIGURE 7.4: Difference between normal operation and pattern P20 attacks

7.4 Data validation

During the course of this research, data and information was collected from experts. This qualitative data was used as input for the framework's various components, in turn validating the researchers work that has been based on theory from the literature review.

Expert data and information was used to populate and design the likelihood, impact and risk matrices as per the design procedure explained in Section 4. The data input and accompanying flow per matrix is illustrated in an overview in Figure 7.5.

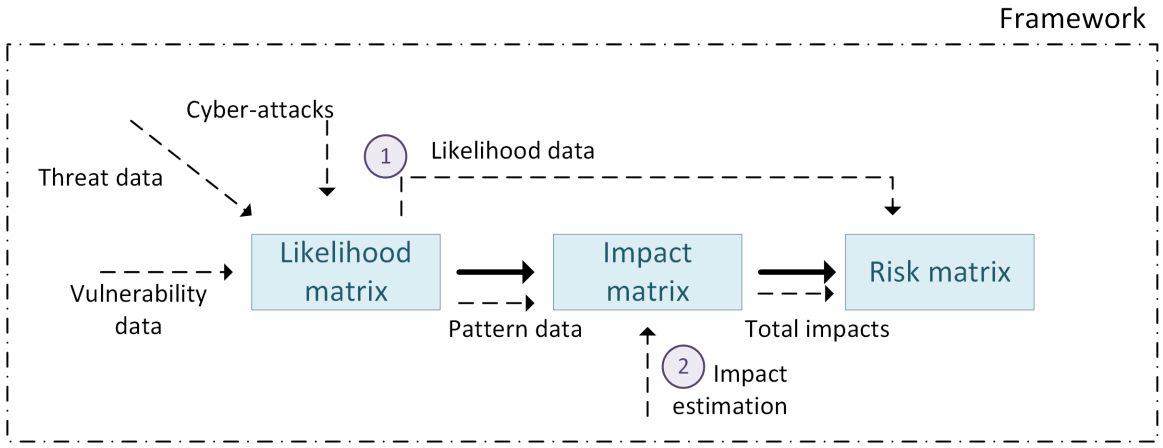

FIGURE 7.5: Input data flow showing where quantitative data is validated

Figure 7.5 shows the three areas (by means of a blue circle) where validation can be done based on feedback from experts. Tables containing the impact and likelihood estimates that experts provided are listed in Appendix A.

1 - Likelihood
In terms of the likelihood of cyber-attacks, estimates showed slight variations per expert. These variations show relative alignment between the researcher's likelihood estimate and that of the experts, the differences cannot be deemed as significant. Average standard deviations below 1 were considered to be acceptable. Table A.4 shows the results of the likelihood feedback.

The different likelihood estimates led to modifications in the framework to improve it's accuracy and correctness.

There was however more consensus amongst technical experts, and alignment with the researcher, in determining the attack pattern that is most likely to occur. Based on the attack patterns, the area that affects attack patterns the most is *process*. This is shown in Table A.1.

2 - Impact
Focusing on impact, the input provided by experts revealed significant differences in impact estimations. None of the experts provided consistent nor similar impact estimates, even when compared to the researcher's estimates based on theory. These results are shown in the Tables A.8, A.9 and A.10. The variables from the aforementioned tables are linked to their definitions in Table A.5.

An observation of the impact type data from experts showed agreement with the data the researcher had obtained from the literature review. This showed damage to an institutions reputation as the most important and common impact type.

The expert input for both impact and likelihood allowed for the risk per attack pattern to be determined. This will be discussed in 8.1.

The results from this data validation are discussed in Section 8.1.

Chapter 8

Reflection

This chapter discusses the findings of the Treatment Validation. The research questions and main goal will then be answered by means of a reflection on the areas in the thesis that contributed to answering them.

Finally, the limitations encountered during this thesis will be explained, as well as future work that can be carried out to expand on work this thesis conducted.

8.1 Discussion

During consultations, experts were noted to have different definitions for various terms and concepts. This revelation suggested that a universal terminology does not exist amongst experts with regards to IT security and risk concepts. This could, in time, lead to misunderstandings or lapses in security/risk assessment and should therefore be monitored closely.

Likelihood

Focusing specifically on the likelihood of cyber-attacks, experts were requested to estimate the likelihood that patterns could occur. Table A.4 shows the estimates per expert A[n]. The standard deviations (σ) are included to show the amount of variation in the data.

As Table A.4 shows, five experts provided likelihood feedback. Experts A1, A2 and A5 were technical experts. The mean likelihood estimates amongst all experts is 2.8, with the highest 3.1 and lowest 2.4.

The likelihood estimates showed variations per expert, although these variations cannot be deemed as significant. The variable likelihood illustrates that expert perceptions of the likelihood of attacks are not the same.

The standard deviation of the likelihoods in Table A.4 shows that the spread in estimates is not excessive as the standard deviation across all patterns-estimates is 0.968. The standard deviation of amongst technical experts is 0.550, showing that experts with technical positions tend to estimate likelihood in a similar manner. Both values, however, show that there is a relative consensus in the estimates that certain occurrences will take place.

Patterns

Technical experts provided the same likelihood estimates in 22.2% of the patterns, and it was observed that all three technical experts had higher mean likelihoods than the other experts. This can be seen as an over-estimation of an occurrence taking place, or that technical experts have higher likelihoods based on their practical experience.

Table A.4 shows that P6 is the attack pattern that is most likely to occur, followed closely by P7 (pattern definitions in Table 4.3). A look at the literature review results of recent cyber-attacks confirms the data that suggests that P6 and P7 are the most likely pattern categories to occur: attacks involving social engineering and deception.

This is likely due to the relative ease at which intruders can mislead users on their devices, and that corporate infrastructure and systems have increasingly advanced mitigation and countermeasures in place. Banking institutions have full control over the frontend and backend, but limited control over the user and their device(s). This is confirmed by Figure 4.9 in which the majority of patterns that compromise the frontend or backend are shown to initiate in the process or governance phases.

Patterns - Vulnerable areas
When examining the attack patterns, the vulnerable area *process* affects patterns the most. This is shown in Table A.1. This can be explained by the fact that processes are the steps involved in carrying out tasks or activities. Therefore weak processes, or loopholes in them, can heavily affect the impact of an attack pattern. As *process* decisions are often made at a management level, *governance* indirectly affects the process vulnerability area.

Further examination of the patterns in Table A.2 shows that *social engineering*, *malware* and *eavesdropping* (espionage) threats are the most common threats. These findings can be deemed as accurate as they are confirmed by theory from the literature and practical review as well as recent news reports.

The blue-highlights in Figure 4.9 show the vulnerable areas that threats affect. The fact that the matrix is not completely blue shows, and confirms, that threats have specific targets. In the case of a banking institution, the target is a vulnerable area in the channel between a customer and a bank. Cyber-attacks in the threat category *social engineering* and *deception* target the user specifically, whilst the *backend* is the most affected area.

Data from Table A.1 and Figure 4.9 shows that several attack patterns aim to eventually compromise the frontend or backend of a bank. However, an analysis of the data and recent cyber-attacks also shows that *users* and their *devices* are often targeted.

Patterns - Complexity
The number of steps attack patterns take is visible in Table A.3. All 4-step patterns are identical in their movement amongst vulnerable areas, starting at governance and ending with a compromise at the backend. As Table A.3 shows, most attack patterns are 2-step patterns. 8 of 9 (88.9%) 1-step patterns target *devices* and the *internet*, whereas 5 of 9 (55.6%) involve the *device* area.

This shows that the risk attack patterns pose does depend completely on the complexity of attacks.

Impact
The results of impact estimates are shown in the Tables A.8, A.9 and A.10. The variables from the aforementioned tables are linked to their definitions in Table A.5.

The variation in impact estimates illustrates that experts perceive the form and level of impact differently. The underestimation or incorrect identification of impact will have consequences for an organisation's risk assessment capabilities. This will also affect risk mitigation abilities and response.

As the expert impact tables show, the total estimates have been calculated per pattern. Analysing the data shows that only 2 experts (40%) had consensus on the pattern with the highest impact, P1. However, when taking the 3 highest impacts per pattern into account, patterns P1, P5, P10 and P11 were revealed by the 5 experts as having high impact.

The lack of consensus on the outright highest impact pattern can have severe consequences for determining risk. On the other hand, the results of analysing the top 3 impacts shows more agreement amongst the experts, which can be interpreted as a wider consensus in impact estimates.

Further observations from the expert impact tables show that the high-impact patterns have a common goal of compromising the backend of a banking institution. This supports the literature and practical review findings that the most valuable data and results remains at the backend of an organisation.

The findings of an analysis into the number of times specific impact estimations were given is in Table A.6. It revealed that *severe* and *catastrophic* impact were indicated sparsely, which show that banking institutions are not as extremely affected when an event occurs.

The only catastrophic impact estimates were given by experts in cases where the impact affects the (technical) categories *availability* and *confidentiality*. This is correct as downtime or losing trust in data stored can have grave consequences for an institution.

Experts estimated negligible impact the most for the regulatory category, evident in Table A.7. This can signify that, from a cyber-attack (or technical) perspective, banking institutions adhere to regulations and therefore have impacts that affect regulation under control.

From a banking institution's perspective, patterns that affect the *user*, *device* and *internet* do not have big consequences. The three patterns with the lowest impact estimates target these vulnerable areas

Impact - Types

Table A.7 shows the impact estimates per impact type. As the table shows, 3 of 5 (60%) experts estimated damage to a banking institution's reputation as the highest impact type. Further data analysis revealed that reputational damage was in the top 3 total impacts across all five experts.

The mean of impact types across the five experts further emphasises that reputational damage is the highest impact type, followed by confidentiality and financial impact. These statistics are in line (agree) with knowledge obtained from the literature and practical review that damage to reputation the highest, and most critical impact is.

The expert impact tables illustrate that technical experts estimated for there to be less financial impact (seen in Table A.7) than other impact types, but that financial impact would occur more often (seen in expert impact tables) than non-technical experts estimated. This can be interpreted as when financial impact occurs, it is hardly a factor when compared to the other impacts types.

Risk

In terms of overall risk, more complex multi-step patterns do not necessarily form a greater risk for a banking institution. 3 and 4 step patterns do not always form a greater risk than a 1 and 2 step pattern.

This is shown in Figure A.1 where the number of steps in a pattern is included in the risk matrix. The average risk per step-category is indicated by means of an 'X' on the matrix. As Figure A.1 shows, none of the attack patterns are a high risk to a bank. This shows that banking institutions have risks relatively under control with mitigation and counter-measures in place.

In this case, all the patterns with an impact score above 3 fall into the Medium-High risk category. Further analysis shows that these patterns all lead to a compromise at a bank's backend, which would support the theory of the patterns being a higher risk due to their intended target, should they be successful.

In terms of the average risk per step-category, only one category (2-step) is considered to be a Medium-High risk, the 3 and 4 step is considered Medium risk whilst 1-step Low-Medium. This enforces the idea that more complex patterns are not directly a higher risk for a banking institution.

When analysing the risk variation of patterns in terms of complexity, Figure A.2 shows that the risk-level of patterns is not necessarily related to the complexity of the attack. 2-step patterns

for example range from Medium-High risk to Medium, Low-Medium and Low risk. 2-step patterns are also shown to have a greater variation in the likelihood.

8.2 Conclusion

This section will briefly recap on the research questions and main goal of this thesis.

8.2.1 RQ1

What aspects of generic risk management are relevant in an IT context?

This research question was answered through the literature review and discussions with a number of experts in the fields of interest. This research focused on six fields that apply risk management concepts: insurance, weather forecasting, healthcare, game theory, economics and political.

Weather forecasting and game theory both use the concept of patterns to model likelihood, that the probability events occur may be related to or depend on other current or past occurrences. Both fields, weather forecasting in particular, acknowledge and account for the variability of impact. Current impact estimation in IT risk does not take varying impact into account, effecting accuracy of risk.

Both concepts, patterns and impact variance, are the most important concepts that this research identified as relevant to determine risk in an IT context. The findings of the review into risk management is presented in Section 3.1.1, the analysis of which is presented in the conclusion of risk management in Section 3.1.4.

8.2.2 RQ2

What defines and characterises a cyber-attack in the banking sector?

The literature review into cyber-attacks in the banking sector revealed several interesting findings. Probably the most important finding of the review is that cyber-attacks are continuously evolving, changing in their techniques and methodology.

Cyber-attacks were defined in this thesis in Section 3.1.5 as: an action executed by an (unauthorised) individual or group with a clear intention of modifying, disrupting or disabling the operations of computer systems or networked devices in an illegal manner.

There are various factors and characteristics that need to be considered when analysing cyber-attacks, making it generally a complex task to mitigate them. The findings of the literature review into cyber-attacks are presented in Section 3.1.5.

This knowledge of cyber-attacks and their characteristics was invaluable input, and laid a solid foundation for the framework design.

8.2.3 RQ3

How can multi-channel cyber-attack patterns be optimally represented?

This research question was answered and supported by the literature review as well as expert opinions. Information was obtained from experts about how they visualise models which was combined with concepts of how models were represented in scientific literature.

A standard, theoretically-proven approach for analysing risk was chosen and used as the basis for the framework. This approach involved the use of three matrices that were based on two formulas to determine risk. A likelihood, impact and risk matrix were designed.

Section 7.1 details the validation by expert reviews in which experts express their satisfaction of the framework's representation of patterns.

8.2.4 Main Goal

To design a multi-channel cyber-attack patterns-based risk modelling framework for the banking sector.

As stated, the main goal of this research was to design a risk modelling framework. The three research questions were answered during the literature review and design phase of the research and all contributed to realisation of the main goal.

The main goal of the research was successful as the validity and completeness was shown and supported by experts in Section 7.1. Section 7.4 presented quantitative data that supports the correctness of the framework, as well as an analysis and findings of the data that was used as input for the framework.

8.3 Limitations

Challenges and limitations were encountered throughout the course of this thesis. These limitations affected the overall process of this thesis as well as the design of the framework. The limitations were as follows:

- An eight-month time schedule was a relatively short period of time to conduct a thorough research whereby the researcher also had to familiarise himself with theory about the topic. The duration of the research also limited the complexity of the designed model.
- The research was conducted at one banking institution, BankY. This likely introduced subtle biases as opinions are likely to be more subjective, regardless of the emphasis on abstraction and objectivity. The majority of the experts that were spoken to worked for BankY.
- Expert availability: it was often a challenge to arrange meetings with experts due to their busy work schedules. This influenced the speed at which progress was made as well as restricted the number of experts that provided input for the framework or that could validate it.
- Banking institutions are secretive about security incidents. This made it difficult to obtain specific information from experts due to confidentiality restrictions. Researching cyber-attacks targeting banks produced less detailed results than expected, possible due to secrecy amongst banks.
- Various concepts in this research were subjective and depended on expert perception. Expert perception therefore played an influencing role in the design of the framework, the extent of which is difficult to judge.
- Due to the relatively new nature of IT risk, there was not a lot of scientific literature available, which meant that grey literature was often consulted to supplement expert opinions and the literature review findings.

8.4 Future work

Further research can be conducted that builds on concepts that have been introduced in this thesis, or that were unable to be researched and analysed further due to the time-restriction of this thesis.

The researcher identified a number of areas in which additional research can be executed in. These are as follows:

- Research alignment with similar IT risk management models in other sectors in order to develop a holistic approach. Risk management is not applied as consistently in the IT field as others,
- Validate the framework with more quantitative impact data as opposed to qualitative input. Qualitative data was used as the primary source of information for this research, which introduces subjectivity. Quantitative data would allow for feedback based purely on experience and factual data which can be seen as more objective, accurate and therefore correct.
- The current model can be expanded to include internal IT risks such as fraud, and non-intentional risks such as operational incidents. These internal risks were excluded from this research due to the fixed time period for thesis, as well as the additional complexity and scope accounting for internal risks will add.
- The risk matrix can be expanded to include and correlate resources (particularly financial) used for risk mitigation. This will support in determining the effectiveness of resource allocation to counter particular risk levels.
- The model can be adapted to validate its potential use for benchmarking purposes. Banking institutions will then be able compare their own risk with that of this framework.
- Use new technology or theory to derive probabilities for where new attack patterns might occur in the future. Details about cyber-attacks and their evolution over the past 20 years can be combined with increasingly effective statistical models to make these predictions.
- Additional research needs to be conducted to improve the technique of identifying attack patterns. This procedure should account for the varying and changing nature of cyber-attacks.
- Variables that affect the impact cyber-attacks (impact variance) have can be researched further to determine which other variables that this thesis has not identified affect impact. The extent of which additional variables affect impact also needs to be verified.
- Current literature states that $likelihood = threat \times vulnerability$, however this research feels that likelihood should be represented as $likelihood = f(threat, vulnerability)$. The relationship between variables in the likelihood formula have to be analysed further to determine their exact dependency.
- Expert perception of likelihood and impact needs to be improved to ensure consensus and accurate risk identification. Ways in which expert perception of these concepts can be improved needs to be looked into.
- The Design Science concept (Wieringa, 2014) could be expanded to include more information or guidelines to validate frameworks.

Appendix A

Data Results

A.1 Likelihood

TABLE A.1: Count of patterns affecting vulnerable areas

Vulnerability	Count
User	5
Device	10
Internet	5
Process	12
Governance	6
Frontend	8
Backend	9

TABLE A.2: Count of patterns involved per threat type

Threat	Count
Theft	2
Vulnerability exploits	3
Unauthorised access	2
Social engineering	4
Destruction	3
Malware	4
Deception	3
Eavesdropping	4
Brute-force	3
DDoS	2

TABLE A.3: Number of steps per pattern

Steps	Count	Patterns
4	3	P2, P3, P12
3	4	P1, P4, P13, P10
2	11	P11, P19, P6, P7, P8,P9, P14, P15, P16, P17, P18
1	9	P5, P20, P21, P22, P23, P24, P25, P26, P27

TABLE A.4: Pattern likelihoods and standard deviations

	Likelihood						Standard deviation σ						
	A1	**A2**	**A3**	**A4**	**A5**	μ	**All**	**A1**	**A2**	**A3**	**A4**	**A5**	**Technical**
P1	3	2	3	3	2	2,6	0,548	0,283	0,424	0,283	0,283	0,424	0,577
P2	3	3	4	2	3	3	0,707	0,000	0,000	0,707	0,707	0,000	0,000
P3	3	2	1	2	3	2,2	0,837	0,566	0,141	0,849	0,141	0,566	0,577
P4	4	4	1	4	5	3,6	1,517	0,283	0,283	1,838	0,283	0,990	0,577
P5	2	3	2	1	2	2	0,707	0,000	0,707	0,000	0,707	0,000	0,577
P6	5	5	5	4	5	4,8	0,447	0,141	0,141	0,141	0,566	0,141	0,000
P7	5	5	3	5	5	4,6	0,894	0,283	0,283	1,131	0,283	0,283	0,000
P8	4	4	1	4	5	3,6	1,517	0,283	0,283	1,838	0,283	0,990	0,577
P9	4	4	2	4	3	3,4	0,894	0,424	0,424	0,990	0,424	0,283	0,577
P10	3	3	1	2	2	2,2	0,837	0,566	0,566	0,849	0,141	0,141	0,577
P11	3	3	1	2	2	2,2	0,837	0,566	0,566	0,849	0,141	0,141	0,577
P12	1	1	3	1	2	1,6	0,894	0,424	0,424	0,990	0,424	0,283	0,577
P13	2	2	4	3	2	2,6	0,894	0,424	0,424	0,990	0,283	0,424	0,000
P14	3	3	1	4	4	3	1,225	0,000	0,000	1,414	0,707	0,707	0,577
P15	2	1	5	2	2	2,4	1,517	0,283	0,990	1,838	0,283	0,283	0,577
P16	3	2	4	2	2	2,6	0,894	0,283	0,424	0,990	0,424	0,424	0,577
P17	2	3	1	1	3	2	1,000	0,000	0,707	0,707	0,707	0,707	0,577
P18	2	2	1	1	2	1,6	0,548	0,283	0,283	0,424	0,424	0,283	0,000
P19	5	5	1	2	4	3,4	1,817	1,131	1,131	1,697	0,990	0,424	0,577
P20	3	3	5	2	5	3,6	1,342	0,424	0,424	0,990	1,131	0,990	1,155
P21	5	5	4	2	1	3,4	1,817	1,131	1,131	0,424	0,990	1,697	2,309
P22	3	3	3	2	2	2,6	0,548	0,283	0,283	0,283	0,424	0,424	0,577
P23	2	2	3	2	3	2,4	0,548	0,283	0,283	0,424	0,283	0,424	0,577
P24	3	4	2	3	2	2,8	0,837	0,141	0,849	0,566	0,141	0,566	1,000
P25	2	2	2	1	2	1,8	0,447	0,141	0,141	0,141	0,566	0,141	0,000
P26	2	1	5	2	2	2,4	1,517	0,283	0,990	1,838	0,283	0,283	0,577
P27	4	4	3	3	3	3,4	0,548	0,424	0,424	0,283	0,283	0,283	0,577
μ	3,1	3,0	2,6	2,4	2,9	2,8	0,968	0,346	0,471	0,869	0,456	0,456	0,550

A.2 Impact

TABLE A.5: Impact type reference variables

Impact type	Reference
Financial	a
Regulatory	b
Reputation	c
Availability	d
Confidentiality	e
Integrity	f

TABLE A.6: Impact estimates spread (percentages) per expert

	Negligible	Low	Moderate	Significant	Severe	Catastrophic
A1	24.1	11.7	30.9	23.5	8.0	1.9
A3	43.8	0.0	11.1	32.7	12.3	0.0
A5	42.6	17.3	21.0	4.9	13.6	0.6
A6	0.0	22.2	29.0	33.3	15.4	0.0
A2	35.2	2.5	17.9	27.2	17.3	0.0

TABLE A.7: Total and average impact estimations per type

	A1	A3	A5	A6	A2	$\sum$	μ
Financial	77	144	166	147	230	764	152.8
Regulatory	53	30	15	182	8	288	57.6
Reputation	222	264	143	276	213	1118	223.6
Availability	149	49	50	153	151	552	110.4
Confidentiality	173	257	110	219	227	986	197.2
Integrity	170	125	129	133	135	692	138.4

TABLE A.8: Expert A1 and A3 impact estimations per pattern

	Expert A1						
	a	b	c	d	e	f	∑
P1	16	4	9	9	16	9	63
P2	4	4	4	9	9	9	39
P3	4	4	4	4	9	9	34
P4	1		16				17
P5	9	1	9	9	9	9	46
P6	1		16		9	9	35
P7			16		4	1	21
P8			9		4	1	14
P9	1		16		9	9	35
P10	4	4	9	9	16	16	58
P11	4	4	9	9	16	16	58
P12	4	1	4	9	9	9	36
P13	1	1	16		4	9	31
P14	4		1	4	4	4	17
P15	4	4	1	4	9	9	31
P16		4	4		4	4	16
P17		1		25	4	4	34
P18	4	1	4	4	9	9	31
P19	4	9	16	25			54
P20	4	9	16	25			54
P21	4	1	9		4	4	22
P22	1	1	9		4	4	19
P23	1		9		4	4	18
P24			4		4	4	12
P25			4	4			8
P26	1		4		9	9	23
P27	1		4		4	9	18
∑	77	53	222	149	173	170	

	Expert A3						
	a	b	c	d	e	f	∑
P1	16		16		16		48
P2			9	4	9	9	31
P3			9	4	9	9	31
P4	9		9		9	4	31
P5	16		16		16		48
P6					16		16
P7	9		9		9	9	36
P8	9		9		9	9	36
P9	16		16		16		48
P10	9	4	16		16		45
P11			16		16		32
P12		9	16		9		34
P13		9	16		9		34
P14			9		9		18
P15	9		9		9	9	36
P16	9		9		9	9	36
P17			9		9	9	27
P18			9		9	9	27
P19	4	4	16	16			40
P20	4	4	16	16			40
P21	4		4		9		17
P22	9		9	9	9	9	45
P23			4		4	4	12
P24	4		9		9	9	31
P25	4				4	9	17
P26	4				9	9	22
P27	9		4		9	9	31
∑	144	30	264	49	257	125	

TABLE A.9: Expert A5 and A6 impact estimations per pattern

	Expert A5						
	a	**b**	**c**	**d**	**e**	**f**	∑
P1	4	1	16		25		46
P2	4	1	4				9
P3	4	1	4				9
P4	4		9			4	17
P5	16	1	1	16		16	50
P6	4		16			16	36
P7	4		4			4	12
P8	4				16	16	36
P9	4		16			16	36
P10	16	1	1			4	22
P11	16	1	1			4	22
P12	4	1	1			4	10
P13	1		4		9	4	18
P14	4	1	16		9	16	46
P15	1		1		9	4	15
P16	1		4				5
P17	4		1				5
P18	16	1					17
P19	16		1	16			33
P20	4	1	1	16			22
P21	16	4	16		16		52
P22	1		1		9		11
P23					4	4	8
P24	1		1	1			3
P25	4		4	1		4	13
P26	4		4		4	4	16
P27	9	1	16		9	9	44
∑	166	15	143	50	110	129	

	Expert A6						
	a	**b**	**c**	**d**	**e**	**f**	∑
P1	4	9	9	1	9	4	36
P2	4	4	16	16	9	9	58
P3	4	4	16	16	16	9	65
P4	9	4	4	1	9	1	28
P5	4	16	16	16	4	16	72
P6	9	4	9	1	9	1	33
P7	9	4	9	1	9	1	33
P8	4	4	4	1	9	1	23
P9	4	4	9	1	9	1	28
P10	9	9	16	16	16	16	82
P11	9	9	16	16	16	16	82
P12	9	9	16	1	9	4	48
P13	9	9	16	1	9	4	48
P14	1	4	4	1	4	1	15
P15	4	4	4	1	4	1	18
P16	4	9	9	1	9	4	36
P17	4	9	16	1	9	4	43
P18	9	9	16	1	9	9	53
P19	4	9	9	16	1	1	40
P20	4	9	9	16	1	1	40
P21	4	9	9	1	9	1	33
P22	4	4	4	1	9	4	26
P23	9	4	4	16	16	9	58
P24	1	1	9	1	1	1	14
P25	4	9	9	4	1	9	36
P26	4	9	9	4	9	1	36
P27	4	4	9	1	4	4	26
∑	147	182	276	153	219	133	

TABLE A.10: Expert A2 impact estimations per pattern

	Expert A2						
	a	b	c	d	e	f	∑
P1	16		16		9		41
P2	9		16	9	4	9	47
P3	16		9		9	9	43
P4	4		9		16	16	45
P5	9		16	16			41
P6	16		16		9	9	50
P7	16		9		16		41
P8	4		4		16		24
P9	4		1		16		21
P10	9	4	4	9	4	4	34
P11	16	4	9	16	4	4	53
P12	4		4		9	9	26
P13	4		9		16	1	30
P14	9		9		9		27
P15	16		9	4	16	9	54
P16	4		9		9	4	26
P17	9		9	4	4		26
P18	16		9	9	16	9	59
P19	9		16	16			41
P20	16		16	16			48
P21	4		1	9	9		23
P22	4		4		9	9	26
P23				9	9	9	27
P24	4		4	9		9	26
P25	4		1	16		16	37
P26	4		4		9		17
P27	4			9	9	9	31
∑	230	8	213	151	227	135	

A.3 Risk

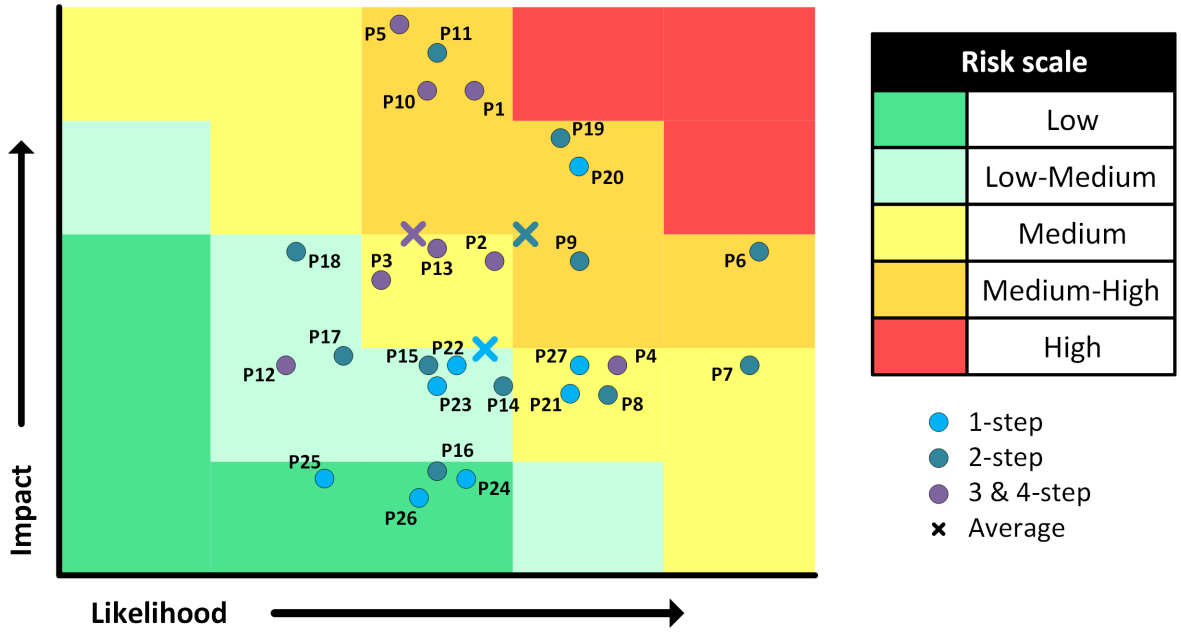

FIGURE A.1: Visualisation of pattern risk per number of steps

TABLE A.11: Count of patterns per risk category

Risk category	Steps		Σ
	Number	Count	
High	1	0	0
	2	0	
	3 & 4	0	
Medium-High	1	1	8
	2	4	
	3 & 4	3	
Medium	1	2	8
	2	2	
	3 & 4	4	
Low-Medium	1	2	7
	2	4	
	3 & 4	1	
Low	1	3	4
	2	1	
	3 & 4	0	

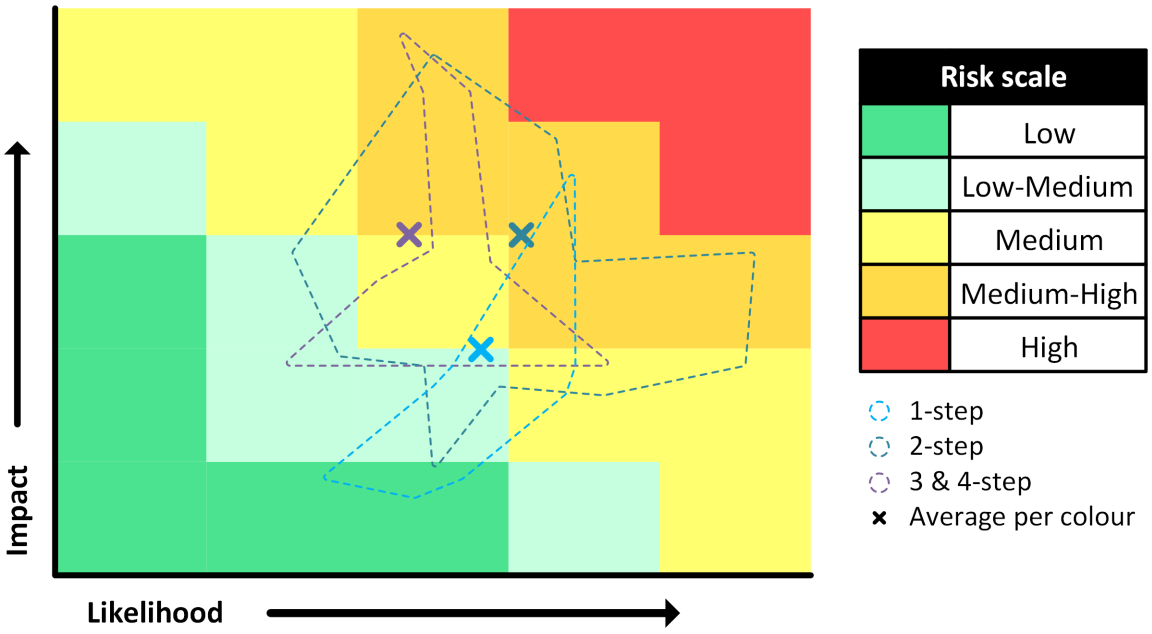

FIGURE A.2: Visualisation of risk variation in patterns per number of steps

Appendix B

Attack-pattern mapping

ATTACK	YEAR	SOURCE	PATTERN				
South korean credit card theft	2014	https://www.bbc.com/news/technology-25808189	P1				
HSBC Data breach	2018	https://www.bbc.com/news/technology-46117963	P1	P16	P18	P3	
		https://threatpost.com/hsbc-data-breach-hits-online-banking-customers/138856/					
		https://securitytoday.com/articles/2018/11/08/hsbc-bank-discloses-security-incident.aspx					
Qatar national bank data breach	2016	https://www.bankinfosecurity.com/qatar-national-bank-suffers-massive-breach-a-9068	P1				
Data breaches Canadian banks	2018	https://www.insurancejournal.com/news/international/2018/05/29/490457.htm	P1				
Cyber attack Mexico (Financial theft)	2018	https://www.welivesecurity.com/2018/06/05/cyberattack-on-banks-mexico-cybersecurity/	P2				
Phishing Belgian bank	2018	https://www.theregister.co.uk/2018/04/06/belgian_bank_argenta_outage_botched_it_infrastructure_upgrade/	P4				
CamuBot phishing Brazilian bank	2018	https://www.darkreading.com/attacks-breaches/attackers-employ-social-engineering-to-distribute-new-banking-trojan/d/d-id/1332731	P6				
		https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/camouflaged-trojan-camubot-targets-brazilian-bankers-via-unique-phishing-scheme					
Metro bank attack	2019	https://www.telegraph.co.uk/technology/2019/02/01/metro-bank-hit-cyber-attack-used-empty-customer-accounts/	P7	P13	P12		
		https://www.itpro.co.uk/security/32898/metro-bank-targeted-with-2fa-bypassing-ss7-attacks					
Banking malware network sniffing	2014	https://thehackernews.com/2014/06/new-banking-malware-with-network.html	P8	P26	P14	P15	
		https://blog.trendmicro.com/trendlabs-security-intelligence/new-banking-malware-uses-network-sniffing-for-data-theft/	P8				
Dark Tequila (Mexico)	2013	https://www.zdnet.com/article/mexicans-served-with-dark-tequila-in-spyware-spree/	P7	P21			
		https://securelist.com/dark-tequila-anejo/87528/					
Carbanak	2013	https://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html	P6	P1	P10	P3	P15
		https://thehackernews.com/2015/02/hacker-malware-bank-heist.html					
		https://securelist.com/the-great-bank-robbery-the-carbanak-apt/68732/					

		https://thehackernews.com/2018/08/fin7-carbanak-cobalt-hackers.html					
Trickbot Trojan	2017	https://thehackernews.com/2017/08/trickbot-banking-trojan.html	P7				
BankBot Trojan	2017	https://thehackernews.com/2017/04/android-banking-malware.html	P13				
NIC Asia Bank SWIFT attack	2017	https://www.bankinfosecurity.com/report-attackers-hacked-nepalese-banks-swift-server-a-10437	P10	P11			P3
Far Eastern bank SWIFT attack	2017	https://www.bankinfosecurity.com/report-malware-wielding-hackers-hit-taiwanese-bank-a-10368	P10	P11			P3
		https://www.finextra.com/newsarticle/31174/taiwans-far-eastern-international-bank-suffers-malware-attack					
Globex bank SWIFT attack	2017	https://www.reuters.com/article/us-russia-cyber-globex/russias-globex-bank-says-hackers-targeted-its-swift-computers-idUSKBN1EF294	P10	P11			P3
Bangladesh SWIFT attack	2016	https://www.bankinfosecurity.com/report-swift-hacked-by-bangladesh-bank-attackers-a-9061	P9	P10	P11		P3
		https://money.cnn.com/2016/03/14/technology/new-york-fed-bank-robbers/?iid=EL					
2018 Dutch bank DDoS'	2018	https://www.nu.nl/internet/5286176/rabobank-en-abn-amro-zondag-weer-getroffen-ddos-aanval.html	P20				
Operation Ababil (DDoS attack)	2012	https://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html	P20				
DarkSeoul	2013	https://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html	P9				
Estonia DDos attack	2007	https://www.bbc.com/news/39655415	P20	P1			
		https://scholarcommons.usf.edu/cgi/viewcontent.cgi					
		https://www.cnbc.com/2018/09/21/when-this-country-faced-a-suspected-russian-cyberattack--it-took-some-big-steps-to-stop-another.html					
Tyupkin ATM attack	2014	https://securelist.com/tyupkin-manipulating-atm-machines-with-malware/66988/	P10				P3
(not)Petya Ukraine attack	2017	https://www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-company-airport-rozenko-pavlo-cabinet-a7810471.html	P10	P11			P3
WannaCry Russian banks	2017	https://www.reuters.com/article/us-cyber-attack-russia-cenbank-idUSKCN18F16V	P10	P11			P3
Sberbank DDoS attacks	2018	https://financefeeds.com/sberbank-fends-off-62-ddos-attacks-since-start-2018/	P20				
		https://www.hackread.com/russia-alfa-bank-target-with-dns-botnet-attacks/	P12	P10	P2		P3

Alfa bank attack	2017	https://www.reuters.com/article/us-russia-cyber-banks/hackers-hit-russian-bank-customers-planned-international-cyber-raids-idUSKBN18I0VE					
Pushnik - QIWI payment system attack	2011	https://www.spamfighter.com/News-15978-Virus-Attacks-Terminals-of-QIWI-Payment-System.htm	P11	P2			P3
NotPetya BNP Paribas	2017	https://www.reuters.com/article/us-cyber-attack-bnp-paribas/cyber-attack-hits-property-arm-of-french-bank-bnp-paribas-idUSKBN19J0TH	P10	P11			P3
		https://www.cbc.ca/news/technology/ransomware-attack-hits-property-arm-of-france-bank-bnp-paribas-1.4181148					
Fake mobile app attack	2018	https://www.rbth.com/science-and-tech/328381-russian-hacker-scored-8000-day	P6	P7	P13		
PIR bank attack (AWS CBR)	2018	https://www.group-ib.com/media/new-attack-moneytaker/	P10	P11	P2	P23	(P3)
		https://securityaffairs.co/wordpress/74586/cyber-crime/moneytaker-cyber-heist.html					
		https://www.theregister.co.uk/2017/12/11/russian_bank_hackers_moneytaker/	(P27)				
STAR card processing attack	2016	Access was gained to First Data's STAR network portal, allowing easier attacks for money mules to do cash withdrawls	P2				
Banco del Austro Ecuador SWIFT attack	2015	https://money.cnn.com/2016/05/20/news/swift-bank-attack-global-ecuador/?iid=EL	P10	P11	P3		
Tien Phong Commercial Joint Stock Bank attack	2016	https://www.bankinfosecurity.com/vietnamese-bank-blocks-1-million-swift-heist-a-9105	P10	P11			P3
ATM Jackpotting Attacks	2016	https://www.databreachtoday.com/report-european-banks-struck-by-atm-jackpotting-attacks-a-9556	P10	P11			P3
		https://www.databreachtoday.com/ripper-atm-malware-where-will-cybercriminals-strike-next-a-9373					
		https://www.bankinfosecurity.com/atm-heist-in-japan-a-9265					
DNC Zero-day flaw	2016	https://www.databreachtoday.com/microsoft-says-russian-dnc-hackers-targeted-zero-day-flaws-a-9495	P22				
Tesco bank attack	2016	https://www.zdnet.com/article/tesco-bank-fined-16-4m-over-cyber-attack/	P2				
HSBC data vulnerability	2009	https://threatpost.com/hsbc-warns-exposed-customer-info-120709/73214/	P1	P2			
		https://www.computerworld.com/article/2521488/hsbc-exposed-sensitive-bankruptcy-data.html					
HSBC DDoS attack	2012	https://threatpost.com/hsbc-sites-knocked-offline-large-scale-dos-attack-101912/77133/	P20				

Commonwealth bank breach	2013	https://www.cyberwarnews.info/2013/04/02/uk-commonwealth-bank-site-hacked-data-leaked/	P1				
BoA 3rd party attack	2013	https://www.computerworld.com/article/2495684/bank-of-america-says-data-breach-occured-at-third-party.html	P21				
BoA DDoS	2012	https://www.esecurityplanet.com/network-security/bank-of-america-hit-by-apparent-cyber-attack.html	P20				
		https://money.cnn.com/2012/09/18/technology/bank-of-america-site-down/index.html?iid=EL					
Chase DDoS	2012	https://money.cnn.com/2012/09/19/technology/chase-site-slow/index.html?iid=EL	P20				
DDoS Dutch banks	2013	https://news.softpedia.com/news/Online-Services-of-Dutch-Banks-Disrupted-by-DDOS-Attacks-343468.shtml	P20				
Mercersburg cyber attack	2013	http://www.ehackingnews.com/2013/04/first-national-bank-security-breach.html	P2				
Regions bank DDoS	2013	https://www.americanbanker.com/news/regions-bank-hit-with-cyberattack	P20				
Cosmos bank attack	2018	https://www.zdnet.com/article/how-hackers-managed-to-steal-13-5-million-in-cosmos-bank-heist/	P10	P11	P6	P23	P3
Coast Capital bank attack	2018	https://www.cbc.ca/news/canada/british-columbia/coast-capital-savings-cyber-attacks-1.4977944	P7	P16			
Banco de Chile	2018	https://threatpost.com/banco-de-chile-wiper-attack-just-a-cover-for-10m-swift-heist/132796/	P2	P10	P11		P3
Bancomext SWIFT attack	2018	https://www.bloomberg.com/news/articles/2018-05-29/mexico-foiled-a-110-million-bank-heist-then-kept-it-a-secret	P10	P11			P3
Chilean bank	2018	https://socprime.com/en/news/chilean-bank-suffered-destructive-cyber-attack/					
Tien Phong bank swift attack	2016	https://www.reuters.com/article/us-vietnam-cybercrime/vietnam-bank-says-interrupted-cyber-heist-using-swift-messaging-idUSKCN0Y60EN	P10	P11			P3
Nonghyup bank attack	2011	https://www.bbc.com/news/world-asia-pacific-13263888	P10	P11			P3
Poland malware attack	2017	https://www.pcworld.com/article/3166456/polish-banks-on-alert-after-mystery-malware-found-on-computers.html	P10	P11	P2		P3
		https://www.csoonline.com/article/3169585/recent-malware-attacks-on-polish-banks-tied-to-wider-hacking-campaign.html					
Valetta attack	2019	https://www.reuters.com/article/us-bank-valetta-cyber-idUSKCN1Q21KZ	P10	P11			P3
Wells Fargo bank attack	2012	https://www.esecurityplanet.com/network-security/social-engineering-attack-nets-2.1-million-from-wells-fargo-bank.html	P4				

Wells Fargo bank attack	2012	https://www.helpnetsecurity.com/2012/03/01/21-million-stolen-with-clever-social-engineering/					
Pathe fraud	2018	https://www.parool.nl/binnenland/ceo-fraude-kostte-pathe-19-miljoen-euro~a4607439/	P4				
Bankasi bank phishing attack	2018	https://blog.comodo.com/comodo-news/phishing-attacks-in-turkish-banks/	P4				
Indian banks credit card comprimises	2016	https://economictimes.indiatimes.com/industry/banking/finance/banking/3-2-million-debit-cards-compromised-sbi-hdfc-bank-icici-yes-bank-and-axis-worst-hit/articleshow/54945561.cms	P10	P11			
Masterard unauthorised access breach	2012	https://arstechnica.com/information-technology/2012/03/massive-credit-card-breach-reportedly-hits-visa-mastercard/	P3				
		https://krebsonsecurity.com/2012/03/mastercard-visa-warn-of-processor-breach/					
		https://arstechnica.com/information-technology/2012/04/frequently-asked-questions-about-a-hack-that-may-affect-10-million-credit-cards/					
Valartis bank attack	2013	https://www.bleepingcomputer.com/news/security/customers-of-liechtenstein-bank-blackmailed-by-unknown-hackers/	P1	P2	P3		
Odinaff trojan	2016	https://www.symantec.com/connect/blogs/odinaff-new-trojan-used-high-level-financial-attacks	P15	P13	P11		
Fakebank mobile app attack	2013	https://www.symantec.com/security-center/writeup/2013-101114-5645-99	P6	P21	P27		
Marcher banking trojan	2017	https://www.scmagazineuk.com/marcher-banking-trojan-campaign-attacks-austrians-finances-three-different-ways/article/1473836	P6	P7			
Bankosy attack	2014	https://www.symantec.com/security-center/writeup/2014-072316-5249-99	P6	P21	P9		
Dyre attack	2015	Spam campaigns were set up that contained a malicious attachment that, when opened, installs malware	P6	P22			
		https://www.computerworld.com/article/3131621/dyre-banking-trojan-successor-rears-its-ugly-head.html					
VPNFilter malware	2018	https://www.symantec.com/blogs/threat-intelligence/vpnfilter-iot-malware	P22	P23			
		http://www.digitaljournal.com/tech-and-science/technology/reviewing-the-impact-of-the-vpnfilter-malware-attack/article/526317					
Bad Rabbit malware Russian banks	2017	https://www.bbc.com/news/technology-41740768	P3	P10	P11		
GozNym attack Germany	2016	https://threatpost.com/goznym-banking-trojan-targeting-german-banks/120075/	P8	P7	P6		
Neverquest trojan attack		https://www.kaspersky.com/blog/neverquest-trojan-built-to-steal-from-hundreds-of-banks/3247/	P6	P7	P8		

Spectre & Meltdown vulnerabilities	2018	https://securityintelligence.com/spectre-meltdown-and-more-what-you-need-to-know-about-hardware-vulnerabilities/	P22	P24	P21		
		https://www.theregister.co.uk/2018/01/04/intel_amd_arm_cpu_vulnerability/					
Slingshot attack/vulnerability	2012	https://threatpost.com/cyber-espionage-campaign-slingshot-targets-victims-via-routers/130348/	P23	P26	P15		
Heartbleed vulnerability	2016	https://www.synopsys.com/blogs/software-security/heartbleed-bug/	P22	P2			
Banco de Espana DDoS	2018	https://www.bankinfosecurity.com/bank-spain-hit-by-ddos-attack-a-11430	P21				
Device zero-days		https://motherboard.vice.com/en_us/article/gyakgw/the-prototype-dev-fused-iphones-that-hackers-use-to-research-apple-zero-days	P22				
Jokra attack	2013	https://www.eweek.com/security/cyber-attack-wipes-data-from-hard-drives-at-major-south-korean-firms		P24	P11		
		https://www.itnews.com.au/news/data-destruction-motive-for-massive-malware-attack-337606					
Emolet	2014	https://www.malwarebytes.com/emotet/	P6				
		https://www.symantec.com/blogs/threat-intelligence/evolution-emotet-trojan-distributor					
MysteryBot	2018	https://www.zdnet.com/article/this-new-android-malware-delivers-banking-trojan-keylogger-and-ransomware/	P6	P7	P8		
DigiNotar attack	2011	https://scholarcommons.usf.edu/cgi/viewcontent.cgi	P23	P2			
		https://slate.com/technology/2016/12/how-the-2011-hack-of-diginotar-changed-the-internets-infrastructure.html					
		https://threatpost.com/final-report-diginotar-hack-shows-total-compromise-ca-servers-103112/77170/					
		https://www.computerworld.com/article/2493095/one-year-after-diginotar-breach--fox-it-details-extent-of-compromise.html					
Comodo CA attack	2011	https://threatpost.com/phony-ssl-certificates-issued-google-yahoo-skype-others-032311/75061/	P23				
RSA SecurID attack	2011	https://www.wsj.com/articles/SB10001424052702304906004576369990616694366	P6	P23	P1		
		https://threatpost.com/rsa-securid-attack-was-phishing-excel-spreadsheet-040111/75099/					
		https://arstechnica.com/information-technology/2011/06/rsa-finally-comes-clean-securid-is-compromised/					

		https://www.bankinfosecurity.com/tricked-rsa-worker-opened-backdoor-to-apt-attack-a-3504					
Lockheed Martin attack	2011	https://www.reuters.com/article/us-usa-defense-hackers/exclusive-hackers-breached-u-s-defense-contractors-idUSTRE74Q6VY20110527	P23	P2			
KeyRaider Jailbreak attack	2015	https://blog.avast.com/2015/09/02/apple-jailbroken-phones-hit-with-malware/	P9				
		https://www.intego.com/mac-security-blog/225000-reasons-not-to-jailbreak-your-iphone-ios-malware-in-the-wild/					
T-Mobile website bug	2017	https://motherboard.vice.com/en_us/article/wjx3e4/t-mobile-website-allowed-hackers-to-access-your-account-data-with-just-your-phone-number	P4	P2	P1		
AT&T server security exploit	2010	https://gawker.com/5559346/apples-worst-security-breach-114000-ipad-owners-exposed	P1	P2			
T-mobile sim swap attack	2017	https://motherboard.vice.com/en_us/article/a37epb/t-mobile-alert-victims-sim-card-hack	P4				
SS7 telecom vulnerability	2014	https://www.wired.com/2016/04/the-critical-hole-at-the-heart-of-cell-phone-infrastructure/	P23	P2			
		https://www.adaptivemobile.com/blog/tracking-the-trackers					
Bengalurean sim swap attack	2016	https://timesofindia.indiatimes.com/city/bengaluru/many-bengalureans-lose-cash-to-sim-card-swap-fraud/articleshow/58387867.cms	P4				
Silicon valley sim swapping attack	2018	https://nypost.com/2018/11/20/man-hacked-into-silicon-valley-execs-phones-to-steal-cryptocurrency-cops/	P4				
Mazarbot screen overlay attack	2016	https://lukasstefanko.com/2016/02/android-mazarbot-stealing-credit-card-information-in-italy-with-certified-issued-by-putin.html	P6				
BankBot screen overlay attack	2017	https://www.infosecurity-magazine.com/news/bankbot-android-trojan-reemerges/	P6				
		https://www.zdnet.com/article/bankbot-android-malware-sneaks-into-the-google-play-store-for-the-third-time/					
		https://www.paymentssource.com/opinion/self-protection-can-shield-banks-from-new-android-bankbot-card-malware					
Phishing Nederlandse banken 2018	2018	https://www.nu.nl/internet/5811852/bijna-4-miljoen-euro-schade-bij-banken-door-phishing-in-2018.html	P7				
		https://nos.nl/artikel/2277755-schade-banken-door-phishing-neemt-explosief-toe.html					

Phishing attack dutch banks and telecoms	2018	https://www.nu.nl/internet/5778129/man-aangehouden-voor-op-banken-en-telecomproviders-gerichte-phishing.html	P7				
BMO and Simpli data breach	2014	https://www.cbc.ca/news/business/bank-hack-tuesday-1.4682018	P1				

Bibliography

Accenture (2017). *2017 Cost of Cyber Crime Study*. Tech. rep. URL: https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf.

Adeoti, Johnson Olabode (2011). "Automated teller machine (ATM) frauds in Nigeria: The way out". In: *Journal of Social Sciences* 27.1, pp. 53–58.

AFP (2019). *Warning Issued Over Attacks on Internet Infrastructure*. URL: https://www.securityweek.com/warning-issued-over-attacks-internet-infrastructure.

Alhawari, Samer et al. (2012). "Knowledge-based risk management framework for information technology project". In: *International Journal of Information Management* 32.1, pp. 50–65.

BBC (2014). *Credit card details on 20 million South Koreans stolen*. URL: https://www.bbc.com/news/technology-25808189.

Ben-Asher, Noam and Cleotilde Gonzalez (2015). "Effects of cyber security knowledge on attack detection". In: *Computers in Human Behavior* 48, pp. 51–61.

Boehm, Barry W (1991). "Software risk management: principles and practices". In: *IEEE software* 8.1, pp. 32–41.

Boone, Harry N and Deborah A Boone (2012). "Analyzing likert data". In: *Journal of extension* 50.2, pp. 1–5.

Briscoe, Neil (2000). "Understanding the OSI 7-layer model". In: *PC Network Advisor* 120.2.

Brook, Chris (2012). *HSBC Sites Knocked Offline in 'Large Scale' DoS Attack*. URL: https://threatpost.com/hsbc-sites-knocked-offline-large-scale-dos-attack-101912/77133.

Camillo, Mark (2017). "Cybersecurity: Risks and management of risks for global banks and financial institutions". In: *Journal of Risk Management in Financial Institutions* 10.2, pp. 196–200.

Case, Defense Use (2016). "Analysis of the cyber attack on the Ukrainian power grid". In: *Electricity Information Sharing and Analysis Center (E-ISAC)*.

Cebenoyan, A Sinan and Philip E Strahan (2004). "Risk management, capital structure and lending at banks". In: *Journal of Banking & Finance* 28.1, pp. 19–43.

Chen, Injazz J and Karen Popovich (2003). "Understanding customer relationship management (CRM) People, process and technology". In: *Business process management journal* 9.5, pp. 672–688.

Choo, Kim-Kwang Raymond (2011). "The cyber threat landscape: Challenges and future research directions". In: *Computers & Security* 30.8, pp. 719–731.

Cybersecurity, Critical Infrastructure (2014). "Framework for Improving Critical Infrastructure Cybersecurity". In: *Framework* 1, p. 11.

Dahbur, Kamal, Bassil Mohammad, and Ahmad Bisher Tarakji (2011). "A survey of risks, threats and vulnerabilities in cloud computing". In: *Proceedings of the 2011 International conference on intelligent semantic Web-services and applications*. ACM, p. 12.

Deloitte (2016). *Political risk: How market leaders create resiliency in uncertain times*. URL: https://www2.deloitte.com/us/en/pages/risk/articles/political-risk-management.html.

Denning, Peter J and Dorothy E Denning (2010). "Discussing cyber attack". In: *Communications of the ACM* 53.9, pp. 29–31.

Disterer, Georg (2013). "ISO/IEC 27000, 27001 and 27002 for information security management". In: *Journal of Information Security* 4.02, p. 92.

Ehrenfeld, Jesse M (2017). "Wannacry, cybersecurity and health information technology: A time to act". In: *Journal of medical systems* 41.7, p. 104.

Evans, Pete (2018). *Hackers threaten to reveal personal data of 90,000 Canadians caught in bank hack*. URL: https://www.cbc.ca/news/business/bank-hack-tuesday-1.4682018.

Fredriksen, Rune et al. (2002). "The CORAS framework for a model-based risk management process". In: *International Conference on Computer Safety, Reliability, and Security*. Springer, pp. 94–105.

Goldman, Jeff (2012). *Bank of America Hit by Apparent Cyber Attack*. URL: https://www.esecurityplanet.com/network-security/bank-of-america-hit-by-apparent-cyber-attack.html.

Gordon, Lawrence A, Martin P Loeb, and Tashfeen Sohail (2003). "A framework for using insurance for cyber-risk management". In: *Communications of the ACM* 46.3, pp. 81–85.

Handel, Theodore G and Maxwell T Sandford (1996). "Hiding data in the OSI network model". In: *International Workshop on Information Hiding*. Springer, pp. 23–38.

Hathaway, Oona A et al. (2012). "The law of cyber-attack". In: *California Law Review*, pp. 817–885.

Hellwig, Martin et al. (1995). "Systemic aspects of risk management in banking and finance". In: *REVUE SUISSE D ECONOMIE POLITIQUE ET DE STATISTIQUE* 131, pp. 723–738.

Impe, Koen van (2017). *Simplifying Risk Management*. URL: https://securityintelligence.com/simplifying-risk-management.

Julisch, Klaus (2013). "Understanding and overcoming cyber security anti-patterns". In: *Computer Networks* 57.10, pp. 2206–2211.

Kalashnikoff, Arseny (2018). *Russian hacker ... fake mobile bank app*. URL: https://www.rbth.com/science-and-tech/328381-russian-hacker-scored-8000-day.

Kaspersky (2017).

Kennedy Jr, Charles R (1988). "Political risk management: A portfolio planning model". In: *Business Horizons* 31.6, pp. 26–33.

Khurana, Himanshu et al. (2010). "Smart-grid security issues". In: *IEEE Security & Privacy* 8.1.

Kitchenham, Barbara (2004). "Procedures for performing systematic reviews". In: *Keele, UK, Keele University* 33.2004, pp. 1–26.

Kobrin, Stephen J (1979). "Political risk: A review and reconsideration". In: *Journal of international business studies* 10.1, pp. 67–80.

Kong, Jiejun, Xiaoyan Hong, and Mario Gerla (2003). "A new set of passive routing attacks in mobile ad hoc networks". In: *Military Communications Conference, 2003. MILCOM'03. 2003 IEEE*. Vol. 2. IEEE, pp. 796–801.

Laszka, Aron, Benjamin Johnson, and Jens Grossklags (2013). "Mitigation of targeted and non-targeted covert attacks as a timing game". In: *International Conference on Decision and Game Theory for Security*. Springer, pp. 175–191.

Lehar, Alfred (2005). "Measuring systemic risk: A risk management approach". In: *Journal of Banking & Finance* 29.10, pp. 2577–2603.

MacMinn, Richard D (1987). "Insurance and corporate risk management". In: *Journal of Risk and Insurance*, pp. 658–677.

Malwarebytes (2018). *Emotet malware*. URL: https://www.malwarebytes.com/emotet.

McGuinness, Damien (2017). *How a cyber attack transformed Estonia*. URL: https://www.bbc.com/news/39655415.

McMillan, Robert (2009). *HSBC exposed sensitive bankruptcy data*. URL: https://www.computerworld.com/article/2521488/hsbc-exposed-sensitive-bankruptcy-data.html.

NCSC (2016). *Whitepaper: Common cyber attacks: reducing the impact*. Tech. rep. National Cyber Security Centre (NCSC). URL: https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/common_cyber_attacks_ncsc.pdf.

Padmavathi, Dr G, Mrs Shanmugapriya, et al. (2009). "A survey of attacks, security mechanisms and challenges in wireless sensor networks". In: *arXiv preprint arXiv:0909.0576*.

Pawar, Mohan V and J Anuradha (2015). "Network security and types of attacks in network". In: *Procedia Computer Science* 48, pp. 503–506.

Peter, Petlee (2017). *Many Bengalureans lose cash to sim card swap fraud*. URL: https://timesofindia.indiatimes.com/city/bengaluru/many-bengalureans-lose-cash-to-sim-card-swap-fraud/articleshow/58387867.cms.

Plate, Erich J (2002). "Flood risk and flood management". In: *Journal of Hydrology* 267.1-2, pp. 2–11.

Robinson, Michael, Kevin Jones, and Helge Janicke (2015). "Cyber warfare: Issues and challenges". In: *Computers & security* 49, pp. 70–94.

Schwartz, Mathew (2018). *French Cinema Chain Fires Dutch Executives Over 'CEO Fraud'*. URL: https://www.bankinfosecurity.com/blogs/french-cinema-chain-fires-dutch-executives-over-ceo-fraud-p-2681.

Sedgewick, Adam (2014). *Framework for improving critical infrastructure cybersecurity, version 1.0*. Tech. rep.

Simonsson, Mårten and Pontus Johnson (2006). "Assessment of IT governance-A prioritization of Cobit". In: *Proceedings of the Conference on Systems Engineering Research*. Studentlitteratur, pp. 1–10.

Singh, Rajni Ranjan and Deepak Singh Tomar (2015). "Network forensics: detection and analysis of stealth port scanning attack". In: *scanning* 4, p. 8.

Stoddard, Donald (2012). *Essentials First: Life in the DMZ*. URL: http://www.ciscopress.com/articles/article.asp?p=1823359&seqNum=5.

Stoneburner, Gary, Alice Y Goguen, and Alexis Feringa (2002). "Sp 800-30. risk management guide for information technology systems". In:

Taleb, Nassim Nicholas (2007). *The black swan: The impact of the highly improbable*. Vol. 2. Random house.

The Hi-Tech Crime Trends (2018). Tech. rep. Group IB. URL: https://www.group-ib.com/resources/threat-research/2018-report.html.

Vijayan, Jai (2018). *Attackers Employ Social Engineering to Distribute New Banking Trojan*. URL: https://www.darkreading.com/attacks-breaches/attackers-employ-social-engineering-to-distribute-new-banking-trojan/d/d-id/1332731.

Vincent, Charles, Sally Taylor-Adams, and Nicola Stanhope (1998). "Framework for analysing risk and safety in clinical medicine". In: *BMJ: British Medical Journal* 316.7138, p. 1154.

White, Sarah (2019). *What is COBIT? A framework for alignment and governance*. URL: https://www.cio.com/article/3243684/what-is-cobit-a-framework-for-alignment-and-governance.html.

Wieringa, Roel J (2014). *Design science methodology for information systems and software engineering*. Springer.

Wohlin, Claes et al. (2012). *Experimentation in software engineering*. Springer Science & Business Media.

Wolke, Thomas (2017). *Risk Management*. Walter de Gruyter GmbH & Co KG.

Zorz, Zeljka (2012). *$2.1 million stolen with clever social engineering*. URL: https://www.helpnetsecurity.com/2012/03/01/21-million-stolen-with-clever-social-engineering/.