Department of Information Security and Communication Technology

IMT4129 - Risk Management for Information Security

Course Report

Author (student number):
Ole André Hauge (538916)

April, 2022

Abstract

The purpose of this report is to demonstrate knowledge, skills, and general competence in the areas of risk management for information security, specifically risk analysis case studies, uncertainties, management tools, balanced scorecard, ignitable assets, lead and lag indicators, vulnerability discovery, controls, compliance-based security, and game theory applied to information security.

The first chapter provides a brief overview of the organization used for the discussion in the report. Chapter 2 presents two case studies of the scenario described in Chapter 1. It demonstrates how two standards, ISO 27005 and CIRA, may be applied to the same scenario to create two entirely different interpretations of the same event. The third chapter examines the prior chapter's numerical values in terms of uncertainty. Relevant quantitative examples are included in our reflections where applicable. Where applicable, relevant quantitative examples are presented in our remarks. Chapter 4 expands on the scenario utilized in this report to give a more realistic source of input data for the report's following chapters. The fifth chapter covers three balanced scorecard metrics and discusses how each measure is related to one or more of the intangible assets discussed in the course literature. Chapter 6 quantifies the lead and lag indicators for different measures in the strategy map, taking care to account for uncertainties as needed. The seventh chapter describes how vulnerability and threat detection methodologies may be employed in a practical situation. We define and evaluate the metrics supplied in the strategy map, considering both lead and lag indications. As vulnerability discovery methodologies, the checklist, VAM, data flow modeling, and top-down approach of controls are used. Chapter 8 identifies and addresses the control categories that are relevant to the vulnerabilities highlighted in Chapter 7. The control categories are found by consulting the ISO 27001 Annex A and COBIT. The ninth chapter looks at risk from a decision-theoretic standpoint by applying decision theory to information security risk assessments. We use Event Tree Analysis (ETA) in conjunction with fuzzy decision theory to achieve this evaluation. The last chapter applies game theory to previously discussed scenarios in this paper.

The report uses the ACM reference format.

Table of Contents

List of Figures

List of Tables

CH1 – Decide on Groups and Select a Target Organization

This group has one group member, namely Ole André Hauge, and focuses on a fictional organization based on actual organizations. The group is using a fictional organization, NTNU Analytica, as its target organization as a layer of abstraction to better preserve potential confidential and privileged information. The objective of this document is to provide a brief overview of the organization which is further intended to be used as the basis for the risk analysis.

CH1.1 – Selection of a Target Organization

The organization that this paper will focus on is NTNU Analytica, a medium-sized Norwegian firm. Organizations are facing several challenges concerning consuming, analyzing, and applying big data to make informed decisions at all levels of the company i.e having good situational awareness (SA). Data availability is increasing, which means more information is available to help a business improve. However, gathering, analyzing, and applying this data frequently necessitates specialized skills, which many businesses lack. Companies are struggling to staff and grow their internal IT and information security teams at the same speed as the digital innovation. As a result, it's typically more cost-effective to outsource part, if not all, of these processes to companies that specialize in these areas, such as consulting firms or, in this example, data gathering and analysis services.

CH1.2 – Target Organization Description

NTNU Analytica is an organization contracted by several Norwegian media houses and political campaigns to collect data from open sources on the Internet and create tailored SA of their targeted demographics with qualified suggestions for further marketing or persuasion campaigns. The organization has to be viewed as that which uses Open Source Intelligence (OSINT) and Social Media Intelligence (SOCMINT) with integrity in keeping with government regulation and other international rules like GDPR applying to data collection, storage, and application.

NTNU Analytica deploys a Data Collection and Storage System (DCSS) for all collected open-source data and a Data Analysis and Situational Awareness System (DASAS) for the analysis and management of the information. The DCSS platform is used by the Data Science (DS) department where all data is collected and processed before it is distributed to DASAS. DASAS then illustrates information in terms of a SA image for the target audience and is used by the Behavioral Dynamics (BD) department to conduct target audience analysis (TAA), behavioral modeling, and target audience profile development (TAP). The Marketing department then uses the results from the BD department presented in DASAS to further create campaign intervention strategies (CIS) using TAP and TAA to tailor strategies for influence, which is presented to the customers with the SA picture of the TA. Moreover, DASAS and DCSS are used to evaluate the effects of the CIS through audience-based measures of effectiveness (AB-MOE) analysis based on baselines models created at the start of the project. The AB-MOE results are used to measure the ROI of the intervention project. In addition, NTNU Analytica has contracted four social media companies (Facebook, Instagram, Snapchat, Twitter) to provide other services for identifying new trends and behavior, and maintaining and monitoring demographic behavior in real-time. The organization has also contracted a third-party company, NTNU Cloud Safe, to provide additional cloud services as a backup to their data center, as well as various off-site social media click farms that are used to boost the engagement of content.

The firm employs 300 staff, 50 of whom work in the departments of information technology (IT) and information security (IS). Information Security Management (ISM) is the responsibility of 10% of the IT and IS staff, while the rest of the staff with different degrees of unverified security clearances are responsible for other IT support functions inside the organization. More than 30% of NTNU Analytica's employees work on a contract basis and are paid low salaries, which has long been a cause of dissatisfaction among many employees who believe it is unfair.

Figure 1 below shows the company's management organizational structure. For incident man-

agement and control, all activities coordination at NTNU Analytica is reliant on support staff at their different workstations exchanging messages via email, phone calls, or SMS alerts via the public network infrastructure. When communicating over the public network, secure services such as Signal and Lavabit are utilized to preserve the confidentiality and integrity of the company's communications.

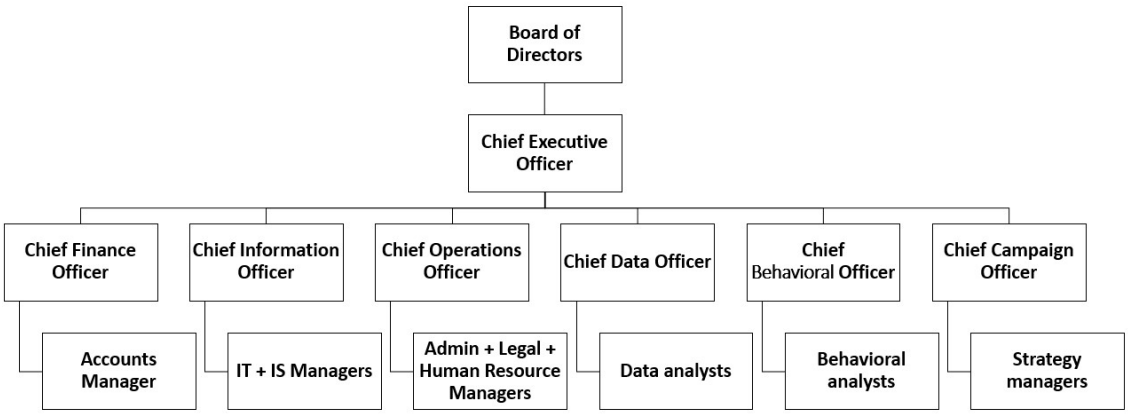

Figure 1: NTNU Analytica Organization Structure.

For the past five years, the business has had a single general-purpose information security management policy, but only department managers and a few chosen staff members have been effectively trained on it. The importance of policy implementation across the organization has never been a priority. This is owing in part to its quick development and emphasis on delivery of the product. However, the agency has seen three significant security breaches, as well as several lesser efforts, since December 2019, resulting in unreported financial losses. In this context, the responsible IT and IS staff at NTNU Analytica has been charged with developing a clear and comprehensive information security risk management strategy and report that is to be used to better manage the risk associated with the confidentiality, integrity, and availability of information assets, as well as the stakeholders in the organization.

CH2 – Risk Analysis Case Studies

In this chapter, we construct two case studies of the scenario that was submitted as a standalone document and that was not to be included in this report document. The first section, CH2.1, illustrates an implementation of the ISO 27005, while the second section, CH2.2, shows how the CIRA standard can be used for the same scenario. The two subsections display how different standards can be used to produce completely different understandings of the same scenario based on a different point of view. This can be highly valuable to get a good situational awareness.

CH2.1 – ISO 27005

The ISO 27005 standard [13] proposes that several stages are to be followed to get a proper result. For the sake of this section, we have decided to divide it into a section per stage to make it easier to follow. The risk analysis that follows will focus on the aforementioned core business sectors of NTNU Analytica, as well as CIS reports and behavioral change. Prior documents including crucial facts about the organization, such as stakeholders, revenue, business goal, objective, structure, and the like, are manufactured and based on comparable firms since this is a fictive corporation. Additional information can be obtained from other publically accessible sources.

CH2.1.1 – Context Establishment

Risk Evaluation Criteria: The risk function, which maps the possibility and consequence to a risk level, defines the risk evaluation criteria for NTNU Analytica. A quantitative risk matrix was chosen as the risk function to facilitate a quantitative risk analysis technique. As shown in Table 1 and 2, the risk likelihood and consequence are graded from 0 to 4. Table 2 additionally shows the Impact criterion with the impact cost in NOK.

Table 1: Likelihood Scale

Rank	Likelihood	Definition
0	Unlikely	$[0, 1 >$: 1 year
1	Rare	$[1, 5 >$: 1 year
2	Possible	$[5, 20 >$: 1 year
3	Likely	$[20, 50 >$: 1 year
4	Certain	$[50, \infty >$: 1 year

Table 2: List of Impact

Rank	C	I	A	Economy	Reputation
0	Insignificant harm to the organization and shareholders	Insignificant loss of integrity	Insignificant loss of availability	[0-10,000>	Insignificant reduction.
1	Minor harm to the organization and shareholders	Minor loss of integrity	Minor loss of availability	[10,000-50,000>	Minor reduction. Little media coverage
2	Moderate harm to the organization and shareholders	Moderate loss of integrity	Moderate loss of availability	[50,000-250,000>	Moderate reduction. Some media coverage
3	Major harm to the organization and shareholders	Major loss of integrity	Major loss of availability	[250,000-750,000	Major reduction. Global media coverage

Table 2: List of Impact

Rank	C	I	A	Economy	Reputation
4	Catastrophic harm to the organization and shareholders	Catastrophic loss of integrity	Catastrophic loss of availability	[750,000-1,500,000>	Catastrophic reduction. Global media coverage and court sanctions

Risk Acceptance Criteria: NTNU Analytica is ready to risk losses of up to 250,000 NOK as long as they occur seldom. They are ready to take risks up to 750,000 NOK as long as the potential reward from the risk investment outweighs the damage by a factor of three and it is not more than likely that it will occur. This may be to risk 200,000 NOK fines for GDPR violations by accessing or analyzing data in a way that gives more accurate CIS findings, in exchange for a 200,000 NOK ROI boost to 600,000 NOK. This corresponds to the likelihood and consequence pairings (0,0), (0,1), (0,2), (1,0), (1,1), and (1,2), with the exceptional instances being (2, 0), (2,1), (2,2), and (2,3). (2,3).

Scope and Boundaries: The risk analysis will concentrate on NTNU Analytica's internal information assets that are related to the organization's vision and goal, i.e. the creation of the CIS. This covers the contractual social media firms as well as the third-party cloud storage provider. This implies that the information assets of the CFO's and COO's departments will not be included in the study since they are not directly related to the creation of the organization's goods while being a vital element of the organization's workings and success.

Roles and Responsibilities of the Organization: The organization previously delegated ISRM duty to 10% of the IT and IS professionals, but without a clear structure. To avoid a conflict of interest between the recommendations of the CIO and the CISO, the business will establish a new department under a CISO post that reports directly to the CEO on ISRM. The CISO reports directly to the CEO and is responsible for developing an information security plan that improves the business without negatively influencing it and, if feasible, boosts the total ROI. As a result, the ISRM department must work closely with the other departments. For the same reason, information security managers must incorporate external and third-party partners in their strategy. As a result, the new organization will have three levels: the CISO, the information security managers, and the information security specialists. The CISO and managers will work with the organization's high-level risk management operations, while the experts will work with other related projects or activities.

CH2.1.2 – Risk Identification

List of Assets: NTNU Analytica's assets are identified based on the aforementioned documents and open sources and listed here. Table 3 provides a summary of the assets, type, value (Val.), and replacement cost (Rep. Cost). The value is derived as a weighted score based on their relationship to disclosure (Disc.), modification (Mod.), and nonavailability (NAV). The tables in this section are only what we see as most important as we are short on space.

List of Threats: We identify and depict the threats that NTNU Analytica faces in their threat environment, as seen in Table 4. The table illustrates the threat type, threat description, and threat origin. The nature of each threat is defined by the origin column, where A stands for Accidental, D stands for Deliberate, and E stands for Environmental. The danger classifications are not listed in any particular order of importance. We also consider the human threat sources described in Table 5, which illustrates the source of the threat, its motivation, and its effects.

Table 3: List of Assets

Nr.	Name	Type	Disc. (50)	Mod. (20)	NAV. (30)	Val.	Rep. Cost
1	DCSS srv 1 & 2	Primary	0.6	1	1	80	150,000 NOK
3	DCSS storage srv 1-50	Primary	0.7	1	1	85	100,000 NOK/pr
4	DCSS ws 1-75	Primary	0.6	1	0.9	77	20,000 NOK/pr
5	DASAS srv 1 & 2	Primary	0.8	0.7	0.9	81	150,000 NOK
7	DASAS ws 1-75	Primary	0.7	0.7	0.9	76	20,000 NOK/pr
8	NTNU Cloud Safe	Supporting	0.9	1	0.5	80	4,000 NOK/mth
9	DCSS LAN	Supporting	0.6	1	1	80	300,000 NOK
10	DASAS LAN	Supporting	0.8	1	1	90	300,000 NOK
11	General LAN	Supporting	0.9	1	1	95	500,000 NOK
12	DCSS app	Supporting	0.7	1	0.8	79	800,000 NOK
13	DASAS app	Supporting	1	0.9	0.9	95	800,000 NOK

Table 4: List of Threats

Type	Threats	Origin
Physical damage	Destruction of media	A, D, E
Loss of essential services	Loss of power supply	A, D, E
Compromise of information	Disclosure	A, D
Technical failures	Software malfunction	A
Unauthorised actions	Corruption of data	D
Compromise of functions	Abuse of rights	A, D

Table 5: List of Human Threat Sources

Origin	Motivation	Consequences
Hacker, cracker	Challenge, ego	Unauthorized system access
Computer criminal	Illegal information disclosure	Information bribery
Insiders	Revenge	System sabotage

List of Controls: Existing controls are outlined to strengthen NTNU Analytica's information security. These are controls that mitigate the aforementioned threats. Table 6 depicts the controls, description, and the target of the control, where the target refers to the relevant threat it can mitigate.

Table 6: List of Controls

Controls	Description	Target
Protection of data	NTNU Analytica have implemented procedures and policies responsible for protecting the collected data on their local servers	Destruction of media, disclosure, corruption of data, abuse of rights
Protection of software	A collection of policies are implemented to ensure that staff cannot access, corrupt or delete software.	Disclosure, corruption of data, abuse of rights
Physical protection	To assure the systems' availability, safety mechanisms have been added. This comprises UPS, fire suppression, redundant air conditioning, and vital environmental parameter monitoring.	Destruction of media, loss of power, corruption of data

List of Vulnerabilities: We discover vulnerabilities in the organization. The vulnerabilities are

included in Table 7, which contains the vulnerability description as well as the accompanying threat.

Table 7: List of Vulnerabilities

Types	Examples of vulnerabilities	Examples of threats
Hardware	Lack of efficient configuration change control	Error in use
Software	Widely-distributed software	Corruption of data
Network	Unprotected communication lines	Eavesdropping
Personnel	Insufficient security training	Error in use
Organization	Lack of continuity plans	Equipment failure
Site	Inadequate or careless use of physical access control to building and rooms	Destruction of equipment or media

CH2.1.3 – Risk Analysis

This section evaluates the relative risk to the information assets of NTNU Analytica. The risks associated with the assets are examined and used to evaluate the effectiveness of the proposed controls and to illustrate the residual risk. We can identify event scenarios and their related consequences by combining assets, threats, and vulnerabilities.

Risk nr. 1 – Information Leakage
Threat: Eavesdropping
Vulnerability: Unprotected communication lines
Asset: DCSS servers, DASAS servers, LAN

Incident: A computer criminal does not like the mission of the organization and decides to gather and share confidential information with the public to negatively impact the organization's reputation.

Impact: C: 4 I: 1 A: 0 E: 4 R: 4 **Total:** 3,25

Likelihood: 2 **Risk:** 6,5

Risk nr. 2: – Corruption of Data
Threat: Corruption of data
Vulnerability: Widely-distributed software
Asset: DCSS application, DASAS application

Incident: An employee manages to corrupt the configuration files of the analysis software leading to the software being inoperable.

Impact: C: 1 I: 4 A: 4 E: 3 R: 1 **Total:** 2,8

Likelihood: 3 **Risk:** 8,4

CH2.1.4 – Risk Treatment

To build treatment strategies, we determine the controls that may be applied to the risks. Table 8 displays a list of some of the controls that may be used associated with the cost. The risks are ranked based on both severities of the risk as well as the efficiency of the proposed treatment. The cost mentioned in the table does not include the number of man-hours required to complete the task. A risk can have multiple proposed treatments with different strategies and costs.

Table 8: List of Treatments

Priority	Risk	Description	Cost (NOK)	Strategy
1	2	Protection of data by investing in backup systems and redundancy.	800,000	Mitigate
2	1	Continuous patching of software and hardware as switches and firewalls.	100,000	Avoid
3	2	Improved access controls (RBAC) and personnel training.	100,000	Mitigate
4	1	Implementing evaluation processes for network and system security i.e. red-teaming	150,000	Mitigate

We propose three treatment options based on the controls in Table 8. These range from low cost with little human work to high cost with a lot of effort. Plan one (1) implements controls 2 and 3, plan two (2) implements 3 and 4, while plan three (3) implements 1-4 for full protection.

CH2.1.5 – Risk Acceptance

As previously stated, NTNU Analytica will assume the risk of losses up to 250,000 NOK on a rare basis, and 750,000 NOK if the potential ROI benefit exceeds the factor of 3. Risk 1 is inside of this scope with E = 3, however as risk 1 adds no benefit to the ROI it should be mitigated. Risk 2 is outside of the scope, with E = 4. However, based on the treatment plans and residual hazards, we may conclude that treatment plan one will not reduce the risk to an acceptable level, but treatment plans two and three would.

CH2.1.6 – Risk Communication and Consultation

The ISRM department will communicate information about risks with the important decision-makers and stakeholders in the organization by producing reports that will be shared internally in the organization. The CISO will receive a weekly report informing about the existence, nature, form, likelihood, severity, and acceptability of risks, as well as new and ongoing treatments. This way he will develop a general SA. His department managers will inform him/her about incidents that occur so that he/she can make the necessary decisions and communicate the situation to the other affected stakeholders. The CISO will also report to the management and CEO about the current and future risks during meetings that are set at agreed-upon intervals. Short weekly reports will be sent to the organization's staff with the intent of maintaining their information security awareness.

CH2.1.7 – Risk Monitoring and Review

As risks are not static the organization will implement measures to monitor risk which will be used to support the aforementioned reporting structure. The ISRM department will monitor access logs and the general public impression of the company to detect any changes. Regular inspections of hardware will be scheduled with the IT department and automatic updates will be implemented and maintained. Other measurements will be implemented for risks as they appear and are evaluated to be lasting or reoccurring and not incidents that happen once. This will be done by using a risk identification checklist developed by the ISRM department in cooperation with the IT department.

CH2.2 – CIRA

The CIRA standard proposes that several stages are to be followed to get proper results. We find support in [19] to properly implement the standard. For the sake of this section, we have decided to divide it into a section per stage to make it easier to follow.

CH2.2.1 – Data Collection (Structural)

Risk Owner: The political party Right Wing (RW) is designated as the risk owner in our scenario. We presume that other NTNU Analytica clients are of a similar sort. Right Wing's persona is given in Table 10.

Risk Owner's Key Utility Factors: During our first meeting with the Right Wing, we agreed that the utility elements shown in Table 9 would give them a perceived advantage. On a scale of 0 to 100, the weight score represents the relevance of each utility element. The primary focus of this analysis is on Right Wing's top utility factor: privacy.

Table 9: Right Wing's Utility Factors

Rank	Utility Factor	Weight
1	Privacy	90
2	Product usability	80
3	Campaign intervention strategies	75

Strategies/Operations Influence Key Utility Factors: We look at the taxonomy of actions that produce privacy issues based on NTNU Analyticas' past studies in the field to determine the tactics. The following techniques are being considered:

- Internal breach of confidentiality – Knowingly or unknowingly disclosure of information across clearance levels at NTNU Analytica.
- External breach of confidentiality – External entity manages to identify the cooperation between Right Wing and NTNU Analytica. Or a hacker gains access to the system.

Roles/Functions Related to the Given Strategies/Operations: There can be many strategy owners capable of executing these strategies. However, for this paper, we consider only three stakeholders as the objective is to show the use of the CIRA method. The stakeholders are the CEO and a hacker, capable of compromising confidentiality.

Strategy Owners: We take into account the following stakeholders: Aleksander (CEO) and Bob (Hacker). Table 10 contains their personas.

Table 10: Personas of Risk and Strategy Owners

Role	Name	Description
Political Party	Right Wing	A young political party focuses on green politics, relies on the support from NTNU Analytica; knows that the exposure of the cooperation can yield negative press towards the party.
CEO	Alex	50 years old, ensures the overall development and relationship with its stakeholders. Has motivation to increase the company's information security capacity.
Hacker	Bob	28 years old, skilled in computing and interested in new challenges; wants to earn money and also build status for himself.

Strategy Owner's Key Utility Factors: The strategy owner's key utility factors are given in Table 11, including associated weights.

Table 11: Strategy Owner's Utility Factors

Rank	Utility Factor	Weight
CEO (Alex)	Privacy Reputation	100 90
Hacker (Bob)	Wealth Prestige	100 95

CH2.2.2 – Data Collection (Numerical)

Operationalization of Utility: We specify the scale, measuring process, value semantics, and explain any underlying assumptions for each determined utility factor. The brief explanations of the measures are depicted in Tables 12, 13, and 14.

Table 12: Right Wing's Utility Factor Metrics

Utility Factor	Definition	Metric
Privacy	Privacy refers to the concealment of the party's identity and involvement with NTNU Analytica. The metric will be Boolean as one is either private or not.	0 or 1

Table 13: The CEO's Utility Factor Metrics

Utility Factor	Definition	Metric
Privacy	Privacy refers to the concealment of the organizations identity and involvement with NTNU Analytica. The metric will be Boolean as one is either private or not.	0 or 1
Reputation	Reputation refers to how the organization is perceived internally and externally. The reputation is continuously affected by incidents.	Reputation= $\frac{1}{1+N}$, where N is the number of incidents.

Table 14: The Hacker's Utility Factor Metrics

Utility Factor	Definition	Metric
Wealth	Wealth refers to the hackers economical assets. This is calculated as an increase/decrease percentage towards the hackers financial goals.	Wealth = $\frac{\text{current}+/-\text{change}}{\text{goal}}$
Prestige	The prestige refers to the recognition of the hacker's work. The prestige is calculated as an interval between 0 and 100.	0 – 100, where 100 is equal to global media coverage.

Weight of the Utility Factors: Each of the stakeholders' utility factors is assigned a weighted score, as shown in Tables 9 and 11s. The scale runs from 0 to 100, with 0 indicating no utility and 100 indicating high utility.

Impact of the Utility Factors: We identify four strategy scenarios based on the previously mentioned strategies:

1. Internal breach due to malice of intent. Information shared with the press. Assumed 750,000 NOK total loss.
2. Internal breach due to ignorance. Disclosure of data across clearance levels. This results in a maximum 100,000 NOK increase in the infosec budget for better access controls and personnel training.
3. External breach by a hacker. Stops availability for three days. Assumed 1,500,000 NOK total loss.
4. No action.

The impact the strategies have on the stakeholder's utilities is shown in Table 15.

Table 15: Strategy Impact

Stakeholder	Utility Factor	Weight	Initial Value	S1	S2	S3	S4
Right Wing	Privacy	1	100	97.6	99	79	100
CEO	Privacy	0.65	79.4	74	80.2	64	81.3
CEO	Reputation	0.53	63	73.4		62.9	
Hacker	Wealth	0.47	39			55	
Hacker	Prestige	0.56	20			73.2	

Estimated Utility: We assess the utility of each strategy for each player using MAUT. We simplify by assuming that the utility is linear. In our case study, we apply the equation to compute the utilities for the stakeholders based on the values in Table 15. We can calculate the estimated utility for each of the stakeholders using MAUT:

Right Wing: $1 \times 100 = 100$
CEO: $0.65 \times 79.4 + 0.53 \times 63 = 85$
Hacker: $0.47 \times 39 + 0.56 \times 20 = 29.53$

Incentives Computation: We must compute the incentives for each method for each participant. This is done by finding the delta between each of the strategies and the initial value. The results are presented Table 16.

Table 16: Incentives

Stakeholder	Initial Value	Strategy 1	Strategy 2	Strategy 3	Strategy 4
Right Wing	100	-2.4	-1	-21	0
CEO	85	2	-4.8	-10.1	-3,7
Hacker	29.53			37.3	

Determined Risk: The impact of each strategy on the risk owner, Right Wing, is given in the format (Incentive, Consequence), as shown in Table 17. The motivation of the strategy owner to implement the plan is referred to as incentive, while the impact on the Right-Wing is referred to as consequence.

Table 17: Risk

Stakholders	Strategy 1	Strategy 2	Strategy 3	Strategy 4
CEO	(2, -2.4)	(-4.8, -1)	(-10.1, -21)	(-3.7, 0)
Hacker	NA	NA	(37.3, -21)	NA

Evaluate Risk: This may be accomplished by comparing each strategy in terms of the amount and direction of the changes identified in the previous stage. We use an incentive graph to evaluate

the usefulness of the strategies once they have been implemented (ref. Figure 2). We can observe that if the Right Wing party picks strategy 4, it does not affect their privacy, but it reduces the CEO's utility as a strategy owner. This implies the CEO will suffer a financial loss as well as a possible loss of the company's reputation. As a result, this is the risk owner's best plan. If the Right Wing party chooses strategies 1 and 2, they will risk a small decrease in their privacy utility, but because the impact of these strategies is low and, in the case of strategy 1, even results in a positive increase in utilities, it is likely that they can achieve cooperation with the risk owners. The risk owner, on the other hand, does not accept the third technique (3a or 3b), because it is solely useful to the hacker (3b).

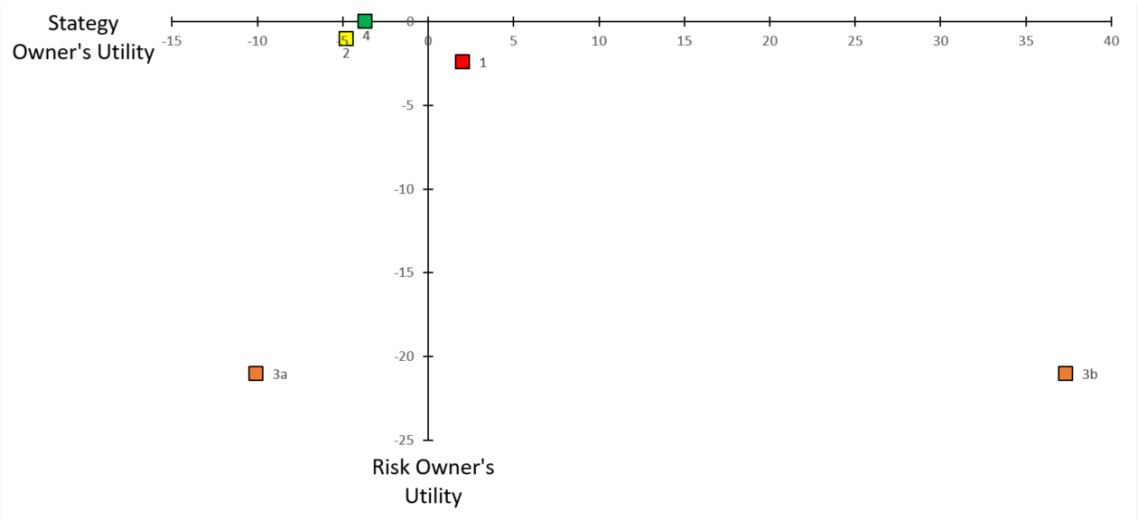

Figure 2: Incentive Graph

CH2.3 – Optional Chapter of Issues

Regarding ISO27005, we identified the following issues: data gathering is quite hard and can be complicated. This could be improved with procedures and a data collection manual for the risk analyst. It seems that the risk analyst and the participants must have the same understanding of the concepts (i.e., utility variables) used throughout the data collection process. This means that one should take the time and effort to operationalize the measurements for the utility variables and assess their worth to improve data quality.

Concerning CIRA, we discovered that it frequently presumed that all participants were truthful while interacting with the risk analyst. However, the fact that people may be reluctant to share information or submit false information during the interview/survey merits more investigation. Furthermore, we found it challenging to generate metrics for some of the utility features, which appear to be a perennial problem in information security. As a result, we found support in the work of others who collated and validated utility factor definitions [19]. Additional study is required to determine if an accomplished collection of utility factors accurately reflects the whole set for a specific stakeholder in a given scenario. Finally, we found it difficult to represent uncertainty in our estimates by utilizing interval arithmetic or constrained probabilities rather than point values.

CH3 – Reflecting on Uncertainties

This chapter considers the numerical values supplied in the preceding chapter in terms of uncertainty. Relevant quantitative examples are included in our reflections where applicable.

Uncertainty is defined as any type of knowledge limitation that influences the range and probability of possible answers to a question [7]. It is also flawed in the relevance, consistency, and reliability of the evidence used in the evaluation, which might include data, statistical evidence, modeling, qualitative evidence, and expert opinion. These things are, to some extent, always unforeseeable. And they are significant because they add to uncertainty in assessment responses and ambiguity of the assessment finding has major implications for decision-making.

The risk analysis chapter includes the likelihood-, consequence-, and impact scales, as well as utility factor metrics and the use of multi-attribute utility (MAUT) functions [15]. In terms of uncertainty, we can say that these statistics are estimates, and probability calculations are based on a combination of historical data and gut feeling, because determining the exact amount is tough. We must make educated guesses due to a lack of information and an inability to predict the future. The majority of the values used in Chapter 2 are frames of values in various possible ranges. The scales for likelihood, consequence, and impact all describe a range to a rank, as shown in Tables 1 and 2. This is done in part to make distinguishing between levels easier for assessing risk, and in part to get a closer approximation to the "real" value. If we look at Table 1, which depicts the likelihood scale, we can see that it is separated into ranks ranging from 0 to 4. The scale was chosen since it is difficult to forecast the times of occurrences or incidents, but it is much simpler to make approximations. As a result, the definitions of the rankings are presented as ranges of predicted occurrences each year.

When dealing with uncertainty, we must consider both first and second-order uncertainties. Scales, asset values, and replacement costs are examples of first-order uncertainty in numbers and simple values. We are dealing with second-order uncertainty when we start looking at the effect of controls, deciding on and assessing risk levels, and picking treatment plans, and we need to think about the relationship between the variables before making any judgments. The procedures used in the ISO 27005 chapter may be unduly simple, failing to represent real-world values and risks. We can look at the small example below to see how uncertainties can affect the calculation of the reasoning for choosing to implement one of the proposed controls. In the example, we focus on Risk 2 – and assume that it will 100% happen during 12 months with a cost between 250,000 to 750,000 NOK. With the organization's interest rate of 2 to 10% we get the incident cost [20]:

$rd = [0.02, 0.10], t = [0, 1], CI = [250000, 750000]$
$rc = ln[1 + [0.02, 0.10] = [ln(1 + 0.02), ln(1 + 0.10)] = [0.019, 0.095]$
$cost = [250000, 750000]e^{-([0,1]\times[0.019,0.095])} = [227343.23, 750000]$

Based on these values the organization can decide on whether or not to accept the risk and cost.

The chapter implementing CIRA deals with uncertainty in a more measurable way by providing utility variables with definitions and measurement procedures. The utility factors are also used in tandem with MAUT to determine how different activities influence the utility factors for each stakeholder. Although we use quantitative approaches to determine the changes, the values provided for the utility factors are still ambiguous, because stakeholders are asked to provide weights to the utility factors ranging from 0 to 100. As a result, subjective biases in the results can be tolerated. We also feel that the functions we utilize to examine the data are appropriate for the purpose and that we can successfully use them.

In terms of framing, we attempted to convey uncertainty by employing methodologies that assess likelihood concerning weights and intervals. It would be interesting to examine if allocating weights to a question to all stakeholders in the same group, i.e. all data analysts results in a more "authentic" value.

CH4 – Management - Expanding the Scenario

This chapter expands on the scenario used for this report to provide a more realistic source of input data for the remaining chapters in our report. As the organization of this report is fictive, we find inspiration from companies with similar business objectives. As This part will provide the following sections: Organization mission, organization vision, the balanced scorecard, and IT systems.

CH4.1 – Organization Mission

As the organization of this report is fictive, we find inspiration from companies with similar business objectives [9]. The mission statement of NTNU Analytica is as follows:

> "Our mission is to shape behavior for domestic and international government customers through research, data, analytics, and strategy."

CH4.2 – Organization Vision

In addition to having a clear understanding of the company's mission, it is as important to have a clear understanding of the company's vision. The vision statement of the company defines what it hopes to achieve. The following is the vision statement of NTNU Analytica:

> "Our vision is to be the leading provider of data analytics and behavior modification strategies."

CH4.3 – The Balanced Scorecard

In a real scenario, we could have chosen to conduct an internal survey to supplement the existing internal reports because NTNU Analytica has established mission and vision statements with associated objectives. For this section, we imagine that this has been done. As a result, we can see if management, board members, and employees all recognized the Objectives in the same way. We also needed to know how well the objectives, measurements, and activities were working and how well they were communicated. Based on this we get the strategy map seen in Figure 3. The graph's nodes represent the various Objectives and KPIs per perspective, while the edges highlight the causality and processes/initiatives that link the nodes. KPI $X \rightarrow$ and KPI Y are utilized to represent the edges.

To measure success toward the Objective, we modified the current Objective KPI (1) to "growing profits" and added two new KPIs to track progress: "increase revenue" and "control costs" (1 and 2). To be quantifiable, each KPI was assigned a target with a numeric value, and KPIs from the financial accounts were employed. KPI 1 strives for a 15% increase in income, whilst KPI 2 has a 5% cost deviation margin. KPI 1 $\rightarrow$ Objective KPI 1 and KPI 2 $\rightarrow$ Objective KPI 1 can be achieved, for example, by analyzing the efficacy of management measures and management cost. Because both KPIs are so inextricably connected (increasing one having a positive influence on the other), efforts may be shared between both. In general, we would assess the effectiveness and cost of management methods, develop and update business strategies, and evaluate the firm's productivity.

Two of the specified Objectives (2 and 3) for customers were buyer expectation fulfillment in terms of specification, delivery, and complaint handling. In this case, we intend to boost customer pleasure by 15%, which we will measure using invoice value and customer feedback. We also see a causal association between Objective KPI 4 $\rightarrow$ Objective KPI 2 and data collection efficacy, as data collection efficacy may impact how the user feels about the product. In addition to the $\rightarrow$ KPI 4 causality of Objective KPI 4, we cannot guarantee that KPI 4 will reflect the influence described

in Objective KPI 4. Based on these causalities, poor performance in certain places may have a higher-level ripple impact on the strategy map. Because NTNU Analytica works directly with its clients, it is possible to get constant feedback during an intervention program. The data and input will be used to improve the product, process, and user interaction. Second, we want to make certain that we provide a one-of-a-kind product to meet market demand. This will be determined by keeping an eye on NTNU Analytica's market-specific unique indexes. The uniqueness will be kept by utilizing cutting-edge data and psychological analysis approaches.

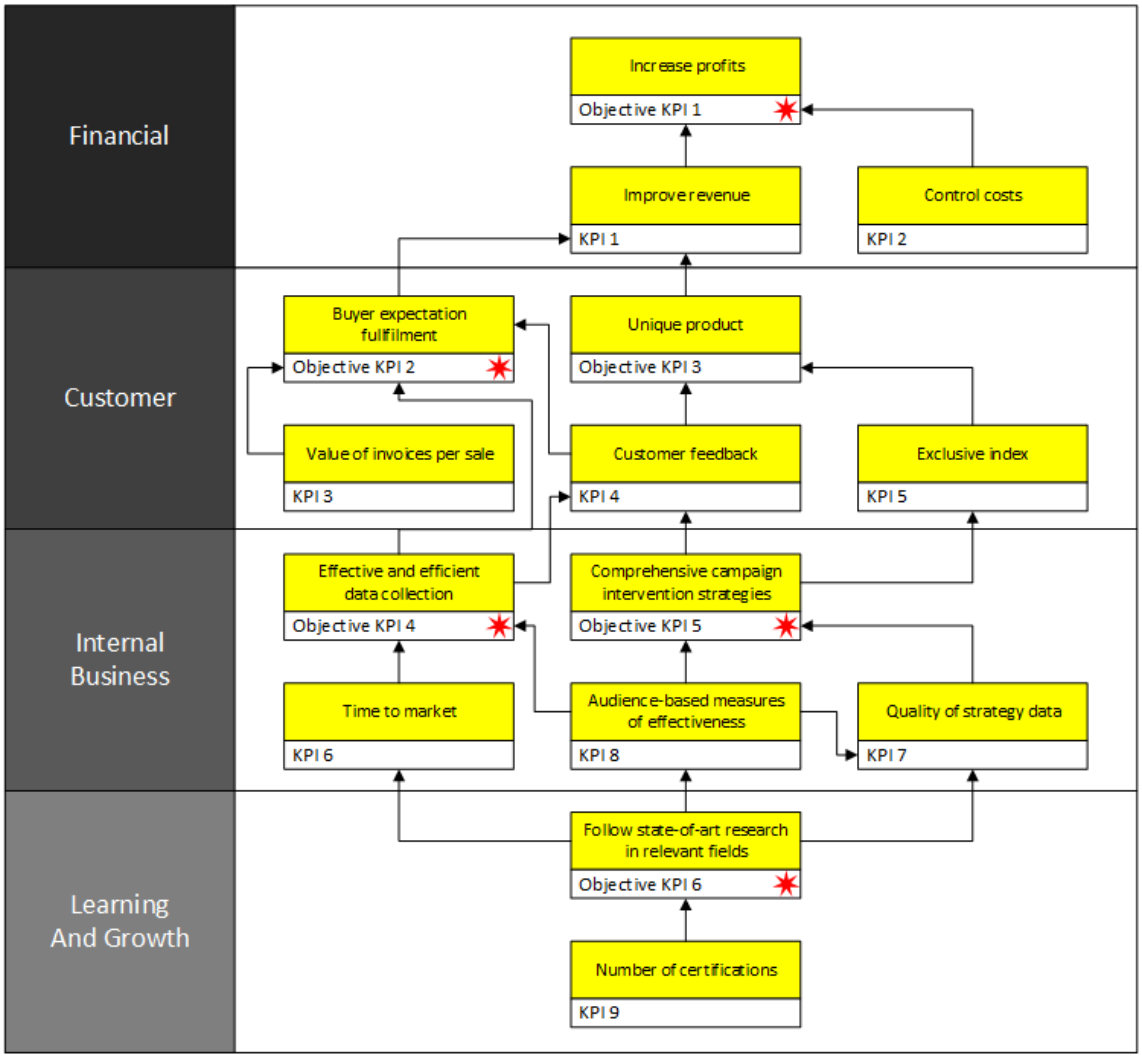

Figure 3: Strategy Map for NTNU Analytica

In terms of internal operations, we identified difficulties in two of the Objectives (4 and 5) regarding how efficient and effective data collection is and how it may be used to produce even more comprehensive CIS for customers to increase their satisfaction and revenue. We hope to spend 10% less time evaluating data and thereby minimize time to market by improving the tools and continuing to educate the team (KPI 6). The audience-based measure (KPI 8) will be used to determine if the target audience's behavior varies in a quantifiable way from the pre-recorded baseline. As illustrated in Figure 3, it contains the causalities, KPI 8 $\rightarrow$ Objective KPI 4, and KPI 8 $\rightarrow$ Objective KPI 5, as both Objectives can have use of this KPI.

There is also a causality KPI 8 $\rightarrow$ KPI 7 since the quality of the strategy data may be seen in the influence it has on the target audience as well as the quality of its presentation. What isn't evident from the strategy map is how we'll implement frequent initiatives to enhance the tools and train the employees. As a consequence, we will be able to develop cutting-edge initiatives, which we will implement by launching a learning platform for employees and customers. Customers' understanding of the product and how it may be utilized will increase as their knowledge expands.

As a consequence, their feedback will improve, and they will be more aware of the overall quality of the product they are receiving.

Finally, and perhaps most crucially, we establish learning and growth goals, which serve as the pillars of the organization's offering. The most important (6) is to stay current on cutting-edge research and emerging developments in data analytics and behavioral psychology. This will be done through staff training and education in a variety of areas, as well as increasing the use of certifications, which will be one of the KPIs used to measure existing knowledge levels. To achieve the aim, NTNU Analytica will develop a partnership with an educational firm to make it easier for the company to receive the information it needed at the pace it demands.

By following the vertices, we can see how everything is connected and can positively affect the main objective.

CH4.4 – IT Systems

The organization's IT architecture, as shown in Figure 4, consists of three LANs: a general LAN with an Internet connection, a DCSS LAN for data collection and storage systems, and a DASAS LAN for data analysis and situational awareness systems.

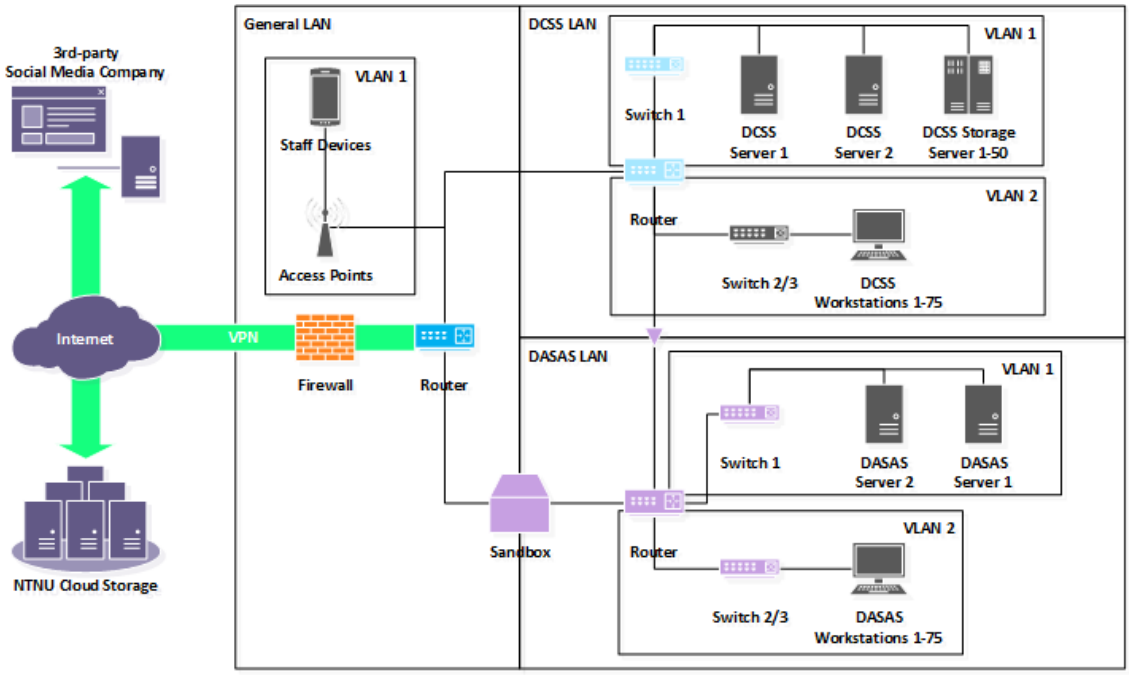

Figure 4: IT Infrastructure for NTNU Analytica

General LAN

The General LAN is used for administrative tasks by the staff with a connection to the internet for all its cloud applications, like O365. The firewall is the first-line defense, the router further interfaces with the access points, the DCSS LAN and DASAS LAN, Switches are used to meet the access demand, Access points are used by all staff devices for general admin tasks and communication via the Internet, and the VPN is used to provide confidentiality for the entire organization. A second purpose is to obscure the traffic to not make the targets aware or suspicious of the data collection of the organization.

DCSS LAN

The DCSS LAN consists of a router providing interfaces to the Internet for data backup to the NTNU Cloud Storage and data collection. An interface via a data diode ensures one-way commu-

nication is open to the DASAS router. Servers and workstations are separated in VLANs. The switches are used for scalability, while the 2 DCSS servers run the DCSS application needed for data collection operations and analysis. The 50 DCSS storage servers are used as local data storage and are frequently backed up to the external cloud storage, and the 75 DCSS workstations are used by the staff in the Data analytics department.

DASAS LAN

The DASAS LAN consists of a sandbox for any data coming from the Internet to the DASAS network; a router provides an interface for the DASAS system so that the behavioral department can forward their reports to the customers (another Internet activity like googling is not allowed for this network); switches used for scalability; 2 DASAS servers used to manage the DASAS application used for the production of the CIS, and 75 DASAS workstations used by the staff in the behavioral analytics department to work on the CIS.

ICT Applications

- The signal messaging application is used by staff to communicate securely in work-related scenarios internally as well as externally.
- The Lavabit e-mail service is used by staff to communicate securely in work-related scenarios internally as well as externally.

CH5 – BSC Measures and Intangible Assets

This chapter examines three measurements that are identified in Chapter 4, section 4.3 – The Balanced Scorecard, and explains how each measure is connected to one or more of the intangible assets mentioned in the course literature. According to the literature, an intangible asset is a non-monetary asset that is recognizable but has no physical substance, such as information (CIA), processes, perception and attitudes, and goodwill. The paper [14] details how intangible assets can be seen as intellectual property, where he further introduces a categorization of such assets.

According to Johnson W., intangible assets can be divided into three main categories: human capital, structural capital, and relational capital. Human capital encompasses the relationship between human intellect and the innovation of the firm. Structural capital regards how well the human intellect and innovation are used to increase the wealth of the firm. Relational capital concerns how the firm can positively interact with the business community to stimulate the increase of wealth. The human and structural capital categories are further divided into two subdivisions each.

Human capital is made up of both ideas and leadership capital. The sustainability and caring nature of the work environment may be used to evaluate ideas. This might be construed to suggest that employee happiness should have an impact on the company's product because it is dependent on their inventiveness and willingness. Leadership capital captures an organization's capacity to sustain critical knowledge and direction by using metrics such as talent and expertise.

Structural capital consists of innovation and process capital. Innovation takes into account what consumers think about a product to enhance it, as well as patenting new technology that adds value to the business. Process capital refers to the processes that an organization uses to grow its wealth.

The next sections are divided into these three categories in a non-specific order and loosely discuss measurements from the strategy map in Figure 3. This means that some of the discussion might touch upon areas of the other categories.

CH5.1 – Relational Capital

The first metric we will look at is the time to market for the internal process goal "Efficient and effective data collecting." In the case of NTNU Analytica, time to market refers to the amount of time it takes the firm to collect and develop a marketing strategy. Although several intangible assets may be stated here, we will focus on perception and attitude property for the sake of argument. This feature indicates that if a consumer has a favorable opinion about NTNU Analytica's product, they are likely to continue using the service, and NTNU Analytica will benefit.

In terms of time to market, we can see that if NTNU Analytica is quick, given quality is maintained, to deliver a product to a client, it will favorably affect their attitude and perception of the organization. This is especially important for NTNU Analytica, whose offering is a campaign intervention plan built using near-real-time data. That is, the strategy's relevance diminishes over time when new trends or viewpoints develop at any moment.

CH5.2 – Human Capital

The second metric we assess is the quality of strategy data, which is the second measure of the internal process aim "Efficient and effective data collecting." The accuracy (or quality) of the data is judged by how successfully the intervention plan helps the ongoing election campaign. The goodwill property is discussed in this measure. Goodwill is defined as the difference in value between the book value and the stock value [6]. We frequently hypothesize, with evidence backing us up, that the difference in value is attributable to the worth of the company's intangible assets, such as intellectual capital. Whereas intellectual capital is defined as a collection of intangible assets that include or make use of human knowledge and invention to generate wealth.

In terms of the quality of strategy data, we can observe that the capacity to develop a competent intervention plan is part of the company's intellectual capital. This implies that the better the organization is at offering high-quality, precise plans, the more credibility it gains for its intellectual ability, and the more profit it may anticipate making in the future. As a result of this, it is reasonable to believe that additional potential consumers will be more willing to begin using their services as the company's goodwill reputation grows.

Furthermore, the quality of strategy data is linked to an intangible asset: information. In this context, we consider the information in terms of secrecy, integrity, and availability (CIA). This is significant because the information that NTNU Analytica has access to and can use is an asset that can be leveraged to produce future value in terms of campaign intervention methods. Confidentiality of information is also an asset, because having knowledge that others do not know may place the firm in a better bargaining position than it would otherwise have. Someone else who is unaware of what the corporation is aware of is a possible source of cash for them.

Finally, integrity, or rather, having information that lacks integrity, i.e. is erroneous, would constitute a cost since the corporation would risk not incorporating data or information, which may result in you making poor judgments. The fact that you have information integrity means that you can use it to build future value. The features of this information that make it helpful for future value production, such as secrecy, integrity, and availability, offer it a unique value. The fact that you know means that you can use it to create money. It is not enough to know. This is why we may argue that information is a potentially valuable asset, and why it is tied to the quality metric. Of course, these features may be applied to or related to many of the other measurements on the balancing scoreboard.

CH5.3 – Structural Capital

The third metric we look at is the number of certificates obtained for the learning and growth goal of "following state-of-the-art research in relevant domains." The amount of certifications is utilized to assign a monetary value to employees' expertise. This has two desired outcomes: (1) management now has a mechanism to assess the knowledge of its employees across divisions, and (2) the organization can use the metrics to promote their certified skill levels to consumers. The first allows management to review how the organization is functioning in terms of learning and personal growth, and it allows them to make decisions to alter internal learning investments as needed. The second consequence allows for greater marketing and will contribute to future profits as they become more appealing to potential clients.

Intangible assets include intellectual capital property, goodwill, information (CIA), and perception and attitudes. There are various additional types of intangible assets, but for argument, we will stick to these. The information gained during the certification procedure contributes to the intellectual property of the firm as well as the attitudes and perceptions of NTNU Analytica. Certifications are one method of demonstrating a company's expertise level since the industry as a whole agrees on the quality and training they give. As a result, they have the potential to boost the company's earnings in the future. Indirectly, the two aforementioned attributes have a favorable influence on NTNU Analytica's goodwill.

The information property is particularly important for measuring certifications because if the organization or employees do not have access to the learning material or data required to study for or take the certifications, they will not be able to achieve their goal. If the information they have access to is of low quality, they may not be able to obtain the needed certifications. Worse, the certificates they get are of low integrity, i.e. they are not recognized by the industry, which means they do not grow their earnings since their clients do not believe the certifications.

CH6 – Quantification of Lead & Lag Indicators

In this chapter we quantify lead and lag indicators for the various measures found in the strategy map (ref. Figure 3), taking care to capture uncertainties as required. These indicators are metrics used to forecast future outcomes and the current performance of the organization's objectives, circumstances, and so on. Both are acknowledged as vital indicators, to minimize the gap between them. The rest of the chapter is divided into sections that focus on a selection of measures from Chapter 4, section CH4.3 – The Balanced Scorecard to provide quantification of the indicators. Finally, there is a section summarizing the significance of uncertainty in indicators.

CH6.1 – Audience-Based Measures of Effectiveness

The audience-based measures of effectiveness will be based on improvement from a predetermined baseline. NTNU Analytica continuously collects data from open sources and uses big data analysis to create an overview of how the public perceives current news and trends. If the customer is in a niche market area, then a baseline will be created before the CIS strategies are applied. However, this means that there will be a delay from the project start to the first strategy applied as the baseline needs to have good accuracy for the purpose. The baseline uses data points to form information related to the big five personality traits: openness to experience, conscientiousness, extraversion, agreeableness, and neuroticism. This measure will heavily depend on the quality of the campaign intervention strategies deployed and the target audience. Therefore, this measure uses two measures: one for the overall performance of the strategies, and the second for measuring the performance of every single strategy as they are applied. Below we present two lead and two lag indicators for this purpose.

Lead Indicator – Overall Strategy Performance

Using historic data from previous years we can be able to calculate the general effectiveness of previous overall scores and compare that to the current score. This could for example be that in 2020 the overall effectiveness score was 78%, in 2021 82%, while this far in 2022 it is 79%. This could indicate that the strategies of 2022 are less effective than previously and warrants further research into why (there are many affecting factors here). This uncertainty would need investigation. By looking at lag indicators as well we could identify if it is a general trend for the company or projects, or if it is only located in a specific project. If it is located to one specific project, then looking at the current factors like the TA, behavioral modifiers, and metrics could help evaluate why the difference is there.

Lead Indicator – Singe Strategy Performance

The service provided by NTNU Analytica is an iterative and continuous process. The customers often get daily reports during their campaign period, which means that the leading indicators can be extracted close to every day. An example would be:

> CIS strategy 3 applied to subgroup 2 of TA.
> Yesterday's big five values:
> O: 2.3, C: 3.3, E: 1.2, A: 4.2, N: 0.3
> Today's big five values:
> O: 2.5, C: 3.1, E: 1.5, A: 4.5, N: 0.2
> Conclusion: Tomorrow's strategy is likely to continue improving in the targeted areas.

Lag Indicator – Overall Strategy Performance

Calculated at the end of the year for each of the projects the company has completed. Example: As of 2021, the average score across projects for performance effectiveness was 79%.

Lag Indicator – Singe Strategy Performance

Calculates the actual effectiveness of the applied strategies. Similar to that of the lead indicator,

but using the actual results. Used to improve the strategies for new projects.

CH6.2 – Increase Profits

The increasing profits indication is based on the company's net income, also resulting in higher shareholder values, and increased market capitalization, all of which can be seen in financial statements and market projections. The net income is calculated as:

$$netincome = income - cost - expenses - taxes$$

There is going to be some uncertainty related to why there is an increase or decrease in the net income of the organization. To answer this we would have to look at the strategy map with all the indicators as a whole to identify changes and variances. It could also be needed to look at the different departments to see if there have been internal changes to the structure or methods that have affected the product quality.

Lead Indicator – Net Income

NTNU Analytica's projected net income is 300 million NOK. To quantify uncertainty in the intervals, we compare the forecast to past historical data. An example of what we may see is a 12 percent greater variance from the expected net income. This results in a prediction interval of [300M NOK, 336M NOK].

Lag Indicator – Net Income

Using example data, the previous net income of NTNU Analytica from its creation have been:

2021: 290M NOK
2020: 220M NOK
2019: 170M NOK
2018: 150M NOK
2017: 120M NOK
2016: 100M NOK

CH6.3 – Exclusive Index

The exclusive index indicator is used to compare the CIS product with other products that are available as it is important to NTNU Analytica to be the leader in the space. The indicator is based on scores from internally produced market analysis on other competitors as well as publicly available data. This measure is dependent on trends in the market and the quality of the CIS product. We aim to use both lead and lag indicators to measure the exclusiveness of the product by using the aforementioned data.

Lead Indicator – Exclusiveness

The lead indicator will be calculated based on the current list of competitive companies and the stock performance of competitive companies. Furthermore, the number of calls, emails, and meetings, with potential and current customers provide indicators of any development in interest in the organization. State-of-art development is also an indicator that can provide an understanding of how interesting the service is and how the competitors are doing which can indicate possible recessions in the market area and/or opportunities.

Lag Indicator – Exclusiveness

The lag indicator is evaluated using the index of year-to-year listed companies in the same operation area with the same vision and mission and financial performance indicators (as mentioned above) can indicate the real interest in the provided service and how saturated the market is. If the index shows a decline in competitive companies it can indicate that the interest in the general product is also declining or NTNU Analytica is outperforming the others, i.e. consuming all the

customers. The uncertainty caused by the decline in competitive companies could be investigated by comparing it with the stock development of the company. If for example the profits or stock of the company is declining, it could indicate that the product has lost some of its relevance and desirability. Furthermore, we could look at the stock and volume of the other companies for indicators of the same in the competitive companies.

CH6.4 – Importance of Uncertainty

As we simplify complicated systems, uncertainty may be identified and incorporated into all indicators and mathematical computations. The discrepancy between the lead and lag indicators indicates the presence of uncertainty. This distinction can assist us in identifying variables that we have not been able to appropriately execute. This might be due to a lack of comprehension of what we are measuring, resulting in a distorted view of the situation. Such a result might potentially be the consequence of our team lacking the necessary competence. Furthermore, if we do not have adequate historical data or if the data gathering is done incorrectly, we may encounter problems with faulty analysis.

As we are working with a fictive company it is hard to provide actual data for examples of how differences in lead and lag indicators would appear. However, we would like to demonstrate three cases.

The first implies that there is a discrepancy between NTNU Analytica's sales and revenue metrics. Assume there is a forecasted outcome for sales and revenue in 2021, and that both metrics are high. This might be because the organization just employed more analysts, updated its approach, and secured a new high-value customer. Thus, the sales revenue was estimated to be 650 million NOK, with a profit of 370 million NOK. However, the true value was 430 million NOK, with a profit of 290 million NOK. This represents a difference of 220 million NOK in sales and 80 million NOK in income.

The second examines a fictive sales value scenario in which the organization's share value increased above the average. This was due in part to the previously mentioned improvements as well as additional clients. However, the firm was subjected to negative press and the loss of a significant client during the year, resulting in a decline in customer satisfaction and lower revenues than expected. As a result, the share price fell, falling considerably below the 2021 average.

The third assumes that sales in 2021 were quite strong, but profits were somewhat low in comparison to prior years. This might be due to the organization incorrectly forecasting the values of the indicators, resulting in a decrease in the company's performance.

CH7 – Vulnerability Discovery

This chapter explains how vulnerability and threat detection approaches may be used in a relatively realistic setting. We define and analyze the measurements provided in the strategy map, taking into account both lead and lag indicators. The checklist, VAM, Data Flow Modelling, and a top-down approach to controls are employed as vulnerability discovery methodologies.

CH7.1 – Checklist

For the first part of this chapter, we employ the checklist methodology to identify threats and vulnerabilities. As there are several different lists to choose from, we combine the ISO 27005 Annex C and D publications [13] with the OWASP top ten list of vulnerabilities [18], as well as the results from the CIRA implementation in Chapter 2, section CH2.2 – CIRA. To focus on the number of threats and vulnerabilities we assume that we can conduct an internal discussion with the IT staff, management, and employees responsible for information security to identify these flaws. As a result, we identify the vulnerabilities in Table 18 and threats in Table 19 (each category is limited to 5 elements to save space in the report).

Table 18: List of Vulnerabilities in Non-Sorted Order

Vulnerability Category	**Description**
Hardware	Insufficient maintenance/faulty installation of storage media
Hardware	Lack of periodic replacement schemes
Hardware	Susceptibility to humidity, dust, soiling
Hardware	Lack of efficient configuration change control
Hardware	Unprotected storage
Software	No or insufficient software testing
Software	Well-known flaws in the software
Software	Wrong allocation of access rights
Software	Widely-distributed software
Software	Insufficient logging and monitoring
Network	Poor joint cabling
Network	Single point of failure
Network	Lack of identification and authentication of sender and receiver
Network	Insecure network architecture
Network	Inadequate network management (resilience of routing)
Personnel	Insufficient security training
Personnel	Incorrect use of software and hardware
Personnel	Lack of security awareness
Personnel	Lack of monitoring mechanisms
Personnel	Lack of policies for the correct use of media and messaging

Table 19: List of Vulnerabilities in Non-Sorted Order

Threat Category	**Description**
Physical damage	Fire
Physical damage	Water damage
Physical damage	Major accident
Physical damage	Destruction
Physical damage	Dust, corrosion, freezing
Natural events	Climatic phenomenon
Natural events	Flood
Loss of essential services	Failure of air-conditioning or water supply system
Loss of essential services	Loss of power supply

Table 19: List of Vulnerabilities in Non-Sorted Order

Threat Category	Description
Loss of essential services	Failure of telecommunication equipment
Compromise of information	Interception of compromising interference signals
Compromise of information	Remote spying
Compromise of information	Eavesdropping
Compromise of information	Theft of media or documents
Compromise of information	Disclosure
Technical failures	Equipment failure
Technical failures	Equipment malfunction
Technical failures	Saturation of the information system
Technical failures	Software malfunction
Technical failures	Breach of information system maintainability
Unauthorized actions	Unauthorised use of equipment
Unauthorized actions	Fraudulent copying of software
Unauthorized actions	Use of counterfeit or copied software
Unauthorised actions	Corruption of data
Unauthorized actions	Illegal processing of data
Compromise of functions	Error in use
Compromise of functions	Abuse of rights
Compromise of functions	Forging of rights
Compromise of functions	Denial of actions
Compromise of functions	Breach of personnel availability
Human threat sources	Hacker, cracker
Human threat sources	Computer criminal
Human threat sources	Industrial espionage (Intelligence, other government interests)
Human threat sources	Insiders (poorly trained, disgruntle, or terminated employees)

CH7.1.1 – OWASPs Top Ten Vulnerabilities

The team determined that the four most relevant vulnerabilities to NTNU Analytica are: vulnerable and obsolete components, injection attacks, cryptography failures, and broken access control by studying the OWASP top ten list of vulnerabilities (also contained in Table 18).

If NTNU Analytica employs out-of-date software, firmware, or hardware in its solutions, they may be subject to threats and assaults from external actors. It will also have a greater impact on insiders since it lowers the bar for misusing the systems. There are online common lists, publications, and newsletters that may be used to supplement updates and raise threat and vulnerability awareness. For an up-to-date list of CVEs, see the "Known Exploited Vulnerabilities Catalog" [1] provided by the US government[1] or the DragonNews Bytes newsletter from [5]. CVE-2021-44228 is a recent example of such a vulnerability (Log4j) [4]. If NTNU Analytica utilized this logging mechanism in their external or internal websites or applications and did not patch it when it was discovered, the firm would be subject to any hacker or script kiddie who could read vulnerability reports. Thus, exposing the organization to attacks in which the adversary gains access to and/or control of its servers. Following that, the attacker's agenda would decide the extent of the company's damage. It may be anything from a ransomware attack to data extraction. This has the potential to have a significant influence on the majority of the measures mentioned in the strategy map in Figure 3.

Furthermore, while the corporation wants to provide a secure website interface to its customers, they are exposed to injection attacks. These attacks take advantage of poor validation and cleaning of database-input data [17]. As a result, an external actor may be able to execute commands on the system. SQL injections are a common example of this, in which the actor may access the database, retrieve client information, and perhaps delete data. As a result of this vulnerability,

[1]The United States has issued a directive requiring all civil federal agencies in the country to patch the vulnerabilities on this list within the timeframe specified. They also recommend that everyone follow the list and, at the very least, patch the vulnerabilities.

the organization's reputation may suffer and progress may be slowed. If clients lose faith in the firm, the company will incur massive economic losses.

Because NTNU Analytica and its clients rely on and value anonymity and confidentiality, they rely on the usage of appropriate cryptographic technology. If the mechanism used to encrypt transmitted or stored data fails, the security against unwanted reading is compromised. As a result, an unauthorized actor can see the content, jeopardizing the product line's confidentiality. In our scenario, the firm employs Signal for rapid secure messaging, client follow-up, and internal communication. For encrypted communication, it also uses the Lavabit email service. An attacker might discover and exploit weaknesses in these systems, exposing the information being communicated between the company and its clients. This again would have a similar consequence as mentioned for the injection vulnerability above.

What is especially important for the company, as has been identified in the previous chapters, is the risk of insiders. Therefore, proper implementation of access control is highly important. If the access control is broken there is a high risk of knowingly or unknowingly disclosure of information across clearance levels. An insider, or external actor if he gains access to the systems first, can abuse this to gain access to confidential information or data. This violation could lead to severe damages to NTNU Analytica, not only because they might lose goodwill and reputation, but also in terms of GDPR fines.

CH7.2 – Inherent Architectural and Element Property Analysis (VAM)

In this section, we will look at how to use the VAM methodology [2]. VAM's purpose is to assist an evaluator in understanding what causes vulnerabilities, what security approaches apply to the detected vulnerabilities, and what possible problems may occur from the security techniques themselves. We should take the following actions to ensure a successful implementation:

1. Identify your organization's essential information functions.
2. Identify essential information systems that implement these functions.
3. Identify vulnerabilities of these systems.
4. Identify pertinent security techniques to mitigate these vulnerabilities.
5. Select and apply techniques based on constraints, costs, and benefits.
6. Test for robustness and actual feasibilities under threat.
7. Repeat steps 3–6 as needed.

The identification of vulnerabilities is done by filling out a vulnerability matrix as seen in Figure 5. To keep the scope of the chapter within the length limitation we will only focus on some of the attributes.

CH7.2.1 – Uniqueness

NTNU Analytica provides a very particular service, namely campaign intervention strategies for altering human behavior. This is why the company is separated into three departments: data analysis, behavioral analysis, and marketing because each department employs specialized and in-depth knowledge on how to carry out duties to bring about such changes. To capture the proper behaviors of the target audience, data analysts must understand how to acquire the relevant data points, and what data points to acquire. The behavioral department must understand how to properly use this data to change and adapt the target audience's behaviors as intended, and the marketing department must understand how to effectively take these ideas and transfer them to the various social media platforms. As a result, the business must retain its staff for extended periods, as training new personnel will take time. The loss of key knowledge can have a significant influence on the growth of NTNU Analytica.

		Object of Vulnerability			
		Physical	**Cyber**	**Human/Social**	**Enabling Infrastructure**
	Attributes	Hardware, network and communication, locality	Software, data, information, and knowledge	Staff, command, management, policies, procedures, training, and authentication	Ship, building, power, water, air, and environment
Design	Singulraity				
	Uniqueness			Highly specialized personnel	
	Centrality		External backup		
	Homogenity				
	Separability				
	Logic/implementation error; fallibility				
	Design sensitivity/fragility/limits/finiteness	Low transmission capacity			
	Unrecoverability		CIS report		
Behavior	Behavioral sensitivity fragility				
	Malevolence			Insider threat	
	Rigidity		Little automation		
	Malleability				
	Gullibility/deceivability/naivete		Social engineering		
	Complacency			Poor risk communication	
	Corruptability/controlabilitiy				
General	Accessible/detectable/identifiable/transparent/intercaptable				Poor physical access control to buildings and rooms, both internally and externally
	Hard to manage or control		Externally managed services		
	Self-unawarenesss and unpredicatability		No implemented logging		
	Predictability	Commercail hardware that is well known			

Figure 5: Vulnerability Matrix

CH7.2.2 – Centrality

Since the organization uses NTNU Cloud Storage for its external backup, they are dependent on a consistent connection. If the cloud storage is unavailable, the corporation might accept missing one backup cycle; nevertheless, not being able to routinely backup the data may have an impact on the organization's resilience if a local data loss incident happens. The same is true if the company wants to access backed-up data but it is unavailable. This might cause issues with the product's development.

CH7.2.3 – Design Sensitivity/Fragility/Limits/Finiteness

The firm is dependent on a high transmission capacity because its core product analyzes open-source data. If the transmission capacity falls below what is required, the pace of data gathering and processing suffers, causing ripple effects across the organization's development process. For the company, intelligence and behavioral data are only valid for a limited time, and they must be able to work quickly. Unavailability will have an influence on various KPIs, including customer happiness.

CH7.2.4 – Unrecoverability

Depending on the backup cycles, part of the organization's data may become unrecoverable if the file is corrupted or similar. If the result, the CIS report, was compromised, the organization may be set back many hours or days. It may not be able to replicate it quickly enough before the data loses value to the client. As a result, unrecoverable is a significant vulnerability for NTNU Analytica.

CH7.2.5 – Malevolence

The vulnerability of an insider has been discussed in earlier chapters. This is due mostly to the clients' emphasis on privacy and confidentiality. If a dissatisfied employee does not like their new customer or acquires a new sense of morality, he or she may wish to leak confidential information to the press. Similarly, the employee may choose to disseminate rumors inside the workplace, which has a detrimental impact on the work environment. These types of sabotage can stifle development and diminish innovation, a healthy work atmosphere, and product quality.

CH7.2.6 – Rigidity

NTNU Analytica has a lot of automation in place to help with data collecting, processing, and presentation. They have not, however, concentrated on the automation of recovery processes in the event of a catastrophe. This lack of automation can have a significant influence on the company's financial loss and is a high risk. If the organization is exposed to ransomware, which is a common malware used to target and blackmail businesses, and does not have an automated procedure for restoring their data from backups, they will end up spending too much time recovering and losing a lot of reputation as well as a lot of money.

CH7.2.7 – Gullibility/Deceivability/Naivete

The organization is said to have lacked attention to information security, which suggests that the employees may have inadequate security knowledge. As a result, they are more vulnerable to social engineering attacks such as phishing, in which an external actor sends a fake email to trick the employee into clicking on malware or otherwise disclosing confidential information. Such vulnerabilities have relatively easy fixes and inadequate awareness training, but the consequences can cause significant financial loss for the business and have an influence the services it provides.

CH7.2.8 – Complacency

Because there is no information security department and no adequate delegation of responsibilities in this area, the business is vulnerable to damage to its profit or reputation as a result of poor risk communication. Management must make judgments based on the facts at their disposal. As a result, if the threats and possible risks are not well conveyed and explained to them, they will fail to invest in the essential security controls or processes. This is because they are pleased with the company's present security posture based on their position and understanding.

CH7.2.9 – Accessible/Detectable/Identifiable/Transparent/Interceptable

The organization is very new and fast-growing, and as a result, they have not yet recognized the significance of the good physical security of the facility. They use a simple card system at the main entry, but no further access control once inside. As they solely employ signs to inform staff about clearance levels, this might lead to personnel entering places holding data of a higher security level. Additionally, there is a possibility that visitors will walk about and acquire access to material that should have been restricted. The repercussions are numerous: theft, destruction, sabotage, financial fines, financial losses, and so forth.

CH7.2.10 – Hard to Manage or Control

The organization's remote site backup repository is NTNU Cloud Storage. As a result, they are dependent on this external service, over which they have no complete control. If NTNU Cloud Storage is vulnerable and attacked by a DDoS attack, the service will be inaccessible to NTNU Analytica, and they will be unable to intervene. External reliances, such as the employment of botnet servers and click farms (used in the CIS deployment), are possible weaknesses that might damage the organization's performance without its ability to regulate it.

CH7.2.11 – Self-Unawareness and Unpredictability

Threat detection is most successful when paired with logging of system and network activities since it allows the organization to apply alternative detection strategies besides signature-based detection. For one thing, signature-based detection only identifies known threats and attacks, which implies that new attacks or zero-days might still be successful on the systems and network. However, if the organization could use anomaly-based detection in targeted and planned portions of its network, it could be able to identify a broader range of threats and attacks. Furthermore, logs would be extremely useful for the incident response team's forensic work after the event.

CH7.2.12 – Predictability

Using well-recognized hardware might be cost-effective, but it also allows external actors to design their assaults more easily, saving them a significant amount of time in the recognizance face of their attack. With this knowledge, attackers may identify previously discovered and exploited malware and vulnerabilities and reuse the code. Furthermore, commercial equipment often comes with servicing agreements done by a third-party organization. If this is the case, the external actor might use this as a possible attack vector by installing malware on the third party's equipment before they enter the premises. As a result, the firewall and other perimeter protection are bypassed.

CH7.3 – Process & Data Flow Modelling

In addition to the VAM technique described before, we may employ process and data flow modeling to detect risks and vulnerabilities [21]. With the knowledge we have learned about the company

from the previous chapters, we can create a data flow chart to uncover risks and vulnerabilities that the VAM technique may have missed. We create a graph containing nodes and edges for this purpose. There are three types of nodes: process, store, and terminator, with an edge representing data flow between the nodes. We obtain the graph shown in Figure 6 by focusing on our KPIs and the organization's ICT systems.

The figure describes the operations and data flows at the highest level. This level may be separated and give even more information, but for the sake of space, we have included only the top level, which presents information about the potential risks and weaknesses faced by the KPIs in the strategy map (ref. Figure 3). For each of the flows we can identify CIA properties and for each process, we can analyze the permitted use of data. This can be used to indicate where there might be vulnerabilities in the model, which we discuss in the following sections.

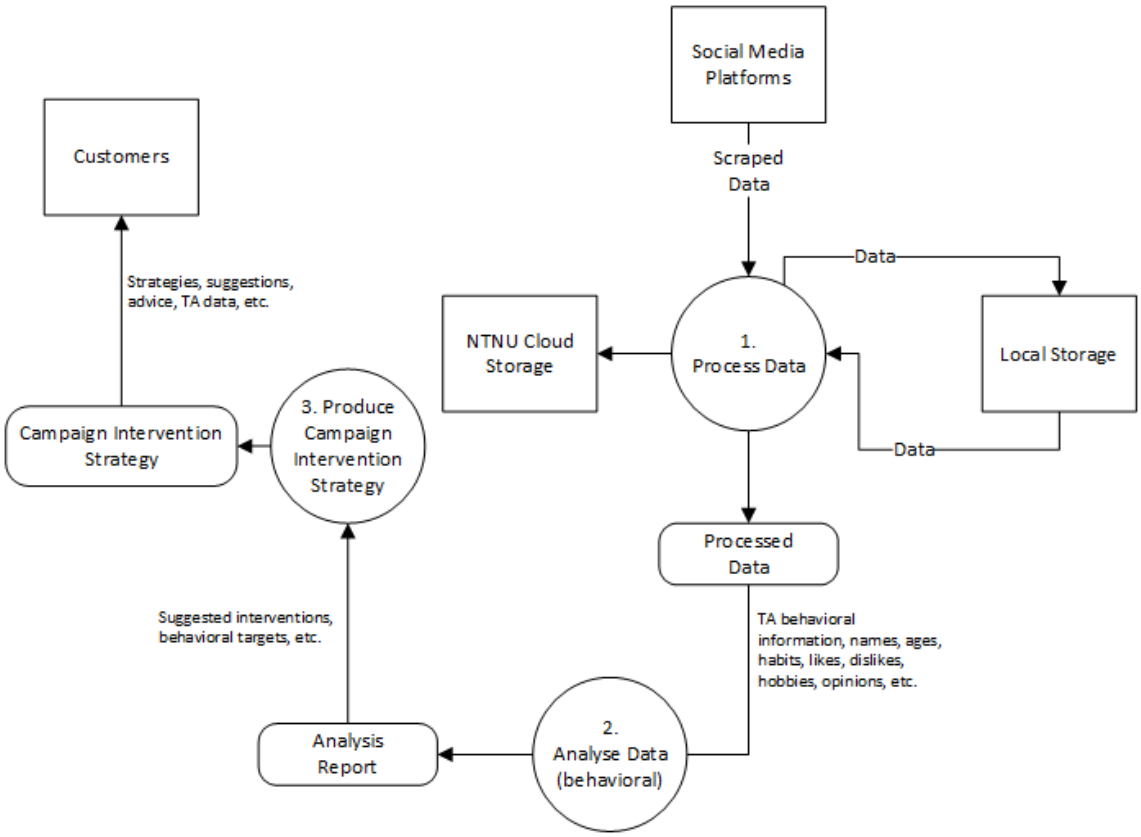

Figure 6: Process & Data Flow Model

CH7.3.1 – Flow From "Social Media Platforms" to Process One

The data is scraped from the social media platforms via VPN. Paid report data is also received from these platforms. The VPN enforces some properties related to confidentiality and integrity, however, the **availability** of the data flow has a possible vulnerability.

CH7.3.2 – Flow From Process One to "Local Storage"

The processed data is transmitted to the local storage server. This happens on a separate VLAN in the architecture, which enforces confidentiality as only those with access to the VLAN can access the data. However we can identify possible vulnerabilities to **integrity** and **availability**. The flow from "Local Storage" to process one has the same attributes as above.

CH7.3.3 – Process One

The scraped data is pre-processed, sent to storage, and forwarded to the next process, which means that the process needs to be allowed to access and modify the collected data. This means that vulnerabilities here can affect all properties of **CIA**.

CH7.3.4 – Flow From Process One to Process Two

The data is sent internally between the one-way filter which ensures the integrity of the original data, however, the integrity of the transmitted data is not protected by this. The confidentiality is kept (to a level) as the data flow happens between VLANs in different LANs, as long as the configuration is correct. There is a potential vulnerability in the **availability** of the service.

CH7.3.5 – Process Two

Not allowed to modify the data, but can access and analyze it.

CH7.3.6 – Flow From Process Two to Process Three

The analyzed data is transmitted to process three. This happens from the DASAS LAN to the General LAN, which means that the **confidentiality** of the data is no longer protected by access to a specific VLAN. The **integrity** or **availability** of the data is also not protected above that of normal network protocols and file handling software.

CH7.3.7 – Process Three

The analysis report is used to produce a campaign intervention strategy. The users need to access the report document, which can affect the integrity. Availability and confidentiality have to be provided.

CH7.3.8 – Flow From Process Three to "Customers"

The final CIS document is sent to the customers via secure e-mail (Lavabit) encapsulated with VPN providing **all** the aspects in the CIA triad. Vulnerabilities in Lavabit, the VPN, or the end-points could be exploited to breach the security.

CH7.4 – Controls, a Top-Down Approach

The most common method for vulnerability discovery is a bottom-up approach, in which we first identify threats and vulnerabilities before looking for controls to mitigate them. In this section, we will use a top-down approach, beginning with the controls, identifying what they protect or address, and then using the identified vulnerabilities or threats to determine whether our company is vulnerable to them.

We start by choosing three controls from COBIT [11]: access control; firewall architectures and connections with the public network; and security principles and awareness training[2]. Next, we identify, for each control, what vulnerabilities it addresses.

[2]Picked from the control list of COBIT.

CH7.4.1 – Access Control

COBIT's identity, authentication, and access control objectives are supported through access control. Its purpose is to prevent unauthorized persons or equipment from gaining access to the system and/or its resources. Access controls provide system owners the ability to govern who has access to what and under what conditions. This is frequently achieved by strategies such as the Chinese Wall or the Bell–LaPadula model. Knowing this, we may deduce that the control is intended to address weaknesses in the areas of confidentiality, integrity, authorization, and authentication.

NTNU Analytica's clients place a high priority on privacy and confidentiality, which extends to the organization's internal procedures. This is one of the reasons for the company's various clearance levels. Vulnerabilities such as broken access controls due to misconfiguration would harm the organization's reputation and might result in financial losses or fines.

CH7.4.2 – Firewall Architectures and Connections With Public Network

The firewall control is used to secure the organization's internal resources from assaults or illegal access. It should also be capable of controlling any application and infrastructure management flows in both directions. As firewalls are used to protect against external threats we can identify threats like denial-of-service attacks or unauthorized access to internal systems. Firewalls can also help identify strange patterns in the network transmissions, which can identify malware communication to remote servers.

We know that NTNU Analytica relies on rapid transmission speeds for data harvesting and that Internet connections must be highly available. This makes them vulnerable to DDoS attacks from actors who deem their operations unethical and wish to obstruct them. Regularly, the business also downloads massive amounts of data. The administration communicates using email. As a result, they may be exposed to malware download and installation.

CH7.4.3 – Security Principles and Awareness Training

The security principles and awareness training control is used to ensure that personnel is properly trained and educated on system security principles. Periodic improvements are part of this, with an emphasis on security awareness and training. This means that management should provide an education and training program that encompasses issues such IT function professional ethics, security measures to guard against harm from failures affecting availability, confidentiality, integrity, and secure job execution. Vulnerabilities and threats that can be identified from this control are those related to ignorance or gullibility. A common example of this is phishing attacks.

Because NTNU Analytica mostly interacts via secure communications, which need the use of a shared cryptographic key, there is a low risk of spam mail or phishing because they visit their clients in-person to share the key. Because new clients are requested to utilize pretty-good-privacy (PGP) encryption for the initial conversation, where the key is presented on their website, most mail that arrives outside of this is rejected by the company's staff. The attackers may spend more time sending phishing emails using PGP, but because employees must use the PGP solution, they are also more conscious of the security component of the emails and are more likely to pay attention.

CH8 – Controls

In this chapter, we first identify relevant control categories for the vulnerabilities identified in CH7 before we address a sample of vulnerabilities. The control categories are found by consulting the ISO 27001 Annex A [13] and COBIT[3] [11] and presented in Table 20.

Table 20: Control Categories

Standard	Control Category
COBIT	Access control
COBIT	Awareness and training
COBIT	Audit and accountability
COBIT	Security assessment and authorisation
COBIT	Configuration management
COBIT	Contingency planning
COBIT	Identification and authentication
COBIT	Incident response
COBIT	Maintenance
COBIT	Media protection
COBIT	Physical and environmental security
COBIT	Planning
COBIT	Personnel security
COBIT	Risk assessment
COBIT	System and services acquisition
COBIT	System and communication protection
COBIT	System and information integrity
COBIT	Program management
ISO 27005	Information security policies
ISO 27005	Organization of information security
ISO 27005	Asset management
ISO 27005	Cryptography
ISO 27005	Supplier relationships
ISO 27005	Information security aspects of business continuity management
ISO 27005	Compliance

The lack of monitoring mechanisms was one of the vulnerabilities discovered using VAM. We consider this a relevant vulnerability because we have previously identified the threat of an insider. This threat could be mitigated by implementing personnel security controls during the recruitment process. This could help ensure that the personnel hired have values and a mindset that aligns with the company's mission and vision, making them less likely to turn against it. This could also include controls that measure staff performance, behavior, and contempt, which can reveal factors such as whether employees are happy or unhappy, or if they are considering quitting. We could also mitigate the vulnerability by enforcing stricter access controls, auditing and accountability, and identification and authentication controls. This would reduce the likelihood of a potential insider threat doing anything wrong by limiting access to information he/she could steal or reveal. Furthermore, the company could devise a strategy for dealing with potential leaks to the press or media, allowing them to take a proactive approach to the threat.

The data flow from social media platforms was identified as another vulnerability using the process and data flow model. If the company is unable to communicate via the Internet, they lose their source of intelligence data, which could halt the production of CIS reports and have a significant impact on the company's revenue in terms of potential project fines for failing to deliver on time, loss of reputation, loss of potential customers, and so on. This could happen as a result of a targeted DDoS attack or a hardware failure because the company's network lacks redundancy. It can be difficult to control the external threat that is causing a DDoS, but the organization can

[3]Due to lacking access to the full ISO 27001 Annexes, we combine other standards to supplement the controls.

protect itself by implementing policies for information security, incident response, and configuration management. NTNU Analytica may be able to reduce its external footprint and become more difficult to target if they have control over which interfaces are open to the Internet and have personnel who know how to communicate securely. In the event of an attack, they may have an incident response and contingency plans in place, allowing them to recover more quickly. Internally, they could improve the network by limiting single points of failure and establishing an SLA with their ISP to reroute data traffic caused by DDoS attacks.

CH8.1 – Real Option Controls

In this section, we include a "real option" control and explain, defend, and compare it to a "possible 'non-real option" control addressing comparable prospective circumstances [10].

The restrictions indicated above might be applied all at once in a single investment. However, it might also be implemented as actual alternatives, giving the organization the ability to extend, change, or discontinue initiatives in response to changing economic, technological, or market conditions. As a result, NTNU Analytica's management has the option, but not the responsibility, to pursue specific commercial possibilities or investments. It refers to initiatives employing actual assets rather than financial instruments and might involve the option to expand, delay or wait, or completely cancel a project. Because actual alternatives have economic worth, financial analysts and business executives may utilize them to make judgments.

As an example, consider using a real choice solution for incident response. Instead of NTNU Analytica investing in their incident response team, which would mean an upfront investment as well as the continuous cost of employing and training staff, they could outsource the service. This would offer them the option to grow which means the right to enhance the operating size of the project if the resolution of the future uncertainty is positive. Furthermore, they may have the option of contracting the project if the resolution of ambiguity is undesirable. Various more actual possibilities apply to this control; in general, it gives for more freedom in investing. In this case, it may be more advantageous because they would invest a lower amount at the start and have the option to delay or increase as needed.

CH8.2 – Quantifying Costs/Benefits

In this section, we use uncertainty frames to quantify costs or benefits in terms of the lead indicators that are identified for the balanced scorecard measures in Chapter 5. For this, we will use an example where we assume that we have access to the financial information of our organization.

The firm has an internal discrete interest rate of 5-15 percent every year. The occurrence to be protected against is likely to occur within 12-36 months, resulting in a loss of 500.000-1.000.000 NOK. The proposed control will limit this loss, but it must be implemented immediately at 400.000-700.000 NOK. We want to determine if implementing the control is useful or cost-effective. The control cost is assumed to be $CC = [400.000, 700.000]$.

We apply the incident cost formula: $CI \times e(-RC \times T)$, where $RC = ln(1 + RD)$ and $RD = [0.05, 0.15], T = [1, 3], CI = [500.000, 1.000.000]$. We chose to be conservative in this computation, therefore a result [a,b] is calculated to be [floor(a), ceiling(b)].

The continuous interest rate: $RC = ln[1 + [0.05, 0.15] = [ln(1 + 0.05), ln(1 + 0.15)] = [0.048, 0.139]$
Incident cost: $IC = [500.000, 1.000.000]e^{-([1,3]\times[0.048,0.139])} = [500.000e^{(-0.139\times3)},$
$1.000.000e^{(-0.048\times1)}] = [329510.459, 953133.787] \approx [329.511, 953.134]$

The management may now consider both the CC and IC costs to determine if it is worthwhile to adopt the control. In this situation, the intervals, [400.000, 700.000] and [329.511, 953.134], overlap, indicating that we do not yet have enough information to decide whether to use the control. More research will be needed to make a decision.

CH9 – Compliance Based Security

In this chapter, we look at risk from a decision-theoretic standpoint. This is achieved by a quick application of decision theory to information security risk assessments. We concentrate on a scenario coming from an initial event related to information system misuse. We derive a series of events/alternatives from the situation. We use Event Tree Analysis (ETA) in conjunction with fuzzy decision theory to achieve this evaluation [8]. In this part, ETA is used to prevent failures caused by the invasion of NTNU Analytica's storage servers. This is done as we analyze the risk associated with the significant events that we identify. As a consequence, the ETA is utilized as a reference to assure the organizations' safety. As a consequence, the ETA is used as a guide to assure the security of the organization's storage servers by applying extra safety measures that match to risk components detected during analysis.

We picked ETA because it teaches us how to protect ICT systems from potential security hazards in the context of information security. Using ETA as a tool to uncover and assess all possible system consequence paths after an initiating event, as well as the consequences that may develop as a result of the occurrence of a potentially problematic event, can lay the framework for the establishment of information security legislation. Furthermore, the National Institute of Standards and Technology (NIST) defines risk as follows [3]:

> "Risk is a function of the likelihood of a given threat source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization."

As can be observed, it emphasizes the need of describing events that cause IT security errors. As a consequence, it's a legitimate option to apply the previously defined ETA technique, which is used to identify and analyze the sequence of events in a likely accident scenario.

In this section, we also use fuzzy decision theory to develop a realistic choice model since it allows us to handle ambiguous data as precisely as possible. This statement may be valid since expecting correct data all of the time, if at all, is impractical. Later in the Risk Assessment process, decision theory and fuzzy logic are used to determine the likelihood of occurrence and make judgments about these elements. We chose the fuzzy expected values (FEV) characteristics since they have been proposed as a method of characterizing the risk associated with an act-event in information security management. To do so, we must first identify two confusing elements:

Fuzzy probabilities: $\tilde{P}_j = \tilde{P}_{s_j} = \{(p, \mu_{P_j}(p) | p \in [0,1])\}$ (1)

Fuzzy utility vales (consequences): $\tilde{U}_{ij} = \tilde{U}_{a_i, s_j} = \{(u, \mu_{U_{ij}}(u) | u \in U)\}$ (2)

Where a_i denotes actions and s_i denotes potential nature states (possible scenarios). We presume that our experts are familiar with the utility function $u = u(g_{ij})$. Following that, the fuzzy outcomes are translated to the fuzzy utilities, or the experts define utility values explicitly, where U is the potential set of crisp utility values.

We also need to assume that all a can be modeled as a fuzzy number like:

$$\hat{A} = \{(x, \mu_{\hat{A}}(x)) | x \in R\} \text{ with } \mu_{\hat{A}}(x) = \begin{cases} 1 \text{ if } x = a \\ 0 \text{ else} \end{cases} \quad (3)$$

Lastly we define that all act-events defined as combinations of (ai, sj), are valued by a fuzzy interval. This can be shown as an function for the membership $\tilde{U}_{ij}$:

$$\tilde{U}_{ij} = (\underline{u}_{ij}^{\varepsilon}; \underline{u}_{ij}^{\lambda}; \underline{u}_{ij}^{1}; u_{ij}^{-1}; u_{ij}^{-\lambda}; u_{ij}^{-\varepsilon})^{\lambda, \varepsilon}, i = 1, ..., m; j = 1, ..., n. \quad (4)$$

The membership is based on an estimate of a fuzzy set generated by two α-cuts: $\alpha = 1 : \mu_{\tilde{U}_{ij}}(u) = 1, u$ has the highest chance of belonging to the set of utility values associated with the act-event combination (a_i, s_j).

$\alpha = \lambda : \mu_{\tilde{U}_{ij}}(u) \geq \lambda$, the decision maker or the expert is willing to accept u as an available value for the time being. A value u with $\mu_{\tilde{U}_{ij}}(u) \geq \lambda$ has a good chance of belonging to the set of utility values associated with the act-event combination (a_i, s_j). Corresponding values of u are relevant for the decision.

$\alpha = \varepsilon : \mu_{\tilde{U}_{ij}}(u) < \varepsilon, u$ has only a very little chance of belonging to the set of utility values associated with the act-event combination (ai, sj). The expert is willing to neglect the values u with $\mu_{\tilde{U}_{ij}}(u) < \varepsilon$.

The information security model is divided into four stages: expert identification, scenario and event determination, fuzzy assessment, and order. We examine the consequences of each solution in terms of financial loss by going through the phases and evaluating the various possibilities.

CH9.1 — Expert Identification

We begin by contacting specialists from NTNU Analytica's several departments to identify vulnerabilities, probable accidents, conceivable scenarios, the chance of occurrence, and their opinion on each of these components. Our specialists have created a preliminary overview of the organization's major features, which is given in Table 21.

Table 21: NTNU Analytica's Services

Services	**Description**
DCSS application	A data collection and storage system used by the Data sicence departmetn to collect, process, and store open-source data before it is distributed to DASAS.
DASAS application	A data analysis and situational awareness system used by the Behavioral department for the analysis and management of the information to conduct target audience analysis (TAA), behavioral modeling, and target audience profile development (TAP).
CIS report	A report produced by the Marketing department which uses the results from the Behavioral department presented in DASAS to further create campaign intervention strategies (CIS) using TAP and TAA to tailor strategies for influence, which is presented to the customers with the SA picture of the TA

CH9.2 — Definition of Events and Scenarios

With the elements and judgments discovered in the previous step, we may propose the ETA model in Table 23. This was built based on expert knowledge to offer definitions of various occurrences and situations in the context of the penetration of NTNU Analytica's data storage servers. Because it is difficult to assign a numerical value to probable accidents due to the uncertainties involved, we have opted to employ triangular fuzzy numbers. The triangular fuzzy values are shown in Table 22 and are used to depict the financial effects of each choice for each condition of nature. The scale is a verbal scale with five levels (very low, low, moderate, high, and very high). Triangular fuzzy numbers are represented by the triple $(a; m; b)$, where a and b represent the bottom and upper limits of a fuzzy set, respectively, and the parameter m represents the modal (typical) value of this set.

According to the expert, the financial damage resulting from a data storage server attack might vary from 100,000 NOK to 2,500,000 NOK. As a result, the verbal scale encompasses this range.

Using the prior results, a taxonomy of the events and scenarios is then built to reflect the concerns connected to assessing the information security risk, their susceptibility, and repercussions (see Table 23).

Table 22: Verbal Scale of Financial Consequences

Verbal terms	Fuzzy number	Values	Unit
Very low	Triangular	(100;250;450)	Thousands NOK
Low	Triangular	(500;750;950)	Thousands NOK
Moderate	Triangular	(1000;1250;1450)	Thousands NOK
High	Triangular	(1500;1750;1950)	Thousands NOK
Very high	Triangular	(2000;2250;2500)	Thousands NOK

Table 23: Event Tree Analysis for the Data Storage Server Invasion (Attack)

Event	Failure Mode	Origin	Possible Scenarios
Invasion of Data Storage Servers	Internal Access	Accidental	Disclouser of Total Data
			Manipulation
			Loss of Information due to misoperation
			Denial of service
		Deliberate	Disclosure of Total Data
			Manipulation
			Loss of Information due to misoperation
			Denial of service
	External Access	Accidental	Disclouser of Total Data
			Manipulation
			Loss of Information due to misoperation
			Denial of service
		Deliberate	Disclosure of Total Data
			Manipulation
			Loss of Information due to misoperation
			Denial of service

CH9.3 — Fuzzy Assessment of Potential Accidents and Ordering

The possible accidents will be assessed in the next step. We use the previously described fuzzy components and scales for this. The first step is to compute the anticipated value of all risk-adjusted options. This is accomplished by specifying the nature states and alternatives in the respective act-event combinations. The evaluation of our experts is then obtained utilizing fuzzy logic and the prior probabilities $p(s_j)$, where the prior probability by can be indicated by π and nature states by θ. This offers us the symbol $\pi(\theta)$ for our prior probability with our natural states. The nature states, θ, are the conceivable outcomes of a data storage server invasion. The states we mentioned are data dissemination (θ_1), data modification (θ_2), data loss or destruction (θ_3), and service interruption (θ_4). The act-event combinations were created by grouping data center services (DCSS application (DC), DASAS application (DA), and CIS report (C) with two failure modes (internal (I) and external (E) access) and two probable sources (accidental (A) and intentional (D), generating a total of twelve alternatives (see Table 24).

Table 24 evaluation shows how experts assess various options and conditions of nature. The five-level verbal scale was used for this. Furthermore, Table 25 displays the decision matrix that displays the expert's judgments on the financial losses of each choice for each natural state. To show the values, we utilize the matching triangular fuzzy numbers.

Now that we've evaluated the nature states, we can turn our attention to the prior probability $\pi(\theta)$. We utilize $\pi(\theta)$ because it takes into account professional expertise or previous data regarding assaults on data storage systems. In our implementation, we believe that our professionals would

Table 24: Expert's Elicitation Evaluation

Alternatives (A_i)	θ_1	θ_2	θ_3	θ_4
DA/I/A(A_1)	H	VH	M	L
DA/I/D (A_2)	L	M	M	H
DA/E/A(A_3)	L	VL	VL	VL
DA/E/D(A_4)	M	M	VH	VH
DC/I/A(A_5)	M	L	VL	L
DC/I/D(A_6)	VL	VL	L	L
DC/E/A(A_7)	M	L	M	M
DC/E/D(A_8)	L	H	M	VH
C/I/A(A_9)	H	VH	VH	M
C/I/D(A_{10})	VH	M	H	VH
C/E/A(A_{11})	L	M	M	L
C/E/D(A_{12})	H	VH	H	VH

Table 25: Decision Matrix

Alternatives (A_i)	θ_1	θ_2	θ_3	θ_4
DA/I/A(A_1)	(650;1000;1300)	(2000;2250;2500)	(1000;1250;1450)	(500;750;950)
DA/I/D (A_2)	(500;750;950)	(1000;1250;1450)	(1000;1250;1450)	(650;1000;1300)
DA/E/A(A_3)	(500;750;950)	(100;250;450)	(100;250;450)	(100;250;450)
DA/E/D(A_4)	(1000;1250;1450)	(1000;1250;1450)	(2000;2250;2500)	(2000;2250;2500)
DC/I/A(A_5)	(1000;1250;1450)	(500;750;950)	(100;250;450)	(500;750;950)
DC/I/D(A_6)	(100;250;450)	(100;250;450)	(500;750;950)	(500;750;950)
DC/E/A(A_7)	(1000;1250;1450)	(500;750;950)	(1000;1250;1450)	(1000;1250;1450)
DC/E/D(A_8)	(500;750;950)	(650;1000;1300)	(1000;1250;1450)	(2000;2250;2500)
C/I/A(A_9)	(650;1000;1300)	(2000;2250;2500)	(2000;2250;2500)	(1000;1250;1450)
C/I/D(A_{10})	(2000;2250;2500)	(1000;1250;1450)	(650;1000;1300)	(2000;2250;2500)
C/E/A(A_{11})	(500;750;950)	(1000;1250;1450)	(1000;1250;1450)	(500;750;950)
C/E/D(A_{12})	(650;1000;1300)	(2000;2250;2500)	(650;1000;1300)	(2000;2250;2500)

stay risk-averse in terms of financial issues. To evaluate the robustness of the final model, we compute $\pi(\theta)$ using two techniques. The first is based on Laplace's criterion: "[I]f no data on the probability of the various possibilities are available, it is acceptable to assume that they are equal"; while the second is based on our experts' experience. This computation yields the FEVs shown in Table 26, which were computed using the following equation:

$$\tilde{E}(a_i) = \tilde{U}_{ij} \otimes p(s_1) \oplus ... \oplus \tilde{U}_{in} \otimes p(s_n) = (\underline{E}_j^{\varepsilon}; \underline{E}_j^{\lambda}; \underline{E}_j^{1}; E_j^{-1}; E_j^{-\lambda}; E_j^{-\varepsilon})^{\varepsilon,\lambda} \tag{5}$$

Table 26 displays the results of the FEV calculations. The first column provides the probabilities defined by Laplace's criterion, whereas the second column has the probability obtained from the expert.

Finally, we show the rankings of the two techniques in Table 27 ranking to make it easier to understand. The ranks were determined by graphing the values of each FEV for both approaches, comparing the projected profits, and determining the maximum values.

According to Table 27, alternative A_{12}, a purposeful external CIS report assault, poses the greatest danger and should be prioritized. This holds for both ways. Using the Laplace's criteria, the risks of alternatives A_9 and A_{10} are comparable. However, it is worth noting that alternative A_{10} had the second greatest risk when employing expert elicitation as well as Laplace's criteria. Another significant finding was that alternative A_3, an unintentional external assault on DASAS, was the least dangerous option for both techniques. We can also observe from the table that the relevance of the choices stays constant despite the difference in the probability determined by the two techniques. Furthermore, we find that the two choices with the largest risk both result from purposeful acts, implying that increased efforts in internal monitoring of the organization's

operations should be emphasized because the repercussions of such deliberate actions generally do greater harm.

Table 26: Fuzzy Expected Value (FEV)

Alternatives (A_i)	**FEV (Laplace Criteria)**	**FEV (Expert's Elicitation)**
W/I/A(A_1)	(703.1; 1109.4; 1421.8)	(676; 1052; 1347)
W/I/D (A_2)	(500; 796.8; 1046.8)	(537; 842; 1102)
W/E/A(A_3)	(171.8; 250; 328.1)	(177; 257; 337)
W/E/D(A_4)	(842.5; 1375; 1750)	(843; 1375; 1750)
EC/I/A(A_5)	(296.8; 453.1; 593.7)	(321; 490; 641)
EC/I/D(A_6)	(218.7; 312.5; 406.2)	(218; 312; 406)
EC/E/A(A_7)	(406.2; 671.8; 890.6)	(410; 681; 903)
EC/E/D(A_8)	(703.1; 1109.3; 1421.8)	(777; 1222; 1555)
DB/I/A(A_9)	(937; 1500; 1906)	(835; 1340; 1715)
DB/I/D(A_{10})	(937.5; 1500; 1906.2)	(1010; 1620; 2047)
DB/E/A(A)	(375; 593.7; 781.2)	(357; 550; 720)
DB/E/D(A)	(1031.2; 1625; 2062.5)	(1066; 1685; 2132)

Table 27: Alternatives Ranking

Alternatives (A_i)	**Ranking (Laplace Criteria)**	**Ranking (Expert's Elicitation)**
DA/I/A(A_1)	4th	6th
DA/I/D (A_2)	5th	7th
DA/E/A(A_3)	10th	12th
DA/E/D(A_4)	3rd	3rd
DC/I/A(A_5)	8th	10th
DC/I/D(A_6)	9th	11th
DC/E/A(A_7)	6th	8th
DC/E/D(A_8)	4th	5th
C/I/A(A_9)	2nd	4th
C/I/D(A_{10})	2nd	2nd
C/E/A(A_{11})	7th	9th
C/E/D(A_{12})	1st	1st

CH10 – The Intelligent and Strategic Attacker

In this chapter, we apply game theory to two previously discussed scenarios in this paper. The first scenario is about an internal violation of confidentiality. The second scenario involves being attacked by a motivated hacker, and the third part expands on the game theory application in the second scenario. The usage of game theory and execution becomes more prevalent as the sections progress to show various levels and outcomes. Do we examine some of the most common issues that emerge when gamifying a scenario: (1) What information does your opponent have about you? (2) the confidentiality of our risk assessments, (3) the processes used, (4) a comprehensive defense (depth), and (5) the budget size We must first decide on the type of game that will be used to represent our circumstance. Is it preferable to cooperate or not? In the described case, we can see dependencies where what is good for one agent is not always good for the other agents, hence a non-cooperative game model looks to be the best choice.

The general game model is made up of various components, including a move, strategy, players, a node, utility, result, reward, and an information set. Moves are activities that advance the game or are connected to the ordering of information. Tactics are ways of play that dictate the players' responses to all conceivable strategies. Players are mechanisms that can make decisions about what to do next. Nodes are areas in the game where players must act. The outcome or a payment motivates players, while the utility is a measure of attractiveness. Utilities might be ordinal or cardinal. The information set is used to store information about prior events in the game that the player is unaware of. This may or may not apply to the player.

We make the following assumptions for this chapter: Players are considered to be economically rational; they assess outcomes, compute pathways to outcomes, and select the actions that result in the optimal outcome given the actions of the other players. In terms of information availability, we suppose that participants might have perfect or imperfect information, and that information availability may influence the result.

CH10.1 – Internal Breach

For our first scenario, we create a situation in which we wish to investigate how we might prevent employees from violating confidentiality from an information security standpoint. We are particularly interested in incidents in which two staff members collaborate to steal and sell information from different clearance levels. The first stage is to identify the scenario's agents. In the scenario, an NTNU Analytica employee violates confidentiality by knowingly or unintentionally providing material to a person outside the firm or to workers who do not have the proper clearance level. We identify three agents: the employee who is leaking information (agent A), the employee who is being exposed to the information (agent B), and the information security officer who is attempting to prevent the scenario (agent C) (agent C). This is predicated on the notion that agent A's optimal action is determined by agent B's and C's views, and these agents' decisions are influenced by A's beliefs. To determine how the employees would react if the situation occurred, we created a game model similar to the prisoner's dilemma [16] using the following scenario:

- Confidentiality breach: Two responsible staff members are discovered leaking information across clearance levels.
- They sold the information to the press.
- The company believes they were attempting to sell the material to the press, but they only have enough proof to show they violated internal confidentially. As a result, NTNU Analytica requires one of the employees to inform the other to prosecute them for the larger offense.
- Based on information from NTNU Analytica's attorneys and internal policies, NTNU Analytica makes each of them an offer. They have the following options:
  - If none of them admits to selling data, the organization may only prosecute them with violating confidentiality on purpose.

    - Punishment: Restricted access for both (utility = -1).
- If one confesses and informs on the other, but the other does not, NTNU Analytica will be lenient on the informer and severely punish the other.
    - Punishment: Fire the other (utility = -3), 0 repercussions for the informer (utility = 0).
- If both of them confess, the organization will penalize them equally.
    - Punishment: Restrict access and fine both (utility = -2).

This gives us the following payoff matrix (ref. Table 28).

Table 28: Prisoner's Dilemma Outcomes

		Player 2	
		Keep quiet	Inform
Player 1	Keep quiet	(-1,-1)	(-3,0)
	Inform	(0,-3)	(-2,-2)

First, we look at Player one's options. Assume he knows that player two will inform. Player one's best option, in this case, is to inform. Keeping quiet will give him restricted access while informing will let him walk away. Assuming that player two will inform we see the same thing. Player one is better at informing as well. If he keeps quiet he will be fired, while informing only restricts his access and gives him a fine. Consequently, Player one will inform in this game. No matter what Player two does, Player one is better at informing. This means that the inform strategy strictly dominates the keep quiet strategy and the rational player by rule, never plays a strictly dominated strategy. Now, let us look at Player twos options. Imagine Player one keeps quiet, as we saw with Player one. Player two's best response here is informing as no punishment is better for her than having her access restricted. If Player one is informed, Player two's best response is to inform as well since restricted access and a fine are better than being fired. So the inform strategy strictly dominates the keep quiet strategy for her as well, meaning Player two will defect in this game. Thus we have a Nash equilibrium: (inform, inform). Both the players would be better off if they both had cooperated, as they would only have their access restricted. But because there is the temptation of screwing over the other player by informing on them, the (inform, inform) Nash equilibrium is the only stable outcome. The rationale here is: why would you want to keep quiet when you could inform and do better?

With this information, we can see that we can, of course, apply tougher restrictions and access controls. However, limiting human error is not always the most cost-effective strategy since we never know what a person will decide to do. As a result, we may wind up spending a lot of money without ever exhausting all of our options. The game model assists us in identifying areas where we may choose to focus our efforts to be more cost-efficient. Furthermore, based on our example, we can see that introducing certain incentives may be a viable alternative. Assuming we can't prevent it from happening, our best bet is to be able to recognize and punish it. Given that the game's Nash equilibrium is that both opt to inform, we may be quite certain that we will be able to penalize the behavior. As a result, focusing on controls such as access logs and alarms, as well as frequent behavioral monitoring of personnel for detection, would be a priority. Because the scenario is a simplification of the actual world, we might alternatively opt to focus on incentives that encourage participants to share information. This might be in the form of physical threats such as big fines or "propaganda" indicating how many employees are caught in comparison to those who attempt. It might also be positive incentives, such as awards, that motivate the player to disclose. This increases the chance of establishing their guilt.

CH10.2 – Attacked by Hacker

Building on the preceding section, we have a situation in which we want to understand how we should deal with an attacker who wishes to violate the confidentiality of the organization. We decided not to consider availability or integrity. What we must remember about confidentiality is that it seeks to limit access to or establish limits on specific types of digital information that is managed by the computer or/and supplied to the destination through a network. The primary distinction between confidentiality and other security attributes is that effective defenses for confidentiality are confined to prevention because once the attacker has gained access to the system, recovery efforts are futile.

It is widely acknowledged that attackers now have the dominant strategy in information security. To address this, we'd like to investigate whether we can alter the situation by including deception in our security procedures. We use a three-shell game model for this. The model consists of three shells and a ball. The ball is concealed behind one of the shells. The dealer shuffles the shells, and the player must predict where the ball is. Statistically, the player will always lose the game over time since it is relatively easy to misinform the player about where the ball is. We consider this ball to be our data. If we shift our data around and build deceiving environments, we will gain a significant edge and ensure that we win in the long run. This is possible by creating deceptive environments in which only the attacker lives. In this environment, we have complete control over the attacker's movements and information, and we have full insight into it. In general, we must be able to redirect attackers away from genuine high-value assets and data and into this deceptive environment. As the attacker interacts with the deceptive environment, he exposes himself since no genuine user functions in it. As a result, we know they're on our network, what they're doing, how they're doing it, and how long they've been doing it. We can also mislead the attacker about the network architecture, what the data is, where they landed, and so on. For this to operate in practice, we must provide incentives for attackers to choose to target deceptive environments. As we wish to detect the attackers, the aim must be for the attacker to notice these incentives while actual users remain unaffected. This may be accomplished by employing honeypots that appear to hold very important information. If the attacker compromises a real environment, we can use baits to trick the attacker into switching to a deceptive environment.

Because of the employment of honeypots, the attacker is slightly more likely to choose two of the misleading settings in our shell game model. We presume that the honeypots function ideally such that attackers do not suspect their authenticity before entering the ecosystem. If he enters a misleading setting, we suppose he has a 20% probability of understanding it is not the genuine world. We anticipate that if he enters a genuine environment, there is a 10% probability that he will be lured by our bait, which will lead him to one of the misleading habitats. The payout for the attacker is lower if he successfully attacks a misleading environment, while the payoff for the defense is larger because the organization suffers less as a result of the breach. If the attacker realizes he is in a misleading setting, his payout is somewhat higher since he can at least cease the attack and save money and time. The defender receives a little lesser payout due to the discovery of the misleading environment but is partly salvaged by the fact that the attacker has lost faith in the prospective stolen data. If the attacker is in the real world and takes the bait, he will very certainly find himself in one of the misleading environments, where the aforementioned scenarios will play out. Finally, the attacker may be completely successful and extract highly valuable data from the real environment. As a result, his payout is the best in this case, while the defender's payoff is the worst.

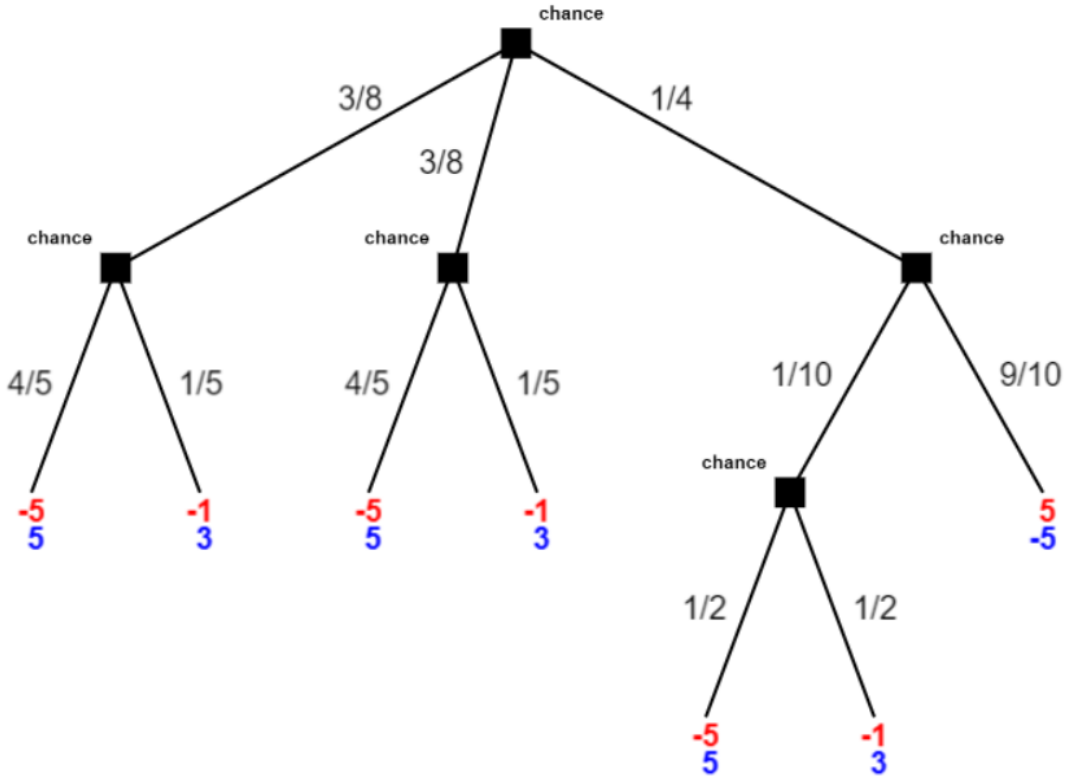

Figure 7: Shell Game Model Produced Using the GTE v2.2.5 Tool.

If we solve the game using the GTE v2.2.5 tool we get the following result:

```
1 x 1 payoff matrix A:
  −21/10

1 x 1 payoff matrix B:
  97/40

EE = Extreme Equilibrium, EP = Expected Payoff
Decimal Output
  EE 1 P1: (1) 1.000000 EP= −2.1 P2: (1) 1.000000 EP= 2.425

Rational Output
  EE 1 P1: (1) 1 EP= −21/10 P2: (1) 1 EP= 97/40

Connected component 1:
{1} x {1}
```

According to the answer, Player two, the defense in this model, has the dominating strategy, with an extreme equilibrium of $\frac{13}{45}$ to the attackers' $-\frac{13}{45}$. Looking at 7, it is clear that we might boost the attacker's odds of accessing a misleading environment even more by widening the attack surface with additional deceptive surroundings. However, this is contingent on the size of the budget. We can also devise methods to raise the attacker's desire to select them to improve our chances. There are three main advantages to using deception:

1. Attacks fail because the attacker is given incorrect information, i.e., they have no idea what the network topology is and hence make poor judgments. The attack takes longer and costs more money because the attacker must continually question whether what he sees is real or not.

2. Because the attacker has no way of knowing if the data is real or not, the stolen information is less valuable. As a result, he no longer has faith in the facts.

3. When security personnel knows where the attacks are, they spend less time searching for them and dealing with false positives. They can shift from damage control to damage prevention.

In essence, we are putting the responsibility on the attacker rather than the security team.

CH10.3 – Attack on the DCSS Storage Servers

This section expands on the scenario of an external attack. The attackers' aim in this situation is the DCSS storage servers. We want to employ decision tree modeling again, but this time we want to build on the notion by incorporating more human behavior thinking. We begin with a SWOT analysis to obtain perspective on NTNU Analytica's position concerning the adversary and vice versa [12]. For brevity, we limit the scope of our study to what is required to demonstrate the notion and reasoning.

Table 29: SWOT Analysis

Strengths	Weaknesses
Understanding of target environment	Inadequate budget
Motivation to not be breached	Lack of personnel
	Limited employee training
Opportunities	**Threats**
Leverage new tech to allow for tear up/down	Attackers can use new tech for scalability
Increased board attention to get budget	Hard to keep up with pace of new attack surfaces

The next step is to conduct a perceptual SWOT analysis, in which we analyze how strengths may become weaknesses and weaknesses can become strengths. The reasoning behind this strategy is to be able to adopt efficient judo strategies in which we leverage our opponents' advantages against them to win the game. This also implies that the organization's key skills may be flaws. An examination of the organization reveals several deeply established knowledge sets that may cause difficulties in the future. This is seen in top management because, most of the time, the organization is in an evolutionary stage, and whoever was in top management did well in the status quo situation. However, when things evolve, they may be unprepared for what is to come, which may be a major issue for the organization. We also noticed that the existing compliance enforced in the firm by information security responsible personnel is fairly tight, with established security principles. This initiative helps to move employees in the correct way for information security, but in the long run, it creates additional rigidity and friction, which can harm the business.

Thinking about it from the opposite side, we concentrate on how we may begin to exploit the attacker's strengths and turn them into vulnerabilities. Having adequate time to prepare the attack is one indication of attacker strength, as revealed in the SWOT analysis (ref. Table 29). Defense is extremely responsive and swift, while attackers usually have enough time for recon to figure out how to construct an attack that will work. What we can do is capitalize on their power by employing techniques that drive them into rabbit holes and squander their time. Another is that attackers are aware of vulnerabilities. We may not have discovered all of our organization's vulnerabilities, and the attacker may know that we are unaware. What we can do is start confusing them with bogus architectures so they don't know which systems NTNU Analytica is operating. This makes it more difficult for the attacker to exploit the flaws they have created.

Using this data as a starting point, we develop belief prompting, which enhances the players'

thinking by one step in our game. The idea here is to get the player to think about their opponents and how they will react to them. We wish to model assumptions about capital, time, tools, risk aversion, and other factors. Attackers, on average, are more risk cautious than defenders. This kind of thinking is used to create a decision tree. We consider the following questions in this regard:

1. How would attackers preemptively bypass the defensive move?
2. What will the opponent do next in response?
3. What is the cost of the opponent's offensive move?
4. What is the probability of the opponent conducting the move?
5. Which of our assets will the attacker want?
6. What is the easiest way to those assets?
7. What countermeasures are on that path?
8. What new path will the attacker take?

In our case, we assume that a hacker has gained access to one of our servers. What are they going to do next? They will most likely perform local recognition and advance to any rights they can obtain. To counteract this, we may enforce privilege separation and guarantee that no credentials are hardcoded in the organization. As a result, the attacker must exploit the server, with the risk that the server may crash. As a result, the attacker's danger increases. In the context of thinking exploitation, we want to start to use the fact that we can think ahead of the attackers and start to model out ahead of time before they have had a chance to act. We intend to model and display both the offensive and defense so that we may find if-then-then patterns. We want to theorize the probabilities of each branch's result so that we can determine the chance of an assault succeeding as well as the likelihood of the defensive measure working. This will provide real measures to discourage self-justification, implying that the decision tree is essentially just a representation of sequential games using game theory as the overarching language. Finally, attackers will follow the shortest path across an attack graph from their start node to their objective node. This yields the decision tree shown in Figure 8:

In our scenario, we observe a criminal organization that gets to arrive on one of our DCSS servers running Linux, and at this point, we suppose that they intend to exfiltrate some database credentials. The first path to the right, where the defenders do not use any privilege separation, is the easiest (noted: No strategy). As a result of taking this route, they now have root access. If they continue on the no strategy path, and the defense does not have role separation, they can use the database on the Linux server; and if the defense does not have segmentation or similar protection mechanisms, the attackers can successfully obtain the credentials and exfiltrate the data from the server. The difficult approach, though, is to declare that we do have privilege separation. The attacker must next employ a known vulnerability or search for accessible data. From then, the defense can employ Grsecurity or Seccomp to move the attacker into the 1-day or 0-day realm, which the defense wants to get to because it is incredibly expensive for the attackers.

We can utilize the decision tree to enhance audits after an event since it encodes what our assumptions were at the time. It also acts as a historical record that may be utilized to improve decision-making by ensuring that choices are reviewed. Finally, it reduces the doubling down effect by highlighting where methods failed, which is connected to investing the money in the proper techniques. In this manner, we can observe which assumptions fail and can more easily choose what to do instead. Another intriguing aspect is that we may examine the tree's commonalities. For example, regardless of the sort of attacker or the varied pathways the attacker takes, two-factor authentication would most likely be on a slew of distinct protective branches. When we see it everywhere, we may begin to remove the "low-hanging fruit," raising the attacker's cost once further. Our advantage is that we understand the system and can figure out how to properly protect the various pathways and increase the security of the trees. A nice option here would be to use a red team as penetration testers. As an alternative to a traditional report, the penetration testers may be requested to create a decision tree based on their results.

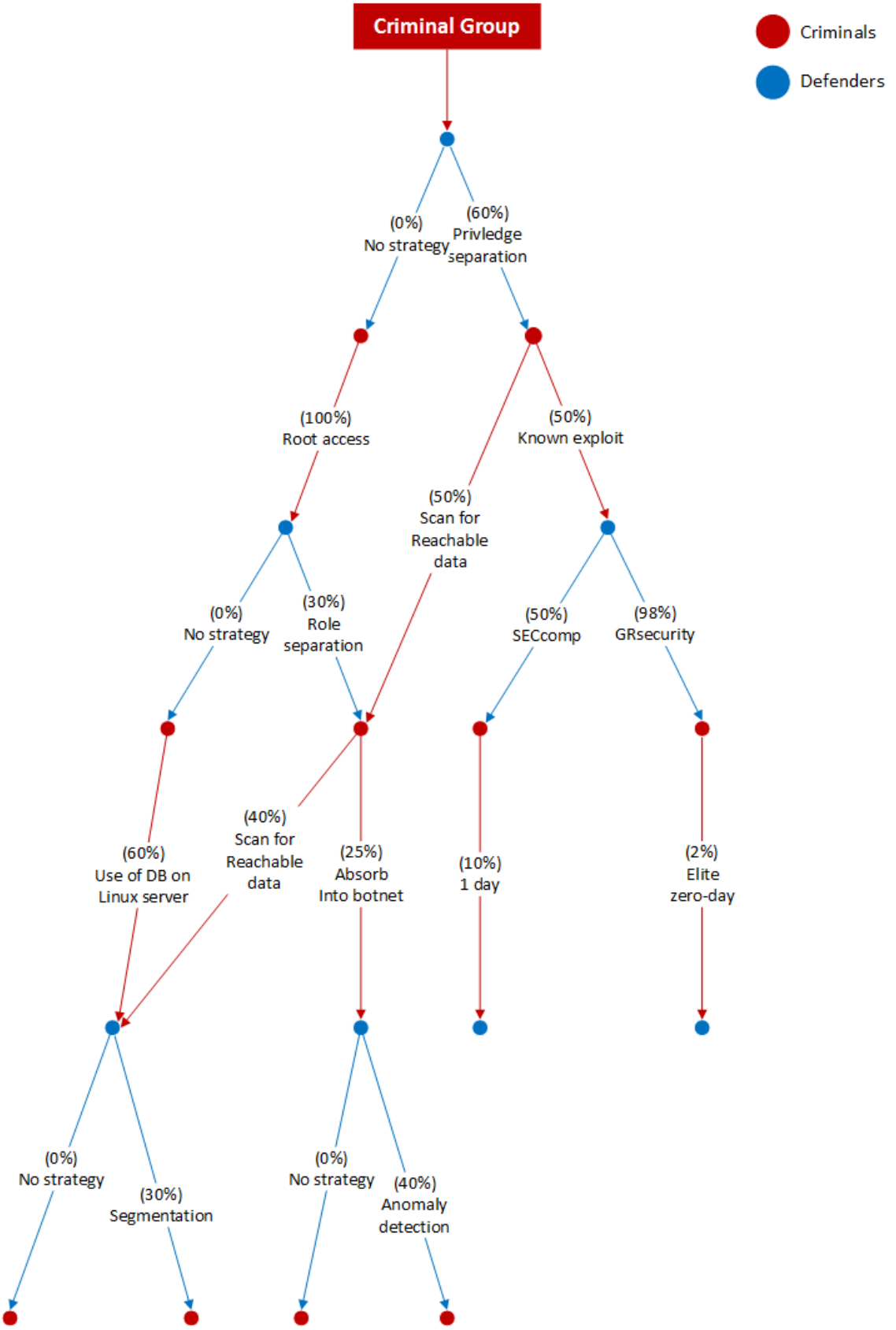

Figure 8: Decision Tree Model

Looking at the decision tree in Figure 8, we can see that interrupting the attackers during their recon phase would be quite beneficial. In general, this may be accomplished by constructing honeytokens that attempt to depict real rules or technology that might be beneficial in attacker reconnaissance. For this, we may use non-determinism, which indicates that whatever the action is, it behaves differently at various times, and one cannot anticipate the same result every time. The idea is to raise the cost of the attack at the very beginning by making the attacker unsure of the organization's defensive profile and surroundings. We want to make the attackers use their zero-day against us. For example, we might make everything in our environment appear like a malware analyst's sandbox every time, because malware frequently does not execute if it realizes or believes it is being examined. To save the cost of constructing many sandboxes, which may cost up to 1,500,000 NOK, we can employ mimicking methods that make it appear as though there are separate sandboxes each time. As a result, attackers may be persuaded to assume that the sandboxes are offered by a variety of suppliers, further confusing their understanding of what is going on. In general, this is accomplished by mixing and combining empty but suspicious-looking artifacts (of the sort malware seeks) on regular, physical computers, ideally during boot. The RocProject, which emulates virtual artifacts on real computers, is one example of a project that enables this. Custom lightweight hypervisors might also be used as an alternative. The evolution of shifting infrastructure shown in Infrastructure 3.0 may also be utilized to make it more difficult for attackers to remain persistent on systems. It also makes it more difficult for them to learn from earlier acts, especially if we use any of the above-mentioned mixing and matching tactics. Netflix's Chaos Monkey is another nice example of integrating a charging infrastructure.

This leads us to the concept of minimax/maximin, in which players choose tactics in ignorance of the other players' strategic decisions, and they choose safe moves to minimize the probable loss for a worst-case maximum loss scenario. We want to discover the minimum of the projected cost of protection plus the expected cost of not protecting. This is akin to non-determinism in that it benefits from not having a monoculture since variety is important for safety. We may lessen the concept of cascading failure or infection by diversifying our systems. Stochastic decisions may be superior to deterministic ones, as research demonstrates that random is superior to fixed and about equivalent to game theory.

However, there are certain difficulties. One of the most difficult difficulties in modeling attacker cognition using model tracking, which is the notion of imagining how attackers learn. Ideally, we'd like to be able to simulate attacker cognition. The issue is that we don't know how to effectively observe attacker cognition; honeytokens might be a good place to start because they allow us to see when and what systems attackers are exploring. Visibility is certainly a major issue. We must also take in mind the attacker's tastes, which vary with experience. In this case, we should include what is called the post-decision state, which allows us to integrate the feedback aspect from learning in attackers. As a result, we must remember that the higher the attacker's learning rate, the easier it is to forecast their decisions. This may be accomplished by the use of basic math, such as:

$$\Delta U_A = \alpha(R - U_A),$$

where U_A is the expected utility of offensive action, α is the learning rate, and R is the feedback (success/failure). For example, if the learning rate is 20%, one gets a one for a win and a negative one for a loss, then:

$$\Delta U_A = 0.2(1 - 0) = 0.2$$

This indicates the attacker is 20% more likely to repeat the activity. As a result, if we can see what actions an attacker takes, we can begin to estimate the learning rate since we can see what they do after that. From there, we may begin to forecast attacker behavior. The purpose is to keep track of the utility values associated with each attacker activity. We should be able to know what the action to result in ratio is for detected or prevented actions, which makes it easier, and then we can look at what the maximum utility factor is from there.

Bibliography

[1] Cyber Security & Infrastructure Security Agency. [n. d.] Known exploited vulnerabilities catalog. Retrieved 14th March 2022 from https://www.cisa.gov/known-exploited-vulnerabilities-catalog.

[2] Philip S. Anton, Robert H. Anderson, Richard Mesic and Michael Scheiern. 2004. *Finding and Fixing Vulnerabilities in Information Systems: The Vulnerability Assessment and Mitigation Methodology*. RAND Corporation, Santa Monica, CA. Retrieved 15th March 2022 from https://www.rand.org/pubs/monograph_reports/MR1601.html.

[3] NIST Information Technology Laboratory Computer Security Resource Center. 2022. Risk. Retrieved 25th March 2022 from https://csrc.nist.gov/glossary/term/risk.

[4] CVE. [n. d.] Cve-2021-44228. Retrieved 14th March 2022 from https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2021-44228.

[5] Team Cymru. [n. d.] Team cymru. Retrieved 14th March 2022 from https://team-cymru.com/.

[6] Cambridge Dictionary. [n. d.] Goodwill. Retrieved 2nd February 2022 from https://dictionary.cambridge.org/dictionary/english/goodwill.

[7] Cambridge Dictionary. [n. d.] Uncertainty. Retrieved 2nd February 2022 from https://dictionary.cambridge.org/dictionary/english/uncertainty.

[8] Ana Paula Henriques de Gusmão, Maisa Mendonça Silva, Thiago Poleto, Lúcio Camara e Silva and Ana Paula Cabral Seixas Costa. 2018. Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory. *International Journal of Information Management*, 43, 248–260. ISSN: 0268-4012. DOI: https://doi.org/10.1016/j.ijinfomgt.2018.08.008.

[9] Craig Hutchison. [n. d.] Cambridge analytica's values are nowhere to be found. Retrieved 4th February 2022 from https://www.linkedin.com/pulse/cambridge-analyticas-values-nowhere-found-craig-hutchison.

[10] Corporate Finance Institute. 2022. Real options - a right, but not an obligation, to make a business decision. Retrieved 25th March 2022 from https://corporatefinanceinstitute.com/resources/knowledge/valuation/real-options/.

[11] IT Governance Institute. 2000. Cobit 3rd edition control objectives, 1–155. Retrieved 21st March 2022 from http://standards.narod.ru/COBIT/control.pdf.

[12] Investopedia. 2021. Strength, weakness, opportunity, and threat (swot) analysis. (March 2021). Retrieved 29th March 2022 from https://plato.stanford.edu/entries/game-theory/.

[13] ISO/IEC. [n. d.] International standard iso/iec 27005. Retrieved 30th January 2022 from http://ce.sharif.edu/courses/95-96/2/ce746-1/resources/root/Resources/ISO-IEC%5C%2027005-2011-Risk%5C%20Management.pdf.

[14] William Johnson. 1999. Integrative taxonomy of intellectual capital: measuring the stock and flow of intellectual capital components in the firm. *International Journal of Technology Management - INT J TECHNOL MANAGE*, 18, (January 1999), 562–575. DOI: 10.1504/IJTM.1999.002788.

[15] Paul Kailiponi. 2010. Analyzing evacuation decisions using multi-attribute utility theory (maut). *Procedia Engineering*, 3, 163–174. 1st Conference on Evacuation Modeling and Management. ISSN: 1877-7058. DOI: https://doi.org/10.1016/j.proeng.2010.07.016.

[16] Stanford Encyclopedia of Philosophy. 2022. Game theory. Retrieved 28th March 2022 from https://plato.stanford.edu/entries/game-theory/.

[17] OWASP. [n. d.] Injection flaws. Retrieved 15th March 2022 from https://owasp.org/www-community/Injection_Flaws.

[18] OWASP. [n. d.] Owasp top ten. Retrieved 13th March 2022 from https://owasp.org/www-project-top-ten/.

[19] Lisa Rajbhandari and Einar Snekkenes. 2013. Using the conflicting incentives risk analysis method. In volume 405. (July 2013), 315–329. ISBN: 978-3-642-39217-7. DOI: 10.1007/978-3-642-39218-4_24.

[20] Einar Snekkenes. 2022. Interval computations of utility change, (March 2022), 6–7.

[21] Ed Yourdon. 2006. Just enough structured analysis - chapter 9: dataflow diagrams. Retrieved 20th March 2022 from http://jjakiela.prz.edu.pl/system_design/dfd.pdf.