CYBECO

Supporting Cyber-insurance from a Behavioural Choice Perspective

D4.1: Cyber-Insurance Use-Cases and Scenarios

Dissemination Level		
PU	Public	x
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Document Status

Document Title	Cyber-Insurance Use-Cases and Scenarios
Version	1.0
Work Package	4
Deliverable #	4.1
Prepared by	Kreshnik Musaraj (AXA)
Contributors	Mathieu Cousin (AXA), Victoria Melvin (AXA), Caroline Baylon (AXA), Aitor Couce (CSIC-ICMAT), David Ríos (CSIC-ICMAT), Jose Vila (DEVSTAT), Wolter Pieters (TU-DELFT), Katsiaryna Labunets (TU-DELFT)
Checked by	
Approved by	
Date	30/04/2018
Confidentiality	PU

Document Change Log

Each change or set of changes made to this document will result in an increment to the version number of the document. This change log records the process and identifies for each version number of the document the modification(s) which caused the version number to be incremented.

Change Log	Version	Date
First draft referring only to use-cases	0.1	July 17, 2017
Second draft including scenarios	0.1	October 1, 2017
Revisions	0.2	Interim
Revisions	0.3	Interim
Revisions	0.4	Interim
Revisions	0.5	Interim
Revisions	0.6	Interim
Revisions	0.7	February 08, 2018
Revisions, including incorporating feedback from project partners	1.0	April 30, 2018

Table of Contents

List of Figures

Part I:
Definition of the cyber-insurance use cases

Abstract:

In order to assess the risk calculation methodology and toolbox, and also to make it possible to incorporate the behavioural components into this methodology, it is necessary to understand the interactions between the parties in the cyber-insurance process through a set of use cases that are sufficiently representative of the global cyber-insurance ecosystem. The use cases presented in this documented are based on the analysis of the value chain for a given company, and the associated assets, and provide the basis for more in-depth cyber-insurance scenarios in this workpackage.

1 Introduction

1.1 Objective and Scope

This section describes the cyber-insurance process and also presents a set of use cases that are representative of some of the most common cyber-insurance incident scenarios. The reader will gain a clear understanding of how the cyber-insurance process operates -- including the underwriting of contracts and processing of claims -- while the use cases illustrate the types of issues arising from cyber-incidents which can be addressed by cyber-insurance.

The use cases are obtained through business and advisory expertise from both the insurance and cybersecurity industries, which are combined into a seamless view of the cyber-insurance lifecycle. The cyber-insurance processes and the use cases were completed with information exchanged with AXA operating companies[1] which conduct activities in the cyber-insurance business through their own internal projects and in their contractual client-based activities, as well as with external 3rd party companies which participated in the audit and scope assessment for existing clients in the context of insurance claims.

1.2 Chapter Structure

This section, Section 1, provides a document overview and key terms. Section 2 describes the approach and analysis on which are based the semantic components of the processes and use cases. In Section 3, the first part describes the cyber-insurance process -- the underwriting process, how companies select cyber-insurance products, and the claims processes. The second part of Section 3 presents the use cases for cyber-incidents resulting in insurance claims. Finally, Section 4 draws the conclusions, and sets the path to the following contributions in the cyber-risk use cases and scenarios.

[1] The main AXA operating companies involved in the cyber-insurance exchange of information are AXA Global Property & Casualty and AXA Corporate Solutions.

1.3 Terminology

The following table provides the definitions of terms and concepts used throughout the document.

Value chain	The process by which businesses receive raw materials, add value to the raw materials through various processes to create a finished product, and then sell that end product to customers. The value chain disaggregates an industry into its strategically relevant processes to understand the activities that produce goods and services[2].
Threat actor	An agent which either perpetrates a cyber-attack or sponsors it by providing funding, technical support, etc.
Market segment	Defined in this document by the size of the company; this should not be confused with the more general definition based on the client segmentation of the market
Market sectors	The classification of companies according to of the set of activities they are involved in; they can be grouped into distinguishable industries or groups of similar industries Market sectors can be defined according to specific needs, and can also use standard classifications of industries such as the Global Industry Classification Standard[3].

[2] Competitive Advantage: Creating and Sustaining Superior Performance, *Michael E. Porter*, Ed. Simon and Schuster, *New York*, 1985

[3] Global Industry Classification Standard, Available at: *https://www.msci.com/documents/10199/242721/MSCI_Global_Industry_Classification_Standard.pdf/88181a98-5eff-4ac7-8409-d30474fc6429*

2 Approach and Analysis

The use cases presented in this documented are based on the analysis of the value-chain[4] for a given company, and the associated assets. These two components are illustrated below in Figure 1. The table provides a correlation between the assets and each step in the value-chain. The steps of the value chain with greatest creation of data and products are given a higher importance given their impact following a cyber-incident. An asset type can be found in several steps of the value chain. This does not mean that we are considering the same exact asset at each step, but only that the asset type is recurrent[5]. The cyber-risk use cases and scenarios are heavily impacted by such assets, as they are mandatory for the quantification of the cyber-incident financial impact. Hence the approach for deriving use cases, and at a later stage risk scenarios, is based on focusing on the assets of the value chain that are impacted during a cyber-incident, since the claim compensation will be proportional to the value of such assets[6].

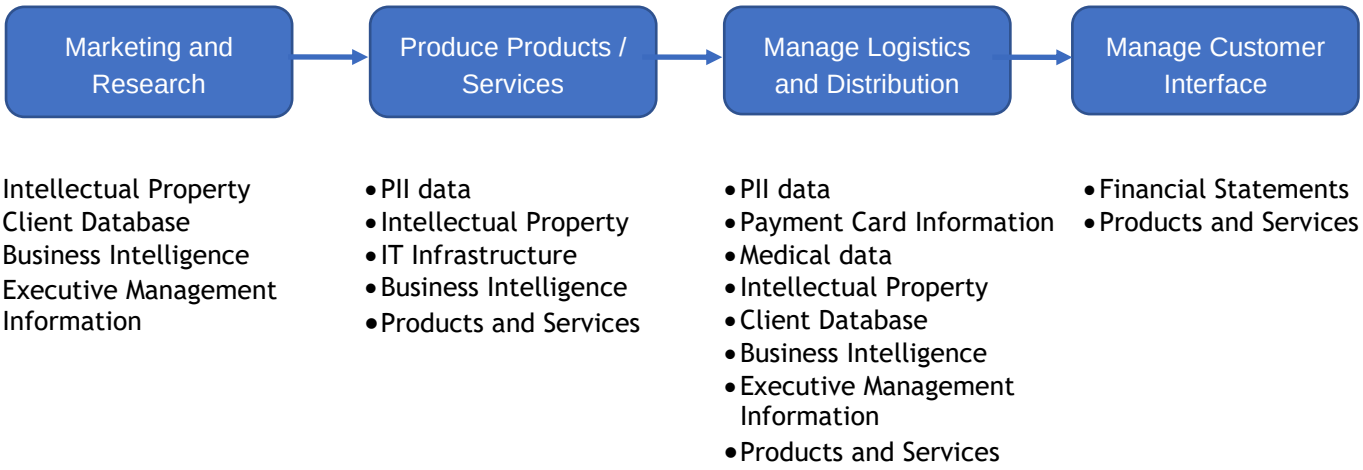

Figure 1: Impacted assets of the value-chain from a cyber-insurance perspective

The value chain provides the common ground for the use cases described in this document, and enables their interpretation in the larger framework of products and services delivered by a company, as well as in terms of impacted assets. In other words, to assess the impact

[4] The concept of value chain was first introduced by Michael E. Porter in 1985.

[5] As an example, it follows common sense that several and different intellectual property assets, such as patents or manufacturing processes, can be used for Marketing and Research which produces or uses intellectual property, Produce Products / Services for the production and service delivery step, and Manage Logistics and Distribution for separately ensuring yet another activity. Each of these intellectual property assets can be impacted separately during a cyber-incident.

[6] The quantification of the underlying assets in the value chain for a given company, and the quantification of the insurance premium corresponding to the insurance of specific cyber-risks are beyond the scope of this document.

of a use case, and more specifically a risk scenario, it is useful to place a cyber-incident in the activities which allow a company to deliver its products and/or services. A cyber-incident, caused by a given attacker with specific motivations, and disrupting a given step in the value chain, would impact specific assets. For a company seeking a specific insurance solution, it is therefore useful to be able to select the insurance product which best fits its own value. The value chain approach is very generic and can apply to all forms of companies, and the impacted assets corresponding to each step are related to what is considered as being the most important assets from the cyber-attack viewpoint. The set of assets, as well as their granularity, are defined through an analysis of the market sectors, and other specific parameters of the company under scrutiny.

There are three main groups of actors: the threat actors, the insured companies, and the companies in the insurance ecosystem. The threat actors considered in this document are the following:

- Hacktivists: A person or group of persons conducting cyber-attacks for ideological, social, or political motivations.
- Insiders: Individuals that conduct cyber-attacks targeting the organization or entity to which they belong or employs them.
- Organised Crime: Includes cyber-criminals which operate within the framework of an organized crime entity, identified as such by the corresponding legal definitions.
- Nation States: the central set of governmental-supported cyber-attackers, which operate either directly through specifically designed teams, or through indirect actions using other threat actors.
- Competitors: Organizations which engage in cyber-attacks motivated by competitive reasons w.r.t the targeted organizations or companies.
- Terrorists: A person or set of persons engaging in cyber-criminal activities either for the account of terrorist organizations, or simply for terror-inducing purposes.

A threat actor can belong simultaneously to multiple groups; however, for clarity we will maintain the separation between these groups. For example, we will maintain the distinction between a Nation State threat actor and an Insider one, even if the insider hacker can work for the Nation State threat actor which provides sponsorship and/or support for a given cyber-attack.

The insured companies are divided into market segments and market sectors. In this document, market segments are divided into three main categories:

- SME: Any company with a staff headcount not beyond 250 persons, and a turnover not exceeding € 50 million, falls into this category.[7]

- Middle market: Although the limits defining a middle market company vary[8], it is commonly accepted that this category includes companies beyond the limits of an SME, and a staff headcount below 2000 persons, and a turnover not exceeding € 500 million.

- Large companies: This category will be defined by companies exceeding the maximal limits of a middle market company, therefore having a staff headcount beyond 2000 persons, and a turnover exceeding € 500 million.

Insurance companies are not divided into rigid categories, but we can divide them into two different types, based on their role in the market:

- Insurance companies: this type includes companies which provide financial compensation in case of different types of loss, damage, or any other event considered as negative by the insured client, in exchange of premium payments. Companies that provide insurance do not only include "pure players" but also banks, stock brokers, and many other institutions in the financial services sector.

- Reinsurance companies: this particular type of insurance companies is used to transfer – i.e. distribute - large risks exceeding the insurance company's capability of coverage. For example, in case the premiums which are collected from a high-risk client are insufficient to cover a loss that occurs too early, this may lead to the incapacity of the insurance company to compensate the loss. Hence, in order to avoid defaulting on the insurance contract, the insurance company reinsures this high risk with a separate contract established between the insurance and reinsurance company. It should be noted however that insurance companies may act as reinsurers for other insurance companies, despite the existence of more "reinsurance-oriented" companies.

Finally, we mention a separate type of company which fits in neither the two aforementioned types: the 3rd party expert companies. This includes companies which are not directly involved in the insurance business, but are tightly linked to insurance companies, since they are often mandated to provide independent and objective assessments in two crucial steps of the insurance process: (i) the scope and audit assessment of the insurance coverage and the risk level posed by a potential prospect, and (ii) the expert audit after the occurrence of an incident followed by a claim, in order

[7] What is an SME?, European Commission, Available at: *http://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_fr*

[8] Middle market companies, Available at: http://www.investopedia.com/terms/m/middle-market-firms.asp

to assess the circumstances of the incident, and consequently the validity of the claim. Based on such an expert audit, the insurance company decides to compensate or not a claim from its client.

3 The cyber-insurance process and use cases

The main global insurers have cautiously started their introduction in the cyber-insurance market, this caution being motivated by the lack of actuarial data available which is required to assess the likelihood of events to be insured, as well as the ever-evolving landscape of technology behind cyber-attacks. Insurance companies have been recently proposing capped cyber-insurance policies which feature exclusion cases such as damages resulting from data stored and/or processed by an external 3rd party. This section includes an overview of the current processes behind cyber-insurance, and is composed of two parts. First, we describe the mechanisms behind the cyber-insurance process, before and after a cyber-incident leading to an insurance claim, in order to provide a clear view of the interactions between the parties described in the previous section. Next, we detail the use cases that will be used in the CYBECO project in order to validate the risk model and the toolbox. These use cases will later be refined with the behavioural dimension, and detailed in the risk scenarios.

3.1 The cyber-insurance process

3.1.1 Establishing a cyber-insurance contract

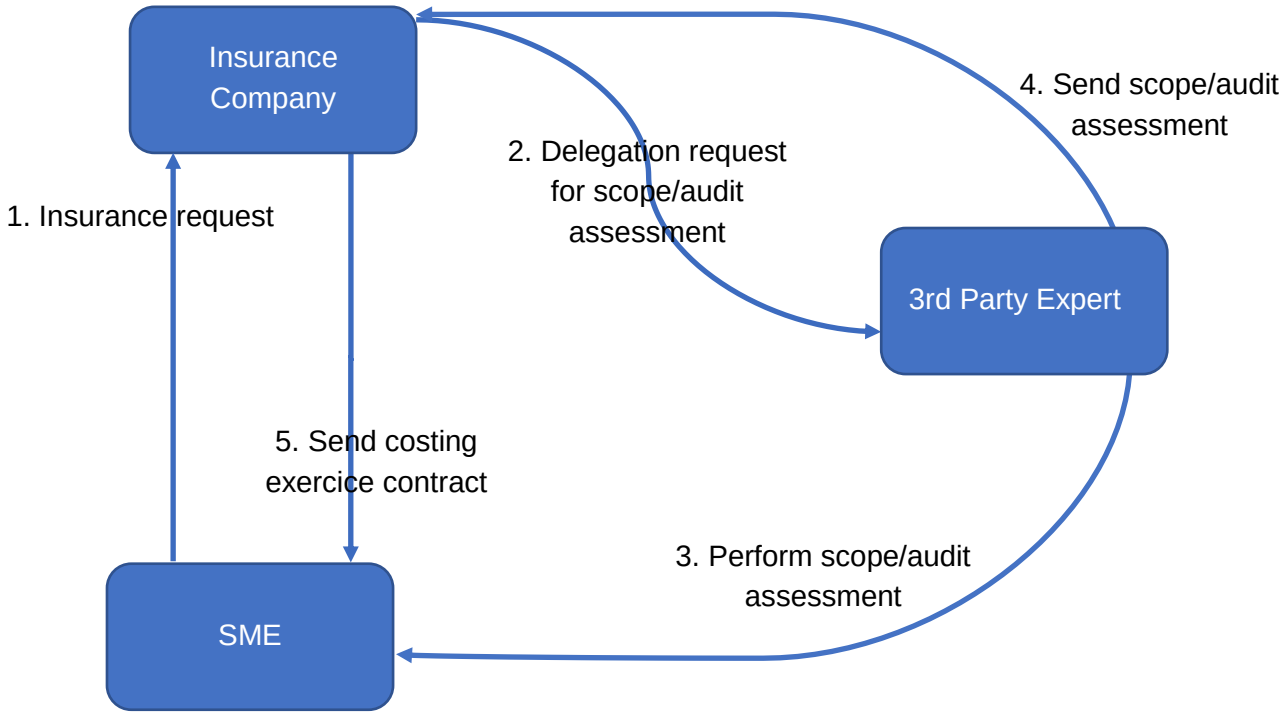

Figure 2: Cyber-insurance process for the SME market segment

The process for establishing a cyber-insurance contract differs slightly depending on the size of the company that wants to be insured. In the case of an SME, once it has made a request for cyber-insurance, the insurance company sends a delegation request to a 3rd party expert

company. The 3rd party expert company will assess the scope of the insured perimeter, and will also assess the cyber risk level of the company requesting insurance. Once the scope and the assessment are carried out, the 3rd party expert company sends the assessment to the insurance company. This assessment allows the insurance company to quantify the company's cyber risk and thus determine an appropriate premium. It then establishes and sends a contract to the SME. The process is illustrated in Figure 2.

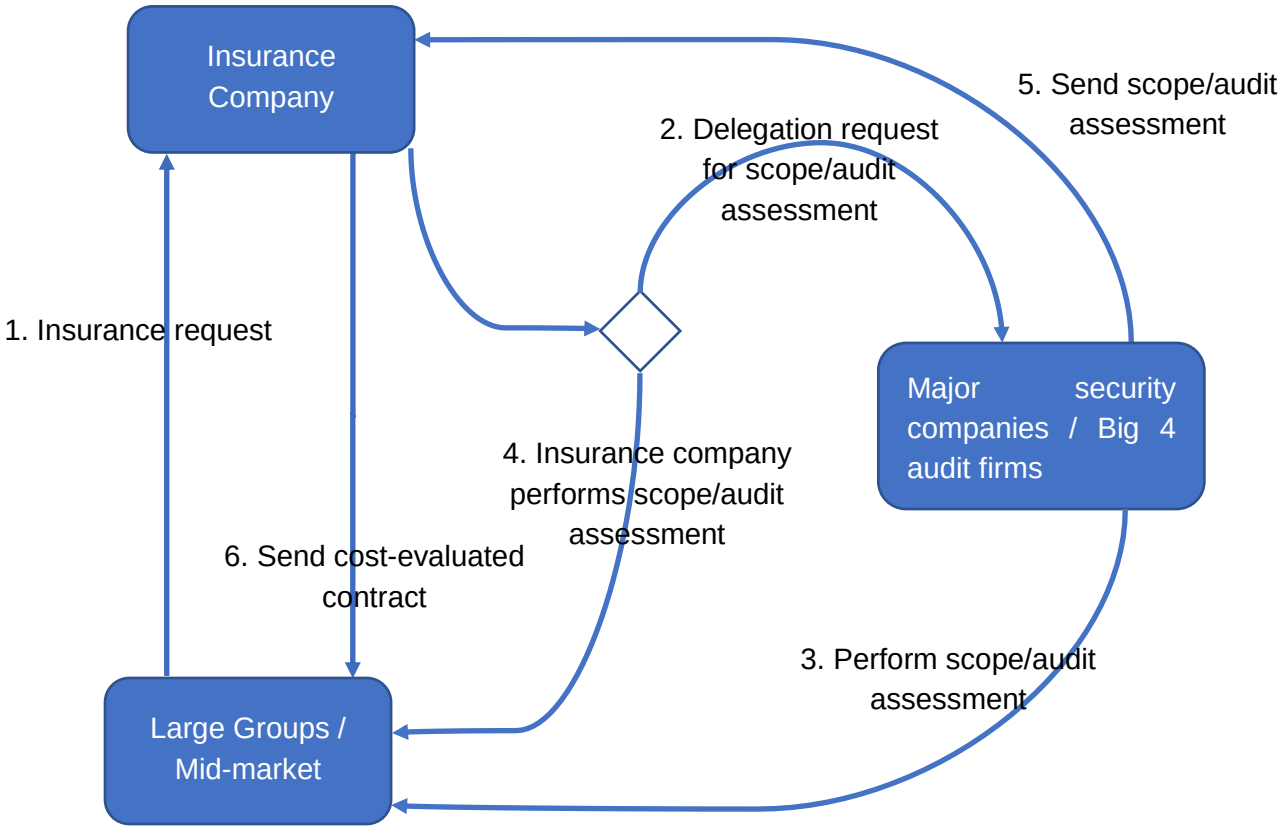

Figure 3: Cyber-insurance process for large groups and mid-market market segments

In the case of large and mid-market companies that need insurance, the process is slightly more complex. After receiving a request from a potential client, the insurance company can choose to either perform the scope and audit assessment itself, using its own internal expertise, or to delegate it to 3rd party security companies or audit firms. The quantification of cyber-risk for large and mid-market companies is a very complex process, so it requires a much more detailed scoping and assessment than for SMEs. Again, once the scope and audit assessment are completed, a cost-evaluated contract is sent to the client company. This process is illustrated in Figure 3.

Whether an insurance company decides to use internal resources to carry out a scope and audit assessment or delegate it to a 3rd party depends on such factors such as business requirements and contractual agreements. Examples include insufficient internal resources

to conduct the scope and audit assessment, large scale global operations requiring the involvement of local external teams in several countries, or regulatory restrictions.

3.1.2 Processing a cyber-insurance claim

The procedure for processing a claim following a cyber-incident also varies slightly depending on a number of factors. After the insured company files a claim, the insurance company sends an audit request to a 3rd party expert company. The 3rd party expert company will either perform the incident audit with its own internal resources or it will delegate the audit to one or several contractors who are auditors, depending on the size of the insured company, the scope of the insurance contract, and the complexity of the cyber-incident. An incident audit report providing expert insights on the incident, damage caused, and forensic evidence is compiled and sent to the insurance company[9]. Based on the elements contained in the report, the insurance company decides to either accept the claim or refuse it if there is no contractual legal ground for it. This process is illustrated in Figure 4.

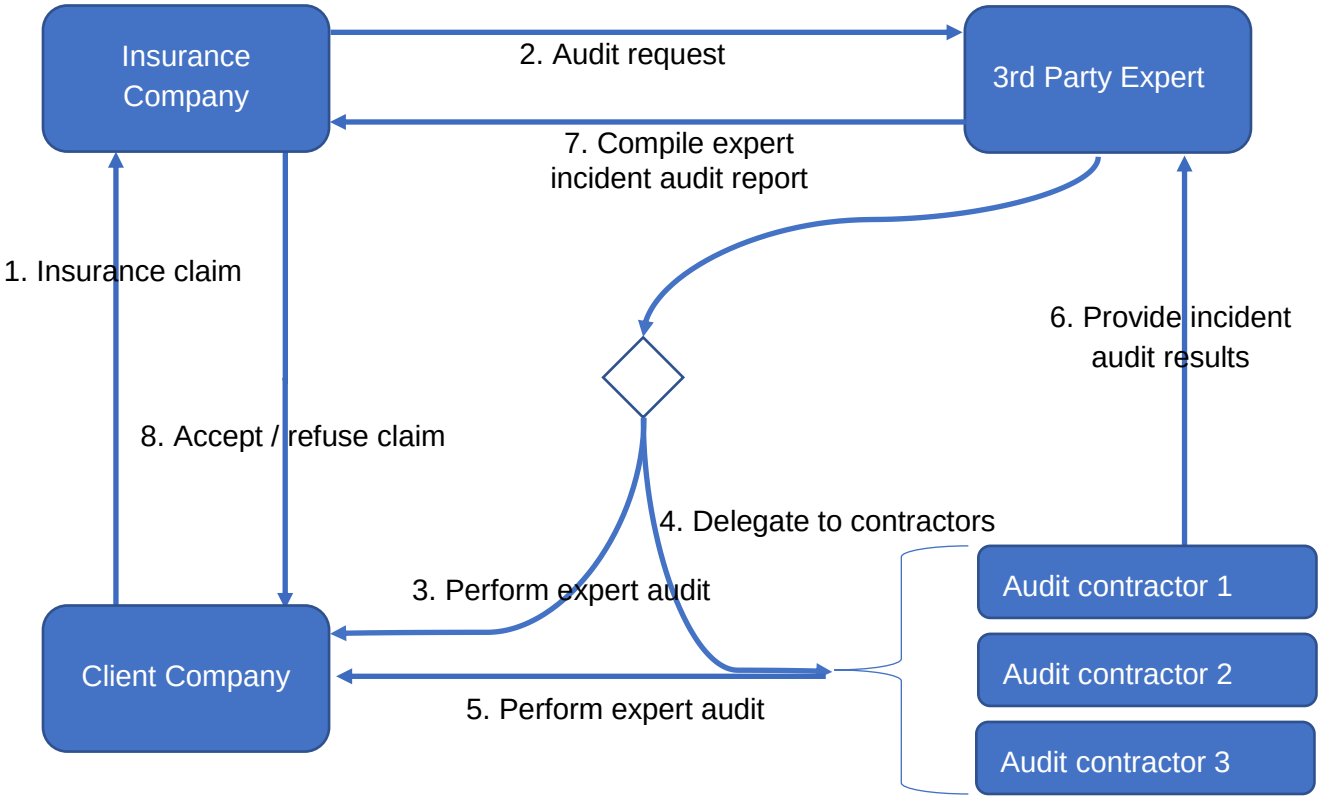

Figure 4: Cyber-insurance claim process for all market segments

[9] The audit report contains information including, but not limited to, implemented security measures, activity logs, traces of the cyber-attack, sequence of events before, during, and after the attack, etc.

3.2 Cyber-insurance use cases

The use cases presented in this document allow to simultaneously cover for several parameters. These parameters include the size of the company, the market sector, the parties involved in a use case, and the main expected outcome of the cyber-attack in a given use case. In this set of use cases, the company size includes both large companies and SMEs. market sectors, they are the IT and heavy manufacturing sectors. The three parties in a use case are the attacker, the insurance company, and the insured client. On some occasions[10], several of these parties may be standing for the same entity, as one of the use cases will show. Finally, the expected outcome of the use cases is composed of the following: "Data loss" and "Products / Services manipulation", as two cases of asset impact, insurance fraud, and insufficient insurance coverage.

We note that the number of use cases provided in this document is motivated by the necessity to cover for the main types of risks for an insured company, but also for the risk to which an insurance company is exposed.

- **Use case 1: Cyber-insurance selection process for an SME**

Overview: For a decision-maker in an SME (e.g. the company CEO), the choice of a cyber-insurance product depends on a number of considerations. This use case describes the selection process of a cyber-insurance product from an SME willing to cover from specific cyber-related risks, and how the SME will decide about the best price/coverage ratio amongst the options offered by the insurance company. The perspective of the selection process is that of the decision-maker in the SME, i.e. the company CEO.

(It is important to note that, given the relatively small size of an SME, the following explanation of how it chooses a cyber-insurance product assumes an underwriting process and insurance coverage that is much less complex than that for insuring a large corporation. This allows the insurance company to make use of a simplified mechanism for the evaluation of the risk.)

Description: An insurance company offers a set of cyber-insurance products based on the main risks posed to an SME as well as the impact that a cyber-attack might have. These products provide increasing levels of coverage along the following lines:

- Insurance Product 1: This covers the risk of internal data loss – including loss of competitive advantage following the loss of client databases, intellectual property, business intelligence, and strategic executive management information.

[10] With respect to use case 3, when the cyber-attack is conducted by insiders, then the insured company and the attacker are the same entity.

- Insurance Product 2: This covers the risks covered by Insurance Product 1 as well as a number of additional risks: brand damage following an information security breach, which includes but is not limited to the loss of private customer data, investor divestment, or a decline in the company's investment rating following a spate of negative media coverage.

- Insurance Product 3: This covers the risks covered by Insurance Product 2 as well as a number of additional risks: failure to deliver products and services / non-fulfilment of service and contractual agreements with respect to 3rd parties and the ensuing impact on the assets and business continuity of these 3rd parties.

A prospect SME is considering to buy one of the proposed cyber-insurance products. When deciding which cyber-insurance product to buy, an SME considers at least two major factors and alongside a third optional factor which may appear in the future:

- The first major factor is the criticality of certain underlying assets. If compromising a certain asset in the value chain could threaten the SME's solvency, then it is essential to insure against that risk.

- The second major factor is the benefit to cost ratio: Would the benefit of being insured against a risk be larger than the cost of paying the premiums? Or is it financially more profitable for a company to cover the damage from a cyber-attack itself, with no insurance to compensate it?

- The third optional factor concerns the regulatory and other legal obligations which the SME may be subject to. Although at present companies are not required to have cyber insurance, this could change in the near future: Like for car insurance, in which all car owners are required by law to be insured against damage caused to 3rd parties, governments may increasingly require the same for cyber-attacks.

If the SME is subject to regulatory or legal obligations, then the SME will begin the cyber-insurance selection process by considering which product's features will enable it to meet its legal requirements. If the SME is not subject to such obligations, then the SME will begin by analysing its value-chain, then classifying its associated assets. Next, it will assess the counter-measures and remediation processes that are in place for protecting its important assets[11]. This is followed by an impact analysis of the effect that a cyber-attack on these assets would have in terms of business interruption and the value chain. If the consequences are deemed to be endanger the solvency of the company, the SME will select the insurance product offering optimal coverage for these assets.

[11] Although the SME probably does not have as precise information as insurance companies on the probability of a given risk, it is likely to have information on its cybersecurity maturity posture from auditing and reviews conducted by external firms. The likelihood of a cyber-risk can be obtained through several methods, including collecting threat information from cybersecurity companies and audit firms which have collections of such data.

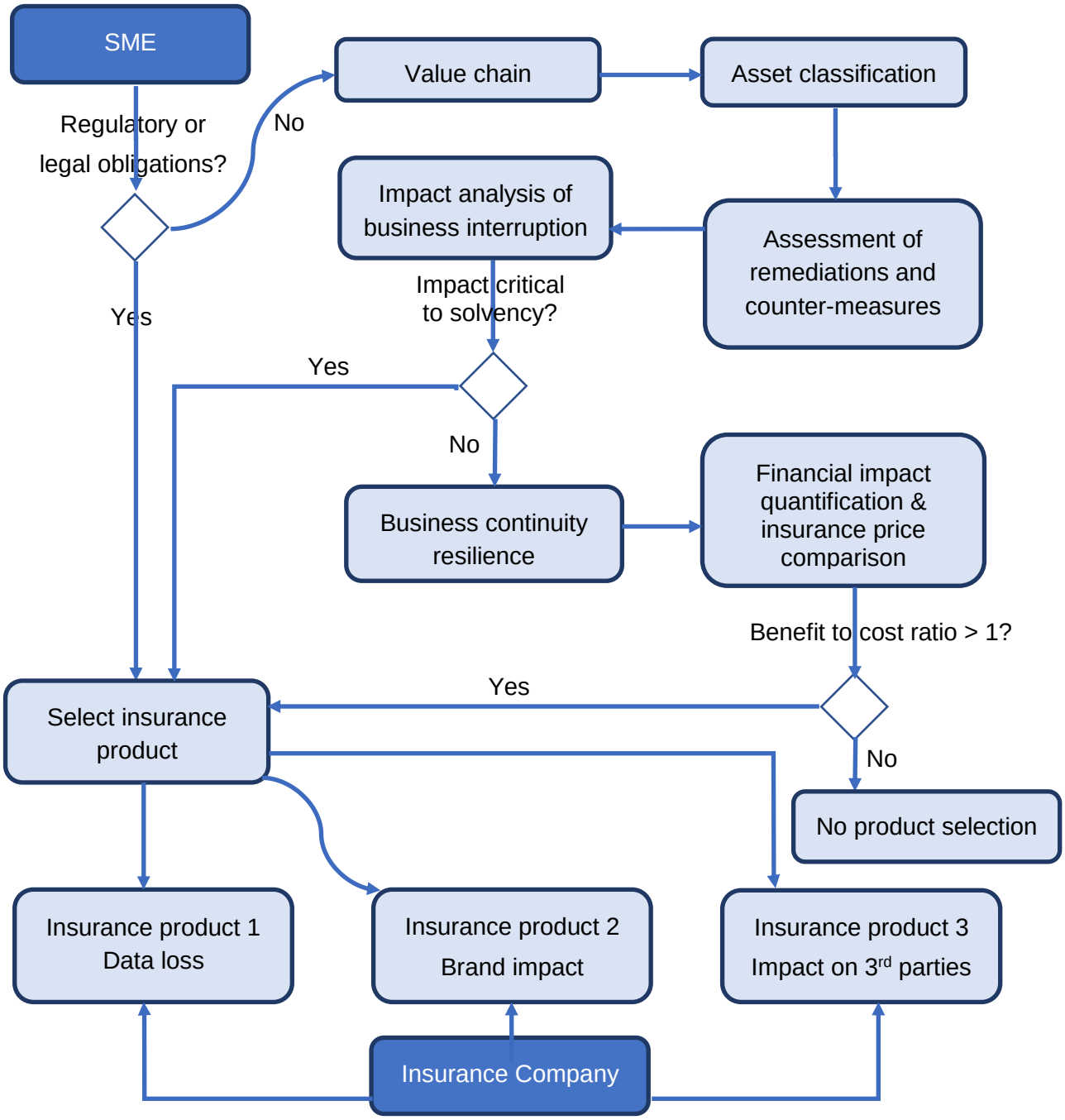

Figure 5: Cyber-insurance product selection use case

If the consequences are not thought to be as critical to the business, then the SME will carry out a business continuity resilience evaluation aimed at minimizing the overall damage caused by the cyber-attack. It will also carry out a financial impact quantification / cyber-insurance price comparison, which consists of simulating the financial cost of a cyber-attack following specific high-risk scenarios and then calculating a ratio of the cost of premiums for each cyber-insurance product versus the financial compensation such an insurance provides.

If the ratio is greater than 1 (i.e. if the benefit of the cyber-insurance coverage exceeds the cost of the cyber-insurance premium), then the SME will likely choose that cyber-insurance product. If not, given that: (i) the cost of the cyber-insurance product would exceed the benefit of financial compensation in case of a cyber-attack, (ii) the SME would not suffer disastrous interruptions from such a cyber-attack, and (iii) the SME is not subject to either regulatory or legal obligations, then it is likely that the SME would not select any of the proposed cyber-insurance products.

These factors in the cyber-insurance selection process are illustrated in Figure 5.

Use case 2: Loss of personally identifiable data for a large company in the financial sector

Overview: This use case addresses the risk of the loss of personally identifiable data for a large company, resulting in a number of negative impacts for the company such as brand damage, loss of competitive advantage, regulatory fines, etc.

The cyber-insurance product in this case would cover the financial impact following such an attack. It is important to note, however, that in this use case regulatory fines are not considered part of the insured liabilities, since it is not standard business practice to do so and in some countries (e.g. France) it is not legally permitted to insure against regulatory fines in such instances.

Description: Hackers in the organized crime category exploit known vulnerabilities on a company server that is exposed on the internet. After a lengthy period of trying various techniques to gain access, the attackers succeed in installing a “command and control” component that can send commands and receive output as well as in identifying personally identifiable user data (PII). Over an extended period of time, the attackers exfiltrate PII data in small components in order to avoid triggering data loss protection measures. This use case is illustrated in Figure 6.

Although this particular example involves the financial sector, this type of attack is an opportunistic attack that does not specifically target financial companies; rather, these hackers use automated scanning tools to search the internet for companies that are vulnerable. Therefore, it involves random attacks targeting any market sector.

This use case has a number of impacts which will be analysed in detail in the cyber-risk scenarios, which will be presented in a follow-on paper. Also, to consider 3rd party impact following data loss for such a company, but this case is illustrated in use case 5.

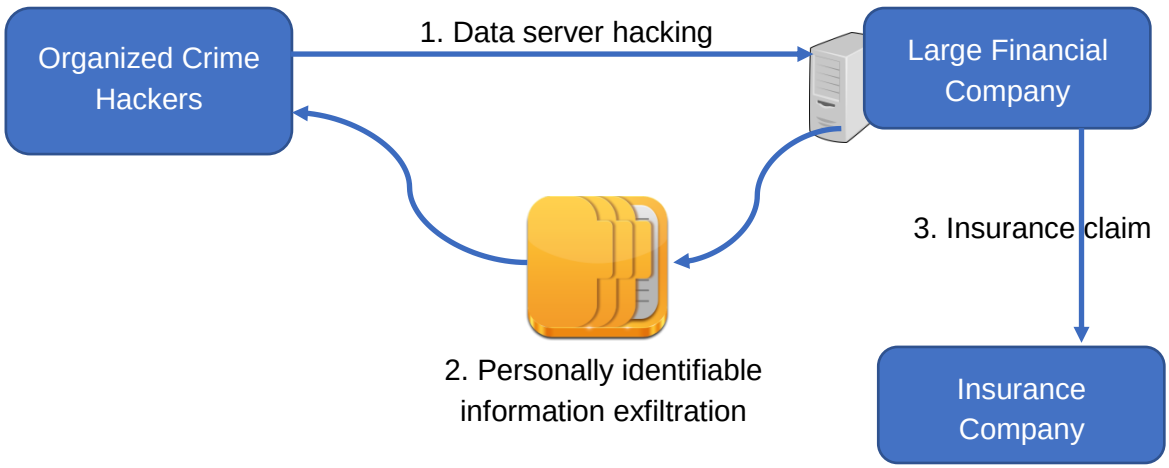

Figure 6: Personally identifiable data loss use case

Use case 3: Insurance fraud for an SME in the professional services sector

Overview: This use case illustrates the risk that an insured company might attack itself intentionally in order to collect an insurance payout.

Description: An SME operating in the professional services sector takes advantage of a widespread ransomware attack campaign in order to commit insurance fraud.

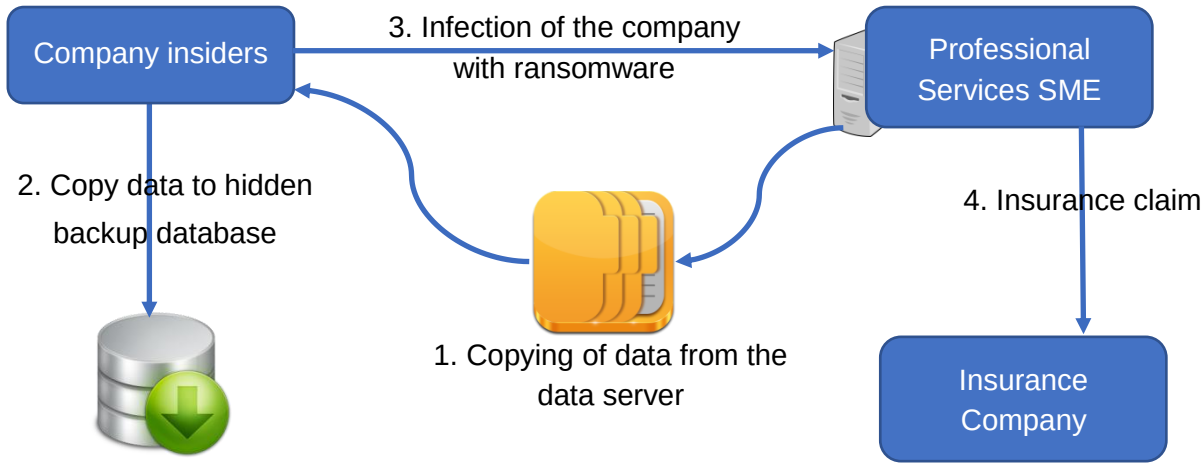

Figure 7: Insurance-fraud use case

The company instructs several employees to secretly make a full backup of the company data, while at the same time intentionally infecting the company's servers with

ransomware[12]. It then files an insurance claim for the loss of critical business data, although it actually still has this data in a secret location. This use case is illustrated in Figure 7.

Use case 4: Products / Services Manipulation for a large company in the manufacturing sector

Overview: This use case addresses the risk of highly skilled attackers targeting large companies involved in manufacturing. This type of attack involves manipulation of products or related services[13], compromising the entire production line.

The cyber-insurance product in the case would cover the financial loss following such a manipulation. This case is addressed by insurance companies through specifically tailored insurance contracts as the potential value of loss is often very large.

Description: Hackers working for competitors are able to access the servers of an airplane manufacturing company which contain the instructions for the production of crucial engine parts in the automated production line.

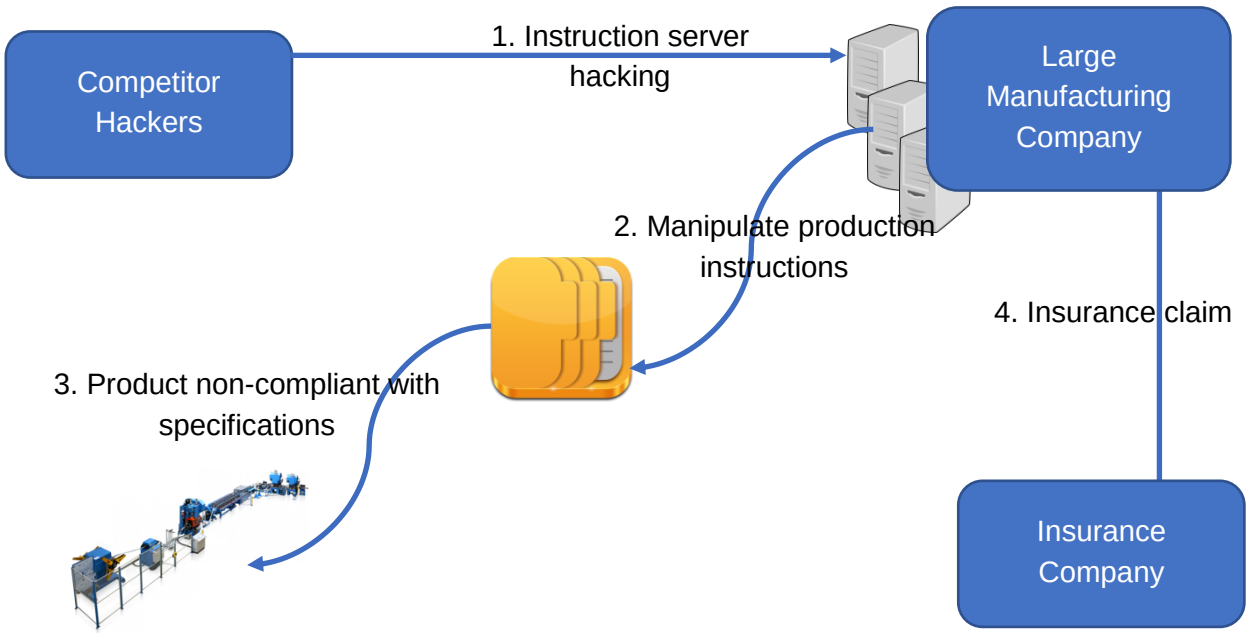

Figure 8: Products and services manipulation use case

[12] I.e. software that encrypts all the data located on hard drives and allows its decryption only against the payment of a ransom.

[13] An example of such services can be product prototype designs, feasibility reports, etc.

Instead of deleting the data, the attackers make small manipulations to the technical production specifications so that the produced parts will not correspond to the required specifications. An illustration of this use case is provided in Figure 8.

Use case 5: Insufficient insurance coverage for an SME operating in the IT industry sector

Overview: This use case accounts for the risk for an SME of insufficient cyber-insurance coverage, in the event that a cyber-attack on an SME has a significant impact to 3rd party companies relying on the SME's products or services.

Description: During a large DDoS (Distributed Denial of Service) attack by a nation state attacker, an SME that provides DNS (domain name system) services for a number of major companies is unable to do so. As a result, the internet platforms and services of its 3rd party clients are unavailable[14]. This business interruption caused to 3rd party companies has an additional financial impact that surpasses the initial estimation.

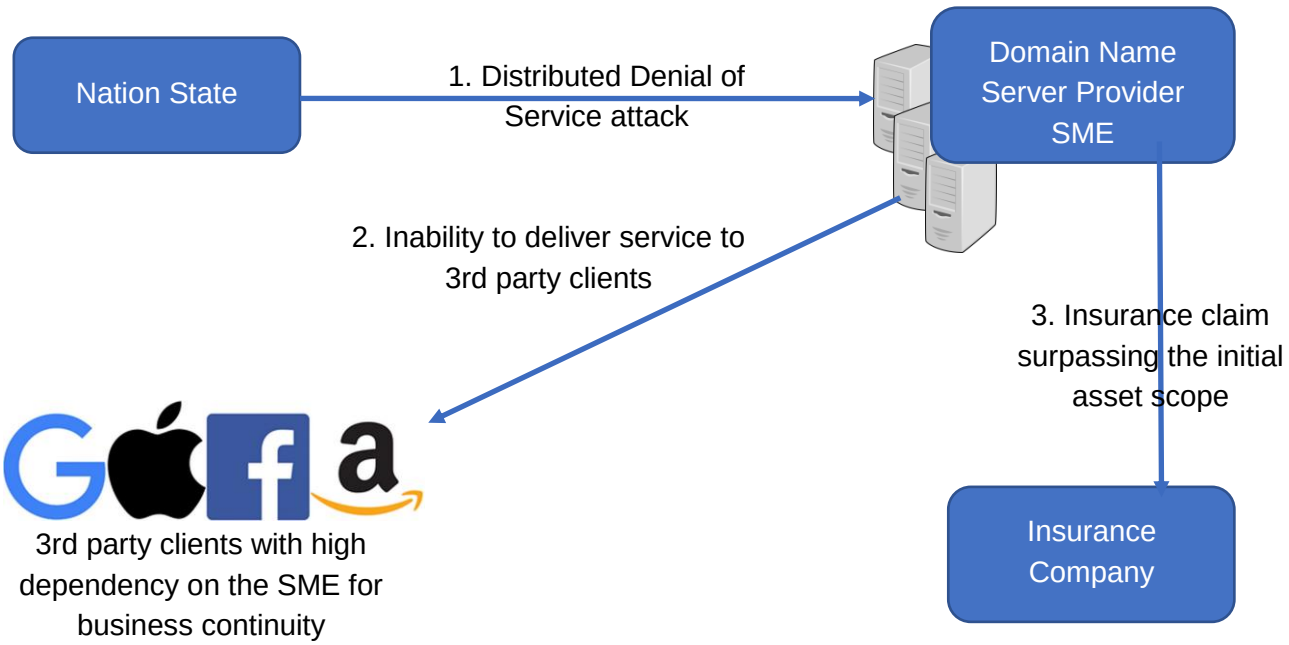

Figure 9: Insufficient insurance coverage use case

[14] A DNS provider provides mapping services to convert a numeric IP (internet protocol) address into an alphanumeric one (e.g. www.google.com) that people can remember; when this system fails, the internet sites are therefore inaccessible.

From the perspective of the insurance company, this use case can be addressed through the application of a maximum cap for claims related to cyber-incidents. However, for the insured company, it is important that it conduct a correct assessment of the financial impact of a cyber-incident on its entire value chain – including **3rd party companies** – if it is to put an effective strategy in place. This use case is shown in Figure 9.

Use case 6: Accumulation of cyber-incidents following a single large-scale attack with involvement of reinsurance in the claim process

Overview: This use case addresses the risk of a targeted or random large-scale attack from highly skilled attackers (for example, nation states or organized crime groups) that has major repercussions on a wide range of market segments and market sectors. It illustrates an accumulation scenario in which a single initiative results in numerous cyber-incidents, heavily impacting a number of insurance companies. Typically, these insurance companies have partially transferred the risk to one or several reinsurance companies.

Description: A threat actor of the organized crime or nation state type launches a malware campaign through non-discriminating techniques (e.g. phishing, infected email attachments, or vulnerability exploits) to compromise large numbers of hosts and servers with ransomware. The non-targeted nature of the campaign combined with a high number of vulnerabilities and unpatched software and operating systems means that the attack results in data loss (encrypted by ransomware[15]) for a large number of companies in many market sectors and market segments.

Moreover, the attack also impacts companies providing telecommunications and cloud services, thereby interrupting communication channels and thus affecting the business continuity of other companies as well. This adds to the accumulation effects of such an attack.

For all of these companies, the loss of critical data impacts business continuity and hence causes financial loss (despite remediation mechanisms such as backed up data, crisis management, and redundancy). Each company therefore addresses a claim to its respective insurance company.

Because many market segments and sectors are impacted, the attack results in claims for large portions of an insurance company's portfolio. However, insurance companies often rely on reinsurance companies to transfer part of the portfolio risk, so that risk can be lowered to acceptable levels. The use case is shown in Figure 10.

[15] I.e. software that encrypts all the data located on hard drives and allows its decryption only against the payment of a ransom.

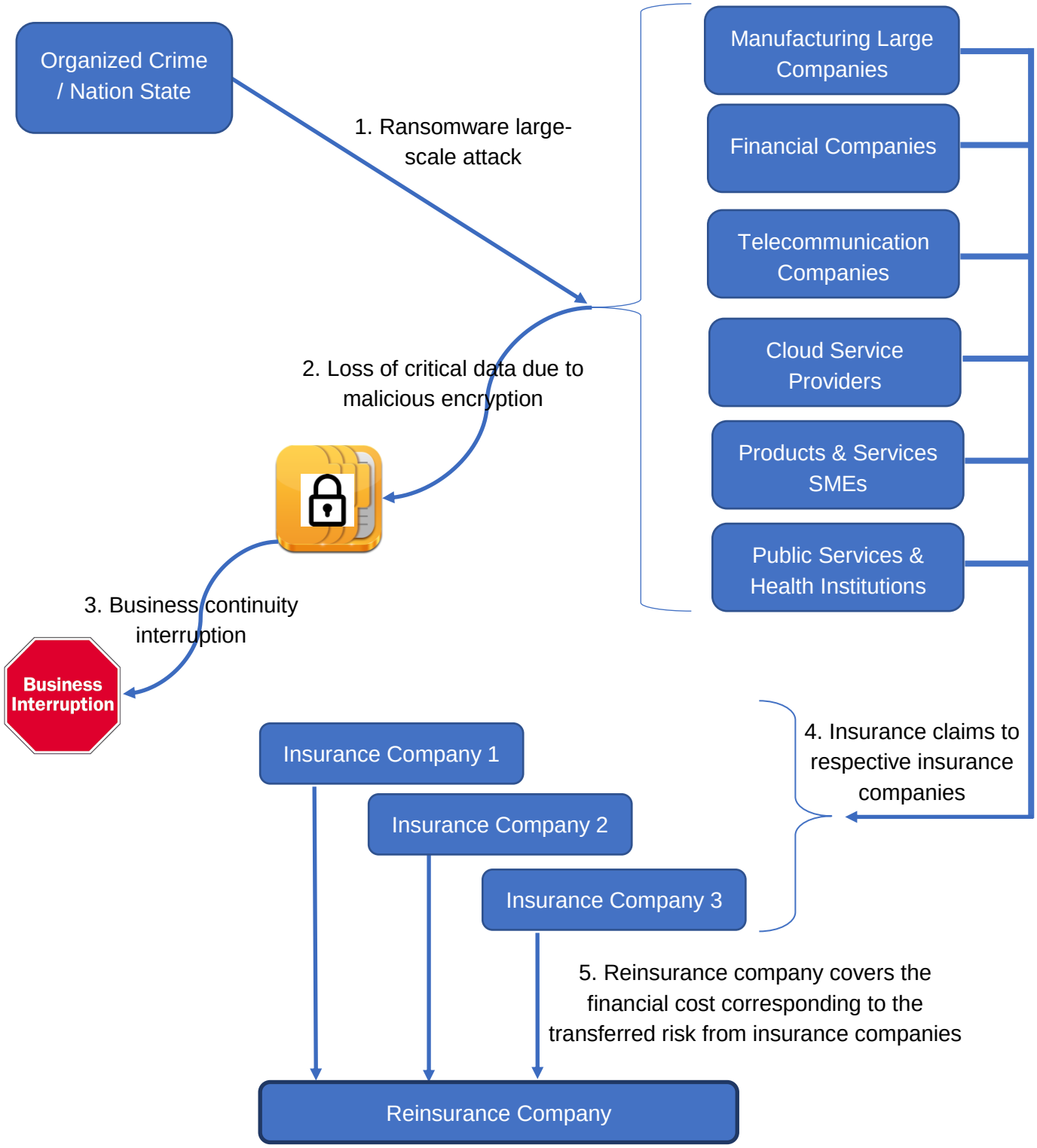

Figure 10: Illustration of the random large-scale use case with reinsurance involvement

4 Conclusion

The use cases provided in this document cover some of the most generic risk scenarios, types of companies, and actors involved in the cyber-insurance process. Although the true level of detail of such real-world use cases and the associated scenarios is much higher, it is necessary for underwriting purposes to keep such complexity to a level that allows the understanding of risks posed by each use case to the inherent company assets, as well as to the insurance company. The behavioural component in these use cases and the future scenarios will be represented by the motivation behind the actions of each actor, as well as other parameters proposed during the ongoing research. The scenarios that will be based on these use cases will push further the analysis based on the value-chain.

It is useful to note that the provided use cases are of interest to both viewpoints in the insurance process (i.e. the insurance and the insured company), and more importantly so for the insured company, since they allow for an organization to identify its activities with the risk examples provided in one of the use cases, even if such use cases are far from exhaustive. Therefore, they can be used to account for such risks, and foresee not only the needs for specific insurance coverage, but also for adequate remediation measures to reduce such risks.

Part II:
Definition of the cyber-insurance scenarios

Abstract:

In order to assess the risk calculation methodology and toolbox, and also to make it possible to incorporate the behavioural components into this methodology, it is necessary to understand the interactions between the parties in the cyber-insurance process through a set of detailed scenarios based on previously defined use cases that are sufficiently representative of the global cyber-insurance ecosystem. The scenarios presented in this documented are based on the use cases which are derived based on the analysis of the value chain for a given company, and the associated assets.

5 Introduction

5.1 Objective and Scope

The objective of this document is to present a series of detailed scenarios that show the interactions between the parties in the cyber-insurance process and are sufficiently representative of the global cyber-insurance ecosystem.

5.2 The cyber-insurance scenario definition process

The scenarios are based on previously defined use cases, which are derived from the analysis of the value chain for a given company and the associated assets detailed in Section I.

The aim in choosing these scenarios was to present a broad cross-section of possibilities. They represent companies of varying sizes – large companies as well as SMEs – together with a range of sectors – financial services, professional services, and manufacturing. They also present a range of situations: loss of personally identifiable data, insurance fraud, and the use of cyber means to manipulate products and services.

5.3 Chapter Structure

Section 6 provides definitions of key terms that are used in the various scenarios. Section 7 presents the scenarios themselves: The first scenario describes a cyber attack on a large financial sector institution results in the loss of personally identifiable data for the company's customers. The second scenario involves an SME in the professional services sector in which insider actors intentionally infect the company with ransomware in order to engage in insurance fraud. The third scenario involves a cyber attack on a manufacturing companies that makes products such as airplanes and satellites that results in the alteration of manufacturing plans, so that the final product is not compliant with the initial specifications. Section 8 concludes and summarizes.

6 Definitions

This section provides definitions of key terms that are used in the descriptions of each scenario.

Table 1: Vulnerabilities

This table provides definitions of the cyber security vulnerabilities referred to in the scenarios – it contains a short description as well as the Code or CVE ID as a reference to further information publicly available.

Code and CVE ID	Name	Description
CVE-2014-6271[16]	Shellshock	Shellshock vulnerability allows to gain unauthorized access to the company server[17].
CVE-2016-5195	Dirty COW	This vulnerability in the Linux Kernel allows local users to achieve privilege escalation[18].
CVE-2012-0507	Oracle Java SE Remote Java Runtime Environment Code Execution Vulnerability	This vulnerability allows remote attackers to affect confidentiality, integrity, and availability of data and code[19].
CVE-2014-0515	Adobe Flash Player Buffer Overflow Vulnerability	This vulnerability allows attackers to execute arbitrary code using Adobe Flash Player[20].
CVE-2014-0556	Adobe Flash Player and AIR Unspecified Heap Based Buffer Overflow Vulnerability	This vulnerability allows attackers to execute arbitrary code using Adobe Flash Player[21].
CVE-2017-6607	Cisco ASA Software DNS Denial of Service Vulnerability	This vulnerability Software allows an attacker to reload a device or corrupt its information[22].

[16] The Common Vulnerabilities and Exposures (CVE) system provides a catalog for known security vulnerabilities and exposures.

[17] http://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2014-6271

[18] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5195

[19] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0507

[20] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0515

[21] http://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2014-0556

[22]https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-asa-dns

CVE-2017-3850	Cisco IOS and IOS XE Software IPv6 Denial of Service Vulnerability	This vulnerability enables an attacker to cause a denial of service situation[23].
CVE-2017-6648	Cisco TelePresence Endpoint Denial of Service Vulnerability	This vulnerability enables an attacker to cause a TelePresence endpoint to reload, leading to denial of service (DoS) situations[24].
CVE-2017-0143/4/5/6/7/8	EternalBlue, EternalChampion, EternalRomance	https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144

Table 2: Regulations

This table provides a set of regulations that are relevant to the scenarios.

Name	**Country scope**	**Description**
EU Data Protection Directive 95/46/EC	EU	This EU directive regulates the personal data processing within the European union. In particular, article 17 "Security of processing", states that "...Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing."[25]
Data Protection Act 1998	United Kingdom	This act is the implementation of the EU Data Protection Directive in UK law. It defines how personal data is stored and processed by public or private entities in the UK.[26]
Federal Data Protection Act (BDSG) (last updated in 2017)	Germany	This act is the implementation of the EU Data Protection Directive in German law. It protects the individual against his/her right to privacy being impaired through the handling of his/her personal data.

[23] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170320-aniipv6

[24] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-tele

[25] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=FR

[26] https://www.legislation.gov.uk/ukpga/1998/29/contents

		Penalties for criminal offences related to this Act may result in fines up to € 300 000 or prison sentences for up to two years.[27] Its last update in 2015 reflects the changes introduced by the new EU regulation (GDPR) of 2016 – see below.
Act No. 78-17 of January 6 1978 on Information Technology, Data Files and Civil Liberties (last updated in 2005)	France	This act is the implementation of the EU Data Protection Directive in French law. Penalties in case of breaches to the Act may result in fines up to 5% of gross year revenue, and even imprisonment in case of impediment of the activities of the French Data Protection Authority (CNIL)[28].
Organic Law 15/1999 of Protection of Personal Data (last update in 2011)	Spain	A national implementation of the EU Data Protection Directive 95/46/EC from the Spanish Data Protection Commissioner's Office (AEPD). The Royal Decree 1720/2007 (last update in 2012) develops the principles of the law and the measures to be applied to comply with them. Obligations for public and private actors processing personal data are in line with those of the Directive 95/46/EC, including security measures and data breach notification. Sanctions are mostly financial, with fines amounting to a maximum of € 600 000 for extremely severe breaches of the regulation[29].
Regulation 2016/679 - General Data Protection Regulation (GDPR)	EU	The GDPR regulation will replace the previous Directive 95/46/EC once it is fully effective starting from May 25, 2018. Financial sanctions span from warnings up to € 10 million or 2% of the annual turnover[30].
EU Directive 2016/1148 - Network and Information Security Directive	EU	The NIS Directive contains legal measures to enforce the improvement of overall cybersecurity of EU Member States, and their increased cooperation via the implementation of Computer Security Incident Response Teams, national NIS authorities, and the identification of operators of essential services (OES). It also requires Member States to provide sufficient security measures for OES sectors, and the

[27] https://www.gesetze-im-internet.de/englisch_bdsg/

[28] https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf

[29] www.legislationline.org/documents/id/9044&usg=AOvVaw3eJTqN5sOdwNZk0ZIl9nbd

[30] http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

		notification obligation of serious incidents to the national NIS authority[31].
IT Security Act (ITSiG)	Germany	The ITSiG Act requires actors identified as critical infrastructure operators to implement state-of-the-art security measures and to report security incidents to the Federal Office for Information Security (BSI)[32].

Table 3: Global risks

Label	**Description**
Data Loss	This risk applies in events confidential information is disclosed to an unauthorized recipient who does not have the clearance to access it. Typically, this would include the exposure of proprietary, sensitive, private or classified information through either data theft or data leakage including personal data e.g. patents, financial statements.
E-Fraud	The use of computers to commit fraud, or theft of money, securities, or other property, having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the organization with a statute to require protection against unauthorized disclosure.
Business / Industrial Process Disruption or Misuse Without Physical Damage	Business / Industrial Process Disruption or Misuse is related to the loss of service or manipulation of the process, resulting in a loss of confidence or system downtime, and excluding physical asset damage.
Manipulation of Products / Services	Manipulation of Products / Services applies when products (data or software) has been deleted or corrupted and refers to unauthorized modifications to code or data, attacking its integrity, availability and functional purpose.

[31] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148

[32]https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*%255B@attr_id='bgbl115s1324.pdf'%255D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s1324.pdf%27%5D__1515322836083

Table 4: Assets

This table provides a list of groups of assets and the typical assets each group include.

Group	**Components**
Process	R&D Sales Design Production and manufacturing Accounting Compliance
Information	Intellectual Property / Patents Customer data Personally Identifiable Information (PII) data Payment Card Information Marketing research and analysis Financial statements Business Intelligence Executive Management Information Source code
Hardware	IT infrastructure Production lines Large Infrastructure (Real-estate, etc.)
Software	Customer relationship management (CRM) Accounting IT (Active Directory) Productivity (Sharepoint, etc.)
Personnel	Executive management Finance Network administrators Security personnel Employees

Table 5: Threat actors

This table provides a list of threat actors or other adversaries that may seek to access or compromise an organisation's information. This list is a subset of the Common Threat List (CTL) defined by the Information Security Forum (ISF) in its information risk assessment methodology IRAM233.

Label	**Typical motivation**
Competitor	Espionage, market share
Employee (general or privileged)	Vengeance, coercion
Hacking group	Financial gain, technical challenge, ideology
Individual hacker	Financial gain, technical challenge, status
Nation-state	Espionage, political or strategic advantage
Organized criminal group	Financial gain

Table 6: Technical types of attack

This table provides examples of technical attacks.

Label	**Description**
Alteration attack	This form of attack leverages unauthorized code and data alterations in order to obtain a change in the intended execution by means of code and data integrity corruption[34].
Botnet	A botnet is a network of remotely controlled machines used to launch wide-scale denial of service (see DoS) attacks against specifically targeted resources[35].
Brute-force attack	In this form of attack, the attacker attempts to identify a password or an encryption key through exhaustive checks until the correct string is identified.

[33] https://www.securityforum.org/tool/information-risk-assessment-methodology-iram2/

[34] https://www.sans.edu/cyber-research/security-laboratory/article/alter-code

[35] https://www.sans.org/reading-room/whitepapers/malicious/bots-botnet-overview-1299

Denial of Service (also Distributed)	A Denial of Service attack consists in an attempt to prevent users from accessing data or services provided by an information system[36].
Eavesdropping/Traffic analysis	This form of attack consists in capturing and analysing network data packets in order to identify any information that may be relevant for other types of exploits.
Email spoofing	This form of attack consists in sending emails with a false sender identity, so that the receiver is misled to believe the message originates from another sender.
IRC[37] Flooding	This attack is a specific case of DoS attacks, and proceeds by either disconnecting users from the IRC servers, or by severely degrading the server's performance.
Malicious code/payload	This is a generic family of attacks all of which involve harmful code or script designed to be executed by programs, operating systems, web servers, and any other IT device, resulting in undesired effects.
Man-in-the-middle	This form of attack is a specific case in the eavesdropping type of attacks, in which a threat actor interposes between the sender and the receiver and misleading them into believing their communication line is direct and secure. This allows to either intercept confidential information, or alter it unknowingly to the legitimate communication participants[38].
Masquerading	This type of attack consists in an attacker posing as a user with legitimate rights and authorizations in order to access to data or network systems.
Replay attack	A particular case of both traffic analysis and masquerade attacks, in which authentic data, collected during a previous eavesdropping session, is resent by the threat actor in order to masquerade her/his identity as a legitimate user.
Phishing	This attack type aims at obtaining confidential information by leveraging techniques such as email spoofing.

[36] https://www.us-cert.gov/ncas/tips/ST04-015

[37] Internet relay chat is a text communication protocol.

[38] F. Callegati, W. Cerroni and M. Ramilli, "Man-in-the-Middle Attack to the HTTPS Protocol," in *IEEE Security & Privacy*, vol. 7, no. 1, pp. 78-81, 2009.

Resource enumeration and browsing	This is a type of attack through which the threat actor is able to obtain from a targeted system the list of resources that are present in the system, therefore enabling the threat actor to refine the targeting process of such resources and their consequent browsing.
Viruses, malware	Viruses and malware are types of malicious code/payload with various objectives, among which can be mentioned replication, data manipulation or destruction, etc.

Table 7: Impact

This table details the typical impacts an organisation may face when the target of an attack. The impact is the consequence an attack may have on an organisation's ability to conduct its operations and provide the services it delivers.

Label	**Description**
Loss of data and software	Information destruction and/or leakage due to data breach and consequent data exfiltration.
Loss or damage to physical properties	Product loss or undesired alteration of its specifications.
Product recall	Product retrieval following the detection of defects in said products.
Fraud	Concealment or distortion of facts leading to undue rights or compensations.
Theft of money, securities	Undue appropriation of financial means.
Extortion	The action of obtaining rights or financial means through threats or violent actions.
Privacy liability	This liability includes the claims which arise following breaches of private or sensitive data.
Identity theft	The intentional use of the identity of another physical or moral person.
Failure to render the service	The inability to provide agreed services on a contractual agreement.
Security liability	This liability includes the claims which arise following security breaches.

Property damage, personal injury	Damage and/or destruction of property, including injury to persons and casualties.
Media liability	The liability including claims of infringement of copyright, plagiarism, and defamation.
Product liability	The act of engaging the responsibility of the provider or supplier of a product following damage caused by the product under scrutiny.
Failure to supply	Inability to provide agreed products.
Management liability	Claims and/or allegations on specific responsibilities targeting the liability of directors or officers of an organization.
Breach of duty	Failure to provide the expected functions and services associated with a certain position for an individual, or with an organization providing products or services.
Loss of competitive advantage	Strong reduction or even complete loss of knowledge providing competitive advantage such as intellectual property, commercially sensitive information, strategic information, etc.
Brand and reputational damage	Decrease in the positive perception that the general public, the market, or investors have on the brand and reputation of an organization.
Non-compliance with regulation	Lack of conformity with respect to regulations.
Business interruption	Discontinuity of business-related processes and tasks.

Table 8: Attack tools

This table provides examples of technical tools referred to in the scenarios that can be used to launch attacks.

Attack tool name	**Description and references**
C99 PHP Shell	A script page in PHP allowing to implement the Shellshock exploit[39].
nmap	Tool for network discovery and security auditing[40].
Shodan	Shodan is a tool that allows to discover devices connected to the Internet, and collect information about their location and users[41].
CryptoWall	Cryptowall is a data encryption ransomware using the RSA-2048 encryption. The operating procedure is similar to other ransomwares such as Cryptolocker.[42]
RIG exploit kit	The RIG Exploit Kit is leveraged to infect systems and different versions of ransomware.[43]
Nuclear[44] exploit kit	The Nuclear exploit kit allows to launch attacks against IT systems[45].

[39] http://web2.clarkson.edu/projects/itl/projects/fa2006/honeynet/files/attack_analysis.pdf

[40] https://nmap.org/

[41] https://www.shodan.io/

[42] http://malware.wikia.com/wiki/Cryptowall

[43]https://community.rsa.com/community/products/netwitness/blog/2017/02/01/rig-ek-chronology-of-an-exploit-kit

[44] https://blog.checkpoint.com/wp-content/uploads/2016/04/Inside-Nuclear-1-2.pdf

[45] https://blog.checkpoint.com/wp-content/uploads/2016/04/Inside-Nuclear-1-2.pdf

Table 9: Identification and response process

This table provides a list of incident identification and response processes, differentiated by the level of required information security capabilities and skills to be implemented effectively in an organisation.

Process ID	Process	Required information security capabilities and skills
1	The process starts with a set of events which are collected from several sources, including human and software. If the set of events matches with a given pre-defined use case corresponding to a specific alert, then the alert is issued. The level 1 of the Security Operations Center (SOC) oversees the validation or invalidation of the alert. In case the alert is qualified as a false positive, then it is documented as such and details are provided on the reasons behind the qualification as false positive. If the alert is qualified as true positive, then its severity is assessed. The assets that would be impacted by such an alert are evaluated. A ticket is created to what corresponds now to a confirmed incident. From this stage, the incident is handled by the incident response team. If the incident is major, then it corresponds to the qualification of crisis, and thus involving also the crisis management and business continuity team.	This process requires an internal team of experts to monitor events, triage and evaluate alerts and then respond. This type of internal capabilities and skills are typically found in large organisations
2	The process for a medium-size company is partially similar to the one for large companies. The first difference is that the collection and analysis of events is most likely to be outsourced to an external security monitoring provider. The security monitoring provider follows the same process as an internal SOC, and finally issues reports on alerts and identified incidents to the client company. Then, the respective officers in the medium-size company in charge of cybersecurity and/or asset protection follow up with identified actions addressing countermeasures, remediation, and business continuity. It should be noted that this may involve additional third-party providers, such as data backup companies, cloud service providers, public cybersecurity agencies, etc.	The process requires the same level of capabilities and skills but from a lower number of people as part of the activities are outsourced to a service provider. The is typically a process used in mid-size organisations.
3	The identification and response process for an SME is significantly simpler than the previous two. For generalization purposes, it is safe to assume the implementation and deployment of minimal baseline incident detection measures, such as anti-virus software and cloud data backup solutions. Unless the SME outsources the incident detection process to a professional cybersecurity company, or even to the cloud services provider, it is very likely that the incident detection	This process is usually applied in small organisations where resources dedicated to information security are very limited and rarely full time.

	will occur when day-to-day activities are impacted by an ongoing or past attack. The response process will in many cases be undefined and will be decided on an ad-hoc basis. Provider and customer management will be the first concern when addressing a serious issue, followed by the business impact assessment and the insurance claim if relevant.	

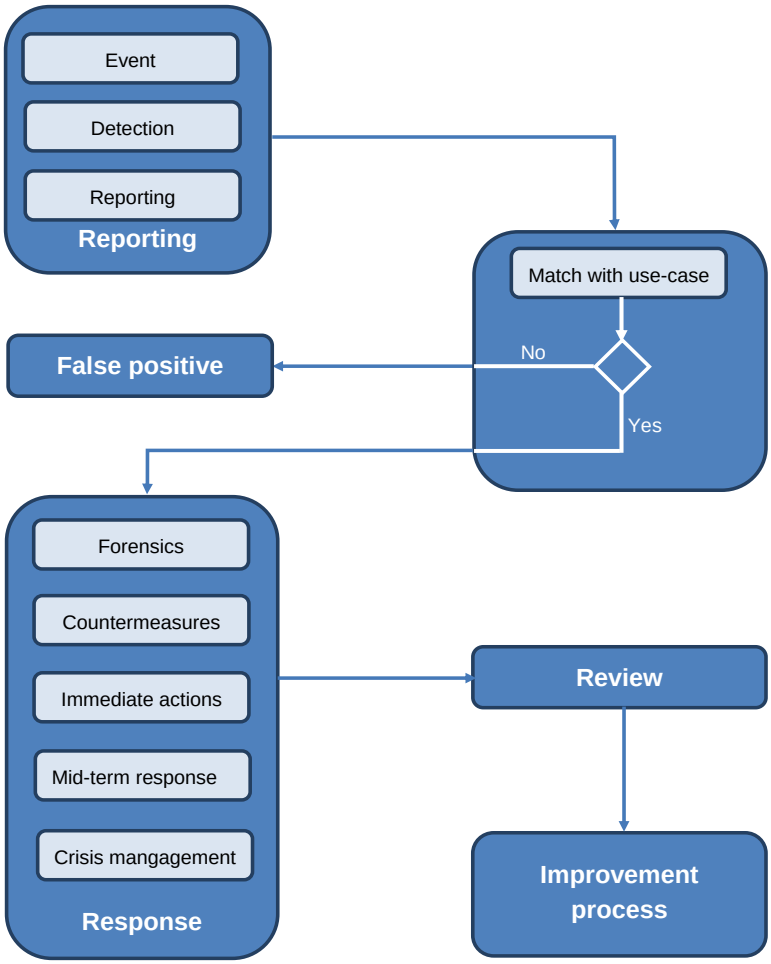

Figure 11: Threat identification and response process for large companies

Table 10: Safeguards and countermeasures

This table provides a list of safeguards and countermeasures that can prevent or mitigate the impact of an attack on an organisation.

Type	Description
Business Continuity Plan	Set of processes which enable an organization to maintain operations during negative events or threat occurrences.
Security Policy	Formal document stating the plans of an organization for protecting its assets.
Common Technical Barriers: Antivirus/Firewall/ Intrusion Detection System/ Data Backup Solution	Technical barriers include all hardware and software solutions which either do not allow threat actors in achieving their objectives, or detect threat actors before, during and after an attack, or compensate for negative impacts in case of a successful attack.
Secure Configuration	Security measures and parameters defined and implemented in such a way as to reduce vulnerabilities.
Awareness Training	Training methods and processes which increase the education and sensitivity level of employees on matters of security.
Honeypots	Security countermeasure consisting of IT assets which appear as very appealing, but with no real value, that an organization deploys in order to deflect the attack attempts from threat actors.
Incident Response	The process, or set of processes, that defines the sequence of actions to be carried in order to detect, react, and provide response to cybersecurity incidents.
Security Personnel / Data Protection Officer	The set of employees whose functions consists in fulfilling the security day-to-day operations and activities, along with officers having specific key roles in a security policy.
Information Sharing Programs	Specifically designed and implemented processes and enabling technology for sharing relevant information in a secure and instructive way.
Inventory of Assets	Exhaustive database of raw materials, hardware, software, products, services, and

	all other assets used in maintaining business operations and client delivery of services and goods.
Continuous Vulnerability Assessment and Remediation	The process of proactive identification and correction of vulnerabilities reported through any source, including regular scans and vendor reports.

Table 11: Potential loss

This table provides a list of potential losses an organisation may face. While ultimately all losses are financial, the categories offered below make it possible to consider losses other than just the direct financial losses from the alteration of production or service delivery.

The loss differs from the impact as the impact considers the change of abilities to produce while the loss focuses on how much an incident may cost to an organisation.

Category	**Components**
Revenue loss	Direct loss Compensatory payments to customers and/or suppliers Future revenue loss Investment loss
Brand and reputation damage	Customers Suppliers Banks Partners Public agencies
Financial penalties	Contractual Regulatory Legal
Loss of competitivity and productivity	Employee activity interruption Interruption of provided services/products

Collateral expenses	Recovery expenses Analysis and audit Additional manpower for temporary activities

Table 12: Levels of financial impact

Level	**Threshold**
Low	Impact < € 500 000
Medium	€ 500 000 < Impact < € 5 000 000
High	€ 5 000 000 < Impact < € 50 000 000
Very high	€ 50 000 000 < Impact < € 100 000 000
Critical	Impact > 100 000 000

Table 13: Criteria for level of likelihood

This table provides indications as to what each level of likelihood means and the criteria are considered to conclude on each level.

Level of likelihood	**Meaning**
Low	The chances that such a scenario happens and the attack it describes is rare, due to the high level of readiness of the organisation targeted and the high level of motivation and means an attacker would have to deploy in order to be successful. For example, an individual hacker may attempt to launch an attack against a EU Member state law enforcement agency and while a few successful cases were reported in the past, the very high level of readiness of law enforcement agencies in detecting and preventing such attack makes it very unlikely to succeed. Therefore, the likelihood of this scenario is **Low**.
Medium	The possibility such a scenario happens and the attack being successful is possible. It happens when the means and motivations of the attackers are of relatively equal level with the maturity and readiness of the organisation to detect and respond to attacks. For example, an organised criminal organisation having the means and motivation to dedicate intelligence

	gathering, time and commitment in hacking a large organisation for its data. Similarly, an individual hacker may launch successful attacks against an organisation with a low level of maturity in information security.
High	This scenario is most likely to happen and the attack to be successful. Scenario with a high level of likelihood often present an attacker with means and motivation that highly surpasses the level of maturity of their target. For example, it's a nation-state, with almost infinite means, targeting a private foreign organisation, an organised criminal organisation targeting a small organisation with limited resources to deploy safeguards and countermeasures.

7 Cyber-insurance scenarios

This section provides the cyber-insurance scenarios in a common and structured view which allows for a standardized analysis in each particular scenario, despite their respective specificities.

7.1 Scenario 1[46]: Loss of personally identifiable data for a large company in the financial sector

1. Background

Rocardier Finance is a large financial company with subsidiaries in over 18 countries, with its headquarter in Paris, France. The company has a strong foothold in EU countries with approximately 52% of its turnover in the European market. The US and Asia represents its second largest markets with 40 % of its turnover, the remaining 8% being distributed in the remaining regions. Rocardier Finance provides portfolio management and brokerage desks to institutional and individual investors regarding most financial instruments such as bonds, stocks, contracts for difference, and real-estate investments.

A. Constraints, assumptions, and preferences

- Regulations

The French legal entities of the company must comply with the following regulations from the data and information security perspective:

- EU Directive 2016/1148 - Network and Information Security Directive
- Regulation 2016/679 -General Data Protection Regulation (GDPR)
- Act No. 78-17 of January 6 1978 on Information Technology, Data Files and Civil Liberties

- Compliance

Because of its banking activities, Rocardier Finance must ensure compliance with the following regulations:

- Bale III, which imposes a solvability ratio of at least 10.5%.
- AMF regulations: Obligation to collect information on all individual and institutional clients for transparency and tracking purpose, especially against market manipulation and insider trading. Such information can also be required by TRACFIN[47] which conducts investigations on specifically targeted individual and institutional clients for anti-money laundering and anti-terrorist funding measures.

- Assumptions

[46] This scenario corresponds to use case 2.

[47] TRACFIN (Traitement du Renseignement et Action contre les Circuits FINanciers clandestins), is a service of the French Ministry of Economy specialized in fighting money laundering and any other illegal financial activities.

- Turnover of the company: € 54 billion
- Net income: € 6.2 billion
- Because of its size and its large potential impact on the global economic landscape, the company has interactions with the French cybersecurity regulator agency ANSSI.

• Preferences
- The company has a strong preference for discretion and anonymity when considering cyber-attacks, regulation and compliance breaches and financial penalties or sanctions.

B. Assets to be protected
• Customer data
• Personally Identifiable Information (PII) data
• Payment Card Information
• Marketing research and analysis
• Financial statements
• Business Intelligence
• Executive Management Information

C. Potential threats[48]
• Threat actors: Organized criminal groups, Employees, Hacking groups and individual hackers
• Motivation: Espionage, Theft, Financial, Ideology
• Types of attack: All types of attacks listed in Table 6.

D. Uncertainties
• Uncertainties of the defender
- The repercussions of a successful attack on the market and stakeholder perception of the company
- The legal and regulatory repercussions following potential breaches
- The probability of successfully repelling or containing cyber-attacks, i.e. the efficiency of security safeguards and countermeasures.
• Uncertainties of the attacker
- The time and effort it will take to penetrate the network of the company and its information systems
- The eventual success probability of identifying valuable assets
- Capability of avoiding detection measures
- The ability to avoid identification during the cyber-attack

E. Safeguards and countermeasures

[48] We recall that in the risk scenarios presented in this document, a threat is composed by the involved threat actor, its capability, and its motivation. Capability is composed of the means to carry out an attack coupled with the required expertise and know-how.

- All safeguards and countermeasures listed in Table 10 are implemented in the organisation, yet the effectiveness of some of these safeguards and countermeasures could be improved.

F. Potential impact and loss
- Potential impact and loss for the attacker
  - IP ban
  - Legal suits from law enforcement agencies resulting in imprisonment or reduced freedom
  - Loss of time resulting in an unfruitful attack effort
- Potential impact and loss for the defender
  - Data loss
  - Response costs
  - Brand damage
  - Regulatory fines

G. Initial considerations on the scenario likelihood

Organised criminal groups are known to perform numerous attack against organisations to steal their data or the information of their customers. Similarly hacking groups and individual hackers may consider Rocardier Finance as a challenge and targeting this organisation in line with their ideology. Therefore, the likelihood for Rocardier Finance to be targeted by such a group is significant due to the information it handles. On the other hand, the overall high level of cybersecurity maturity posture of large financial organisation and the regulations they need to comply with, that require information security safeguards and countermeasures, provides Rocardier Finance with a high level of readiness in identifying, responding and preventing this attack considered in this scenario.

The likelihood of this scenario is therefore estimated at a **Medium** level.

H. Insurance perspective
- Risk assessment and recommendations
  - Cyber-risk assessment
    Rocardier Finance is subject to regular and extensive cyber-assessments programs (cybersecurity maturity ratings, penetration testing campaigns). Consequently, the profile of the company appears very solid.

  - Estimated cost of potential losses
    Given the risk scenario and the considerable domino impact of a successful cyber-attack on the financial market sector on a large financial institution, the estimated cost of potential losses[49] is set at High (see Table 12).

  - Recommended security controls

[49] We recall that the potential loss includes the loss of each individual impact and loss for the defender.

Rocardier Finance has already implemented all recommendable security control. No additional recommendations can be provided.

- Insurance policy 1
  The insurance policy in the scope of this risk scenario is defined by the following elements:

  - Insured legal entity: Rocardier Finance S.A, France
  - Customer declaration elements: The customer has declared the value of the covered assets and, as well as the security measures taken as precautionary measures in the event of incidents impacting such assets.
  - Covered risks: Data loss, Fraud
  - Exclusions: 3rd party liability, stock market depreciation following risk occurrence
  - Endorsements: The cyber-insurance policy for Rocardier Finance S.A is conditioned upon the effective risk assessment and any additional audits required by the insurance company prior to, and after the occurrence of, the risk events covered in the insurance policy.

- Insurance policy 2
  The insurance policy in the scope of this risk scenario is defined by the following elements:

  - Insured legal entity: Rocardier Finance S.A, France/Italy
  - Customer declaration elements: The customer has declared the value of the covered assets and, as well as the security measures taken as precautionary measures in the event of incidents impacting such assets.
  - Covered risks: Data loss, Fraud, Identity theft
  - Exclusions: Regulatory financial penalties
    Endorsements: The cyber-insurance policy for Rocardier Finance S.A is conditioned upon the effective risk assessment and regular independent audits required by the insurance company prior to, and after the occurrence of, the risk events covered in the insurance policy.

- Insurance policy 3
  The insurance policy in the scope of this risk scenario is defined by the following elements:

  - Insured legal entity: Rocardier Finance Group, Europe/U.S.
  - Customer declaration elements: The customer has declared the value of the covered assets and, as well as the security measures taken as precautionary measures in the event of incidents impacting such assets.
  - Covered risks: Data loss
  - Exclusions: 3rd party liability, stock market depreciation following risk occurrence
    Endorsements: The cyber-insurance policy for Rocardier Finance Group is conditioned upon the effective risk assessment of individual legal entities. The underwriting pricing and contractual agreements will be fixed separately for each legal entity of Rocardier Group in Europe and U.S.

- Covered loss
  - Business interruption
  - Brand damage

- Premiums
  The insurance company offers legal advice in case of legal suits from 3rd parties following cyber-attacks which are identified as in scope of the insurance policy contract. Also, insurance companies provide free security modules to the software and mobile apps that Rocardier Finance offers to the organization's individual and institutional users for their day-to-day operations.

- Deductibles
  - The insurance company will deduct 3% of the premium for every additional year without filed claims. The deductibles will be null after each year with reported incidents followed by a filed claim.

2. Scenario execution

A. Involved threats

- Actors and motivation
  The risk scenario is perpetrated by an actor of the Organized crime category, and the motivations belong to the Financial and Theft types.

B. Attack vector and execution

- Vulnerabilities and tools
  - nmap
  - Shodan
  - CVE-2014-6271 - Shellshock
  - CVE-2016-5195 - DirtyCOW
- Execution of the attack
  1. The attackers follow one of the following: (i) scan the website of the company for vulnerabilities with nmap, or (ii): lookup on Shodan for vulnerable websites belonging to this company, or associated contractor websites.

  2. The attack is activated through a vulnerability such as Shellshock which allows attackers to gain unauthorized access to the company server. More precisely, attackers are able to use Shellshock to execute code and add a malicious web page on the website allowing the attacker to connect to the database, since the webserver must have access to the database in order to interact with it. After gaining access to the server, the attackers use another vulnerability exploit such as Dirty COW through a modified version of the C99 PHP script to gain administrative power on the server. Such action is useful for privilege escalation required for long-time persistence. This allows the attackers to install a command and control malware module allowing them to orchestrate the exfiltration of data from the company server.
  Identification and response process

- The Identification and response process is the one described by Process ID #1 in Table 9, and illustrated in Figure 11.

C. Impacted assets
- The impacted assets are composed of the type Information: Personally Identifiable Information (PII) data, in Table 4.

D. Observed impact and loss
- The observed impacts include Loss of data and software, Privacy liability, Security liability, and Brand and reputation damage, as per Table 7.
- Observed losses include: (i) Customer's loss due to Brand and reputation damage category, and (ii) Recovery expenses, Analysis and audit expenses related to the Collateral expenses category, as per Table 12.

E. Post-attack insurance overview
- Audit and forensics
- Scope analysis of incurred loss
- A priori decision on insurance coverage

7.2 Scenario 2[50]: Insurance fraud for an SME in the professional services sector

3. Background

Iberia Consultivo is a professional services SME with its headquarters in Madrid, Spain. It operates solely on the Spanish market. Iberia Consultivo provides advisory services to individuals, companies, and public institutions on topics including legal, regulatory, and business strategy.

A. Constraints, assumptions, and preferences

- Regulations
  - Regulation 2016/679 -General Data Protection Regulation (GDPR)
  - Organic Law 15/1999 of Protection of Personal Data
- Compliance

  Given the activities of the company, no compliance requirements are mandatory for Iberia Consultivo.

- Assumptions
  - Turnover of the company: € 37 million
  - Net result: € 4.7 million
- Preferences
  - The company prefers internalized IT infrastructure and cybersecurity solutions. It strongly avoids outsourced services.

B. Assets to be protected

- Customer data
- Personally Identifiable Information (PII) data
- Financial Statements
- Executive Management Information
- Business Intelligence
- Marketing research and analysis

C. Potential threats

- Threat actors: Organized criminal group, Employee, Individual hackers
- Motivation: Theft, Financial, Vengeance, Technical challenge
- Types of attack: All types of attacks listed in Table 6.

D. Uncertainties

- Uncertainties of the defender[51]
  - The legal and regulatory repercussions following potential breaches
  - The impact of successful cyber-attacks on the business activities

[50] This scenario corresponds to use case 3.

[51] In this particular risk scenario, the defender is assumed to be the legal representative of the company, i.e. the CEO.

- Uncertainties of the attacker[52]
  - The legal repercussions in case of their identification
  - The success in perpetuating the fraud the insurance company

E. Safeguards and countermeasures
- The safeguards and countermeasures are limited to an antivirus commercial product, a firewall for the company internet gateway, and a data backup solution deployed internally.

F. Potential impact and loss
- Potential impact and loss for the attacker
  - Legal suits from law enforcement agencies resulting in imprisonment or reduced freedom
  - Loss of time resulting in an unfruitful attack effort
- Potential impact and loss for the defender
  - Data loss
  - Brand damage – loss of clients
  - Regulatory fines
  - Refusal from insurance company to cover the induced costs

G. Initial considerations on the scenario likelihood

The likelihood for the scenario of insurance fraud by insider actors is estimated at a **Medium** level. While the risk of insurance fraud has a high level of frequency on a global scale, yet the relatively low implementation of cyber-insurance policies moderates this risk[53].

H. Insurance perspective
- Risk assessment and recommendations
  - Cyber-risk assessment

    Iberio Consultivo conducts occasional cyber-risk assessments in the framework of penetration testing missions by external and independent audit companies.

  - Estimated cost of potential losses penetration

    Given the risk scenario, the profile of the company, and the repercussions of cyber-attacks on the business sector of Iberia Consultivo, the estimated cost of potential losses is set at High (see Table 12).

  - Recommended security controls

    The insurance companies may require additional security controls consisting of Inventory of assets and a Business continuity plan as per Table 10.

- Insurance policy 1

[52] The attacker in this scenario is composed by a manager and a subset of the employees.
[53] In the future there may be an increase in the trend of this risk, due to the increasing subscription of cyber-insurance policies.

The insurance policy in the scope of this risk scenario is defined by the following elements:

- Insured legal entity: Iberia Consultivo, Spain
- Customer declaration elements: The customer has declared the value of the covered assets and, as well as the security measures taken as precautionary measures in the event of incidents impacting such assets.
- Covered risks: Data loss
- Exclusions: 3rd party liability, Incidents following acts of negligence.

Endorsements: The cyber-insurance policy for Iberia Consultivo is conditioned upon the effective risk assessment and any additional audits required by the insurance company prior to, and after the occurrence of, the risk events covered in the insurance policy.

- Insurance policy 2

The insurance policy in the scope of this risk scenario is defined by the following elements:

- Insured legal entity: Iberia Consultivo, Spain
- Customer declaration elements: The customer has declared the value of the covered assets and, as well as the security measures taken as precautionary measures in the event of incidents impacting such assets.
- Covered risks: Fraud, Privacy liability
- Exclusions: 3rd party liability, media liability, extortion.

Endorsements: The cyber-insurance policy for Iberia Consultivo is conditioned upon the effective risk assessment and any additional audits required by the insurance company prior to, and after the occurrence of, the risk events covered in the insurance policy.

- Covered loss
  - Business interruption
  - Brand damage

- Premiums

The insurance company offers an external data backup solution hosted on a recommended and trusted Cloud operator.

- Deductibles
  - The insurance company will deduct 35% of the premium for every year in which a data backup service has been subscribed by the insured company.

4. Scenario execution
   A. Involved threats
   - Actors and motivation

The risk scenario is perpetrated by an actor of the Insider category, and the motivations is of the Financial type.

   B. Attack vector and execution
   - Vulnerabilities and tools

- Cryptowall
- Rig
- Nuclear
- Oracle Java SE Remote Java Runtime Environment Code Execution Vulnerability (CVE-2012-0507)
- Adobe Flash Player Buffer Overflow Vulnerability (CVE-2014-0515)
- Adobe Flash Player and AIR Unspecified Heap Based Buffer Overflow Vulnerability (CVE-2014-0556)

- Execution of the attack

  1. The insider threat actor intentionally infects company servers with ransomware such as the CryptoWall ransomware, by following malware-infected adds on the Zedo ad network[54]. Then tools such as the Rig and Nuclear tools exploit one of the aforementioned vulnerabilities to install the CryptoWall on the servers of the company.

  2. The CryptoWall ransomware encrypts the data located in the company servers, therefore interrupting their usage for day-to-day operations of the company.

C. Identification and response process
- The Identification and response process is the one described by Process ID #3 in Table 9.

D. Impacted assets
- The impacted assets are composed of the type Information: Customer data, Personally Identifiable Information (PII) data, and Financial Statements data, in Table 4.

E. Observed impact and loss
- The observed impacts include Fraud, Media liability, Management liability, and Brand and reputation damage, as per Table 7.

F. Post-attack insurance overview
- Audit and forensics
- Scope analysis of incurred loss
- A priori decision on insurance coverage

[54] Zedo is a privately held company specialized in online advertising of products and services to Internet publishers, advertisers, and agencies.

7.3 Scenario 3[55]: Manipulation of Products / Services for a large company in the manufacturing sector

5. Background

European Aerospace Company (EAC) is a large manufacturing company with subsidiaries in 7 countries, with its headquarters in Stuttgart, Germany. The company has a global foothold with approximately 48% of its turnover in the Middle East, 23% in Europe, 17% in Asia, and 12% in the US. EAC manufactures airplanes, satellites, and related technology for commercial and military clients.

A. Constraints, assumptions, and preferences

- Regulations
  - Regulation 2016/679 - General Data Protection Regulation (GDPR)
  - EU Directive 2016/1148 - Network and Information Security Directive
  - Federal Data Protection Act
  - IT Security Act (ITSiG)
- Compliance
  - Given the activities of the company, confidentiality compliance is required from the Department of Defense of the respective country in which the company operates for military clients.
- Assumptions
  - Turnover of the company: € 69 billion
  - Net result: € 1.4 billion
  - Given the size and the sensitive domain of activity, the company has tight links with governmental cybersecurity and defense agencies.
- Preferences
  - EAC has a strong preference for locally deployed cybersecurity protective measures, and prefers specifically-tailored services and products developed by external providers.

B. Assets to be protected

- IT Infrastructures
- Production lines
- Intellectual Property / Patents
- Customer data
- Personally Identifiable Information (PII) data
- Financial statements
- Business Intelligence
- Executive Management Information

C. Potential threats

- Non-intentional threats
  - Natural disasters

[55] This scenario corresponds to use case 4.

  - Production line failures and accidents
  - Fire
- Intentional threats
  - Threat actors: Hacktivists, Competitors, State Actors, Organized Crime
  - Motivation: Espionage, Financial, Ideology
  - Types of attack: All types of attacks listed in Table 6.

D. Uncertainties
- Uncertainties of the defender
  - The repercussions of a successful attack on the market and stakeholder perception of the company
  - The legal and regulatory repercussions following potential breaches
  - The probability of successfully repelling or containing cyber-attacks, i.e. the efficiency of security safeguards and countermeasures.
- Uncertainties of the attacker
  - Ability to penetrate the IT infrastructure
  - Ability to manipulate the product manufacturing designs
  - Ability to avoid detection measures
  - Ability to avoid identification

E. Safeguards and countermeasures
- All safeguards and countermeasures listed in Table 10

F. Potential impact and loss
- Potential impact and loss for the attacker
  - Reinforced protective measures leading to excessive loss of time and effort.
  - Increased risk of traceability and identification leading to increased legal and penal risk, especially for competitor companies.
  - Political and economic implications in case of identification, including commercial bans in case of international retaliation.
- Potential impact and loss for the defender
  - Loss or damage to physical properties
  - Product recall
  - Brand and reputational damage
  - Non-compliance with regulation
  - Business interruption

G. Initial considerations on the scenario likelihood

Product/Services manipulation attacks by malicious actors happen on a regular basis. While competitors may not conduct such an attack themselves, due to the potential trackability of such actions and the potential backlash on reputation from customers, the industry and regulators, organisations may profit from a nation-state sponsored campaign from their government in an attempt to give an edge to their local economy. Such campaigns though are only conducted when a sector's contribution to the

country's economy is significant and the potential gain outweigh the potential sanctions, official or not, the country may face, such as on its import of other goods.

Therefore, the likelihood of this scenario is **Medium** given the increasing frequency with which state actors are waging attacks.

H. Insurance perspective

- Risk assessment and recommendations
  - Cyber-risk assessment
    EAC undergoes regular internal and external cyber-assessments programs. Given the confidential nature of some of the activities of the company, the insurance companies will have access to assessment reports of non-confidential entities in Germany.

  - Estimated cost of potential losses
    Given the risk scenario, and the large repercussion from a contractual perspective in the aeronautics domain, the estimated cost of potential losses is set at **Very high** (see Table 12).

  - Recommended security controls
    EAC has already implemented all recommendable security control. No additional recommendations can be provided.

- Insurance policy 1
  The insurance policy in the scope of this risk scenarios is defined by the following elements:

  - Insured legal entity: European Aerospace Company, Germany.
  - Customer declaration elements: The customer has declared the value of the covered assets and, as well as the security measures taken as precautionary measures in the event of incidents impacting such assets.
  - Covered risks: Data loss, Product recall
  - Exclusions: 3rd party liability, and any other liability not specifically mentioned in the covered risks.
  - Endorsements: The cyber-insurance policy for European Aerospace Company is conditioned upon yearly risk assessments and any additional audits required by the insurance company prior to, and after the occurrence of, the risk events covered in the insurance policy.

- Insurance policy 2
  The insurance policy in the scope of this risk scenarios is defined by the following elements:

  - Insured legal entity: European Aerospace Company, Europe/Asia/U.S.
  - Customer declaration elements: The customer has declared the value of the covered assets and, as well as the security measures taken as precautionary measures in the event of incidents impacting such assets.

- Covered risks: Data loss, Property damage and personal injury, Media liability, Theft of money and securities.
- Exclusions: Risks related to military, spatial, and/or government-related activities and any other liability not specifically mentioned in the covered risks.
- Endorsements: The cyber-insurance policy for European Aerospace Company is conditioned upon yearly risk assessments and external independent audits required by the insurance company prior to, and after the occurrence of, the risk events covered in the insurance policy, including the regular audit programmes initiated by EAC.

- Covered loss
  - Revenue loss: Direct loss, Compensatory payments to customers and/or suppliers
  - Collateral expenses: Recovery expenses, Analysis and audit

- Premiums
  The insurance company offers legal advice in case of legal suits from 3rd parties following cyber-attacks which are identified as in scope of the insurance policy contract.

- Deductibles
  The insurance company will provide deductions conditioned to the subscription of additional insurance policies on property damage and personal injury. Such deductions will be proportional and up to 7% of the contract size of the additional insurance policies.

6. Scenario execution
   A. Involved threats
   - Actors and motivation

   B. Attack vector and execution
   - Vulnerabilities and tools
     - Open file-sharing folders,
     - CVE-2017-0143
     - CVE-2017-0144
     - CVE-2017-0145
     - CVE-2017-0146
     - CVE-2017-0147
     - CVE-2017-0148
   - Execution of the attack
     The first step may involve one of the following options:

     - Option 1: The attacker employs a phishing campaign to obtain access in the internal network through user machine,
     - Option 2: If an available 445 port is open, then the attacker can use it as a gateway for a foothold in the internal network.

Then the attacker proceeds with lateral movements to elevate privileges, e.g. through the Eternal family of exploits activated on unpatched internal assets, such as Windows 2003 servers, or by means of old legacy applications, default passwords, etc.

The attack follows through the targeting of e-mail servers or Active Directory to identify technical personnel and/or network administrators and thus to specifically target the production chain.

Finally, with the high-privilege role obtained, it becomes possible for the attacker to connect to the computer containing the Catia[56] design file, and thus alter it, resulting in final component being non-compliant with the initial specifications.

C. Identification and response process
The Identification and response process is the one described by Process ID #1 in Table 9, and illustrated in Figure 11.

D. Impacted assets
- The impacted assets are composed of the type Hardware: IT Infrastructures, and Production lines in Table 4.

E. Observed impact and loss
- The observed impacts include Product recall, and Loss or damage to physical properties, as per Table 7.
- Observed losses include: (i) Contractual and Regulatory loss under the Financial penalties category, (ii) Customer's loss due to Brand and reputation damage category, (iii) Interruption of provided services/products due to the Loss of competitivity and productivity category, and (iv) Recovery expenses, Analysis and audit expenses related to the Collateral expenses category, as per Table 12.

F. Post-attack insurance overview
- Audit and forensics
- Scope analysis of incurred loss
- A priori decision on insurance coverage

[56] Catia is a proprietary computer-aided design software from Dassault Systemes that is commonly used to design components.

8 Conclusion

This document has presented three scenarios: Scenario 1 describes a situation in which a cyber attack on a large company in the financial sector results in the loss of personally identifiable data for its customers. Scenario 2 presents a situation in which an SME in the professional services sector engages in insurance fraud; insider actors intentionally infect the company with ransomware so that they can claim a pay-out. Scenario 3 involves a cyber attack on a company that operates in the manufacturing sector – notably, making airplanes and satellites that it sells to a number of defence and military clients – that results in the alteration of manufacturing plans so that the final product is not compliant with the initial specifications. These scenarios were chosen in order to present a broad cross-section of possibilities.

They build on the use cases set out in Part I, which are themselves based on based on the analysis of the value chain for a company and its associated assets. These scenarios will then be used in order to assess the risk calculation methodology and toolbox, and also to make it possible to incorporate the behavioural components into this methodology.