TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Simo Hurttila 165605IVCM

FROM INFORMATION SECURITY TO CYBER SECURITY MANAGEMENT – ISO 27001 & 27032 APPROACH

Master's thesis (ITC70LT)

Supervisor: Andro Kull
PhD

Tallinn 2018

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Simo Hurttila 165605IVCM

INFOTURBEST KÜBERTURBE HALDUSENI – LÄHENEMINE VASTAVALT STANDARDITELE ISO 27001 JA 27032

Magistritöö (ITC70LT)

Juhendaja: Andro Kull
PhD

Tallinn 2018

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Simo Antero Hurttila

22.4.2018

Abstract

Term cyber security has been obfuscated by mainstreaming many of the ICT and information security issues under this single umbrella term. ISO/IEC 27001:2013 as an all-industry standard for information security provides countermeasures to mitigate risks to information-based assets in a defined scope, leaving cyber security guidelines introduced by the ISO/IEC 27032:2012 seemingly obsolete because of the before mentioned obfuscation. This thesis argues that terms information security and cyber security cannot be used interchangeably and understanding the fundamental differences between both security domains is inevitable in order to implement efficient cyber security controls. Analysing the unique characteristics of cyber space and cyber security from the standardized point of view has led this thesis to a conclusion and a set of process proposals where the cyber security management is recommended to be included as part of an information security management system. This thesis provides a framework for a standard-based understanding of cyber space and cyber security helping organizations to identify and analyse key stakeholders (their characteristics and dependencies) and cyber security assets of high interest with their unique characteristics introduced by placing the information-based (and non-information-based) assets to cyber space. The groundwork presented in this thesis within the before mentioned areas of focus will efficiently and eventually guide the actual implementation process to a successful identification of risks unique to cyber space.

This thesis is written in English and is 93 pages long, including 10 chapters, 18 figures, 7 tables and 5 appendixes.

Annotatsioon

Infoturbest küberturbe halduseni – lähenemine vastavalt standarditele ISO 27001 ja 27032

Mõiste küberturvalisus on saanud ühe üldtermini alla IKT ja infoturbe küsimuste liigitamise tõttu moonutatud. Kogu infoturbe sektorit puudutav standard ISO/IEC 27001:2013 sätestab konkreetselt määratletud ulatuses vastumeetmed teabepõhisele varale avalduvate riskide leevendamiseks, kujutades standardis ISO/IEC 27032:2012 toodud küberturbega seotud juhiseid ülalnimetatud moonutuse tõttu iganenuna. Käesolevas lõputöös väidetakse, et mõisteid infoturve ja küberturve ei saa kasutada üksteise sünonüümidena ning mõlema turvadomeeni põhimõtteliste erinevuste mõistmine on tõhusate küberturbe kontrollimeetmete rakendamisel möödapääsmatu. Käesolevas lõputöös on analüüsitud küberruumi ja küberturbe unikaalseid omadusi standardiseeritud vaatepunktist ning toodud välja protsessisoovitused küberturbe halduse integreerimiseks infoturbe haldussüsteemi. Käesolev lõputöö esitab raamistiku küberruumi ja küberturbe standardipõhiseks mõistmiseks, aidates seeläbi organisatsioonidel tuvastada ja analüüsida peamisi sidusrühmi (nende omadusi ja sõltumisi) ning unikaalsete omaduste poolest suurt huvi äratavaid küberturbe varasid, mis on tekitatud teabepõhiste (ja mitte-teabepõhiste) varade küberruumi panemisega. Käesolevas lõputöös toodud alused eelnimetatud fookusalas suunavad tõhusalt ja viivad tegeliku rakendusprotsessi küberruumile omaste riskide eduka tuvastamiseni.

Lõputöö on kirjutatud inglise keeles ja koosneb 93 leheküljest, sealhulgas 10 peatükist, 18 joonisest, 7 tabelist ja 5 lisast.

List of abbreviations and terms

ISO	International Organization for Standardization
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
ICT	Information and Communications Technology
ISMS	Information Security Management System
CIA	Confidentiality, Integrity, Availability
IT	Information Technology
CERT	Computer Emergency Response Team
RMM	Resilience Management Model
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
NIST	National Institute of Standards and Technology
ENISA	European Union Agency for Network and Information Security
ISACA	Information Systems Audit and Control Association
CI	Critical Infrastructure
MITRE	MITRE Corporation
CVE	Common Vulnerabilities and Exposures
ITU	International Telecommunications Union
CIS	Commonwealth of Independent States
CBL	Composite Blocking Lists
CIIP	Critical Information Infrastructure Protection
CII	Critical Information Infrastructure
DPA	Data Protection Authority
EU GDPR	European Union General Data Protection Regulation
NIS	The EU Directive on security of network and information systems
ISP	Internet Service Provider
ASP	Application Service Provider
FICORA	Finnish Communications Regulatory Authority

RASCI	Responsible, Accountable, Support, Consulted, Informed
IPO	Information Providing Organization
IRO	Information Receiving Organization
ADM	Asset Definition and Management
SEI	Software Engineering Institute
DHS	Department of Homeland Security
R&D	Research and Development
IP	Intellectual Property
IoT	Internet of Things
DNS	Domain Name System
IP	Internet Protocol
SLA	Service Level Agreement

Table of contents

List of figures

List of tables

1 Introduction

The primary objective of the ISO/IEC 27001:2013 standard (hereafter, the information security standard) is to secure the valuable information assets by implementing an information security management system – ISMS for short [1]. The ISO/IEC 27032:2012 (hereafter, the cyber security standard) on the other hand can be seen as a set of security guidelines and controls for a larger scope, the cyber space[1], that is not fully under the influence or control of the ISMS itself [2]. The information owned and controlled by the organization is not the only asset to protect in this case – it can be almost anything that can be reached via cyber space [3]. Thus it is vital to find the key limitations in the traditional information security in order to be able to point out the actual opportunities and weaknesses in the standardized cyber security approach. In the present world, the threats in cyber space are quickly becoming threats to the information assets under the ISMS but those new generation threats might not only have a direct impact on the classical paradigm of information confidentiality, integrity and availability[2]. Therefore, the traditional ISMS will soon run short in protecting the most valuable assets for the organization and broader, still practical, framework for analysing and dealing with a variety of rapidly evolving threats in cyber space must be created. The general problem with the international standards is that they are usually very vague so they would be adaptable, in theory, to most of the industries out there. This will also make the transition from the theory to practice very difficult for most of the organizations.

First, a problem statement is introduced with an applicable research and validation method, including an area of contribution and a look into the already available literature. A short intro is made to the particular cyber security standard. After that, reader's cyber security vigilance is being activated by diving into the current global attack surface

[1] 'Complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form.' [2].

[2] The CIA paradigm [1].

presenting information regarding current trends in sources of risks in cyber space, followed by an analysis of theoretical differences between information and cyber security, and the primary security domains involved in this work. The areas of contribution (stakeholders and assets) are presented with a practical mid-to-high level approach supporting organization's implementation of the cyber security standard, maintaining the international applicability of the guidelines at the same time. Proposed methods regarding stakeholder and asset identification and analysis are tested on a generalized environment, and corresponding tools and frameworks introduced to help the implementation process and integration of cyber security management as part of an existing ISMS. This all results in a definition and testing of a stakeholder-asset-dependency framework, also leading into a differentiating definition of cyber security asset, and its divergence to a pure information asset. At the end of the work, everything is brought together as a summary and a set of pre-filled tables, sheets, and process diagrams are provided for planning and implementing these guidelines.

2 Audience

This thesis is targeted to people who are interested in or responsible for governing information and cyber security in an organization that is providing services in cyber space, excluding Internet Service Providers as they are generally heavily regulated by local laws and therefore would undermine the purpose of this research to be internationally applicable. Previous knowledge regarding Information Security Management System (ISMS) that has been build based on the ISO/IEC 27001:2013 is required. General understanding of threats and risks to information security and cyber security is required. It is also assumed that the organization has already implemented an ISMS based on the ISO/IEC 27001:2013 standard with the majority of the controls in the Annex A, and may consider this thesis as a stepping stone towards cyber security management. The types of organizations that are suitable for absorbing the information this thesis provides would be the ones mostly providing a variety of digital services (not necessarily only IT services), using a variety of modern technologies to enable business, brand, and presence online.

3 About the work

3.1 Problem statement and hypothesis

The term cyber security has been obfuscated by mainstreaming many of the ICT and information security issues under the umbrella term of the cyber security. The popularisation of the term itself has been mostly done by the mass media [4]. The increasing amount of data breaches has accelerated the process [5] due to more visibility in the mass media. Moreover, the rising trend has been supported by the branding of the vulnerabilities in recent years [6]. The current situation now is where all of the domains of security (Figure 6) have started to overlap and melt together exceedingly and therefore slowly obfuscating, mixing and scattering the fundamental understanding of cyber space and cyber security at the same time. However, this thesis' purpose is not to try to redefine the fundamentals of cyber space or cyber security.

This thesis argues that the cyber security as a security domain differs from the other security domains (Figure 5), such as information security domain which is the base domain for this work, and these terms cannot be used interchangeably within the international standards to efficiently identify and manage threats. The fundamental understanding of each security domain, especially the information and cyber security domain, is a prerequisite to a successful implementation of the ISO/IEC 27001:2013 and the ISO/IEC 27032:2012 standards. The ISO/IEC 27032:2012 standard, as a set of high-level processes and guidelines, do not specify the requirements enough in order to efficiently identify the relevant stakeholders and assets relevant to cyber security. This will make the mentioned cyber security standard seemingly obsolete mostly because of the quality and amount of security controls available already in the ISO/IEC 27001:2013 standard. This will undermine the effects and slow down the adoption of the cyber security standard to practically make cyber space more secure.

3.2 Literature review

This work has received its groundwork mostly from the two international standards directly, as they set the requirements for an ISMS and propose guidelines and security controls for implementation to mitigate risks. Academic research sources are used whenever a fundamental knowledge has been acquired, such as definitions and analysis of topics around key terms. This area also includes the contribution of knowledge made available by the CERT Program (especially the Resilience Management Model, RMM) under the Carnegie Mellon University's Software Engineering Institute, which is also the major contributor towards the OCTAVE method. NIST and ENISA have provided valuable guidelines in the area of protecting the nations' interests and supporting the continental cyber security strategies.

Lack of information has been acknowledged to reside in the areas of foundational academic research around cyber security and cyber space. The existing research mostly focuses on problems emphasized by the increasing use of cyber space, forgetting to study the fundamental and unique characteristics of cyber space, therefore melting several security issues together and sitting them under one umbrella term known as cyber security. The lack of fundamental understanding of cyber security and cyber space among common security practitioners has supposedly resulted in a situation where practitioners believe that cyber security is an overly challenging problem for an IT department to handle and needs technologically advanced products to tackle those problems.

3.3 Methods and solution

This thesis will research gaps in a standardized approach between two security domains – information security and cyber security. The research method used relies on the foundations of information from academic resources and proposes new solutions in the most problematic areas in terms of identifying the stakeholders and assets that are relevant to cyber security, and where information security controls have little to no effect. The work in this thesis has successfully identified the problematic areas with proposals for resolution helping other industries, organizations, and businesses to move to establish stronger cyber security posture.

The research method used in this thesis is best described as a method where the environment being researched cannot be fully reproduced in a laboratory due to the complexity, uncertainty, and uncontrollability of an environment leading to a situation where a full experimental research is not possible. Results may not be fully reproducible in an external environment without certain bias. The underlying reason for this is that the research in this thesis relies mostly on the characteristics of cyber space that is accessed via the Internet, which is naturally an uncontrolled environment, and which has also lead to the initial need for cyber security. Therefore, this work forms a generalized environment to act as a common ground for the experimental research.

3.4 Validation

The validation of results has been carried out using best practices from the field in different types of industries to maintain the international applicability of this work. These best practices are supported by information and cyber security communities around the world, such as ISACA, Software Engineering Institute, ENISA, and NIST. The proposed solutions have been tested in theory in a generalized environment, still leaning towards a more practical direction if compared to the contents of the original cyber security standard. The reason for this approach is originating from the characteristics of the international standard, which purpose is to be internationally applicable, leaving certain aspects unexplained or without adequate details. Validation of hypotheses in this work will go to a certain extent without removing the international applicability of the cyber security standard. The exact level of validation would require a fully controlled environment which would require the removal of the general applicability of the cyber security standard, and wouldn't therefore substantially contribute to the security of cyber space.

3.5 Contribution and future research

Contribution to this work has been made in the areas of understanding the stakeholders in cyber space and their interdependencies with differentiating the cyber security as its own domain also from the asset perspective. This helps organizations to understand cyber security as an independent domain that still has overlapping and strong connections to other security domains. Understanding the overlapping of domains and complex

interconnections ensures that organization's risk management process understands the unique characteristics of cyber space.

Future research in this field should focus on a truly experimental validation and testing of stakeholder analysis in a more controlled environment using real data acquired from a real organization based on the proposed analysis process. After that, carrying out an asset evaluation, analysis and experiment on top of the verified stakeholder analysis data, rather than relying on data and knowledge derived from the hypothetical environment, should be a logical step before moving into actual risk assessment and treatment activities.

4 About cyber security standards

The ISO/IEC 27032:2012 standard's purpose is to present guidelines and security controls at a high level to ensure better applicability internationally among many types of organizations, businesses, and industries [2]. This may sometimes heavily obfuscate the concept and make implementation process harder and even act as a divider with the decision if to proceed with the implementation at all. This thesis will act as a connection point (see Figure 1) between the types of organizations described in the audience section earlier and the actual international standard.

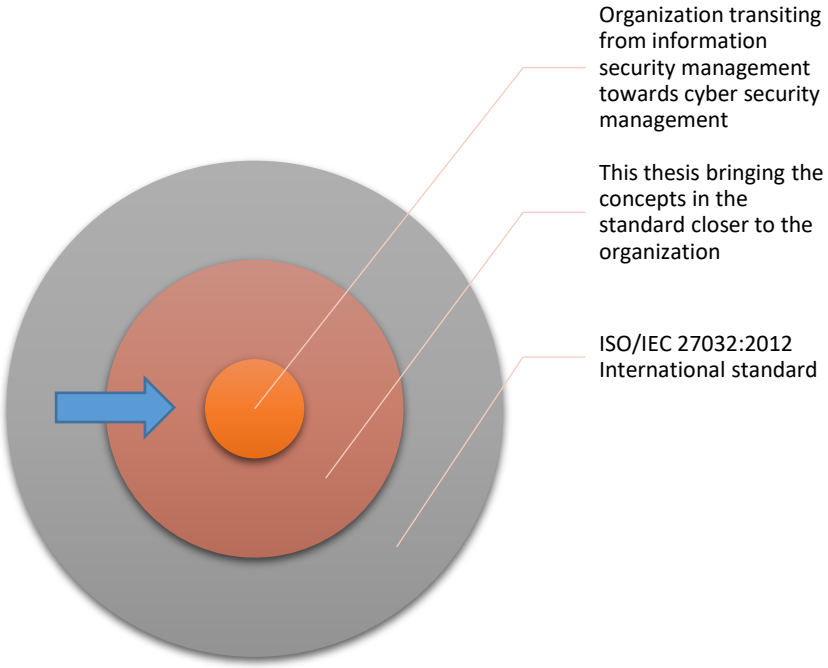


Figure 1. Hierarchy of this work.

The reason for choosing the ISO/IEC 27032:2012 standard as a base for this work is that the ISO/IEC 27001:2013 is widely adopted (+ 21 % increase from 2015 to 2016 [8]) among private organizations and has many connection points with the international cyber security standard as well (11.4.2.1 Information security management system [2]). The ISO/IEC 27032:2012 cyber security standard differentiates the cyber security from information security in a way that is suitable for private organizations to complement their information security posture and it does not pay too much attention to the critical

infrastructure (CI) protection. There are other cyber security guidelines that have been designed to help to protect the CI, such as NIST[1] cybersecurity framework [9]. This work will align itself also with the NIST cybersecurity framework – the five core functions of the mentioned framework are: Identify, Protect, Detect, Respond and Recover [10]. This thesis will partly cover the first core function of the NIST framework where the goal is to identify the environment and understand the organization, its assets, data and capabilities in order to effectively manage cyber security risks.

The ISO/IEC 27032:2012 standard has been recently compared with other cyber security standards by ENISA. They describe the mentioned cyber security standard as a voluntary, CIA-based standard where the involved assets origin in the cyber space, and which consists of information and cyber assets and threats to assets are either intentional or unintentional [4].

[1] NIST – National Institute of Standards and Technology

5 Cyber security and cyber space

> *'...cyber security can be defined as the protection of cyberspace itself, the electronic information, the ICTs that support cyberspace, and the users of cyberspace in their personal, societal and national capacity, including any of their interests, either tangible or intangible, that are vulnerable to attacks originating in cyberspace.' [3]*

In light of the above quote, the digital world, that is the cyber space, is a limitless environment without centralized control or governance, still vital to almost any nation and economy that exists [11]. The combination of the before mentioned attributes has led to a situation where economies and nations have found and fixed their presence in cyber space, while effectively promoting the benefits of this environment to miscreants or actors with lower moral principles. The appetite for protection of individuals and stakeholders in cyber space is stemming from the increase in cybercrime and the negative consequences it has to a wellbeing of an individual, society or a nation. It can be summarized that the virtual problems in cyber space have started to lead into more serious physical negative consequences in the real world as well. The unevenly distributed security in cyber space has been slowly introduced by the incoherent interests and information sharing among stakeholders operating in the cyber space, and the differentiating or non-existent level of governance by nations. The EU has a cyber security strategy in place promoting the openness of the Internet and policing their fundamental individual rights by ensuring safe and sound access to knowledge and information in the cyber space [11].

Cyber space, or cybernetic space, takes all the benefits (and negative aspects) of interconnected high-speed ICT (Information Communications Technology) systems

processing, storing, transmitting and presenting information and provides that information to be accessed by a physical entity, a human, in any location in that space. This has also led to a situation where the access to cyber space has become such a necessity (due to the psychological and economic reasons) that it already has started shaping how humans are building physical spaces (to support the access to cyber space via wireless Internet hotspots and outlets to power the devices used to connect to it). [12]

Although cyber security, according to the ISO/IEC 27032:2012 standard, is to preserve the confidentiality, integrity, and availability (CIA paradigm) of information residing in the cyber space, the standard also states that the security of the information may have additional requirements as well, such as authenticity, accountability, non-repudiation, and reliability [2].

6 Current global attack surface

As the businesses move to maximize their income utilizing the opportunities created by the Internet, they also have to publicly expose more and more services, systems and information about themselves in order to compete in this ever-changing field. We can express this phenomenon with a term "global attack surface" [13]. When the attack surface is expanding and increasing in density it will obviously result in a situation where the risks are also increasing as the businesses adopt the cost-efficient and resource-rich cloud platforms, and utilize the social media in communications with customers while building their brand. The security spending (median of 4 – 6 % from an IT budget in 2014 [14]) may not always match the inherent risks and threats by looking the yearly global losses of $400 billion estimated by the UK insurance company in 2015 [15]. We can also support the theory of increasing threats and risks by doing some simple statistical analysis based on the publicly available data. The following sub-headings will present the details with results. This information will act as a cornerstone in understanding the increasing size and density of the cyber space and sets pressure on organizations to start building better cyber security. The ENISA Threat Landscape 2017 report [16] summarizes the previous year's trends regarding the threats to cyber security, and is, therefore, a highly recommended reading parallel to this thesis.

6.1 Vulnerabilities

The figure (Figure 2) has been created using the MITRE CVE data [17]. Only the actual disclosed vulnerabilities have been included. The vulnerabilities that have been either reserved, rejected or disputed have been excluded from the numbers.

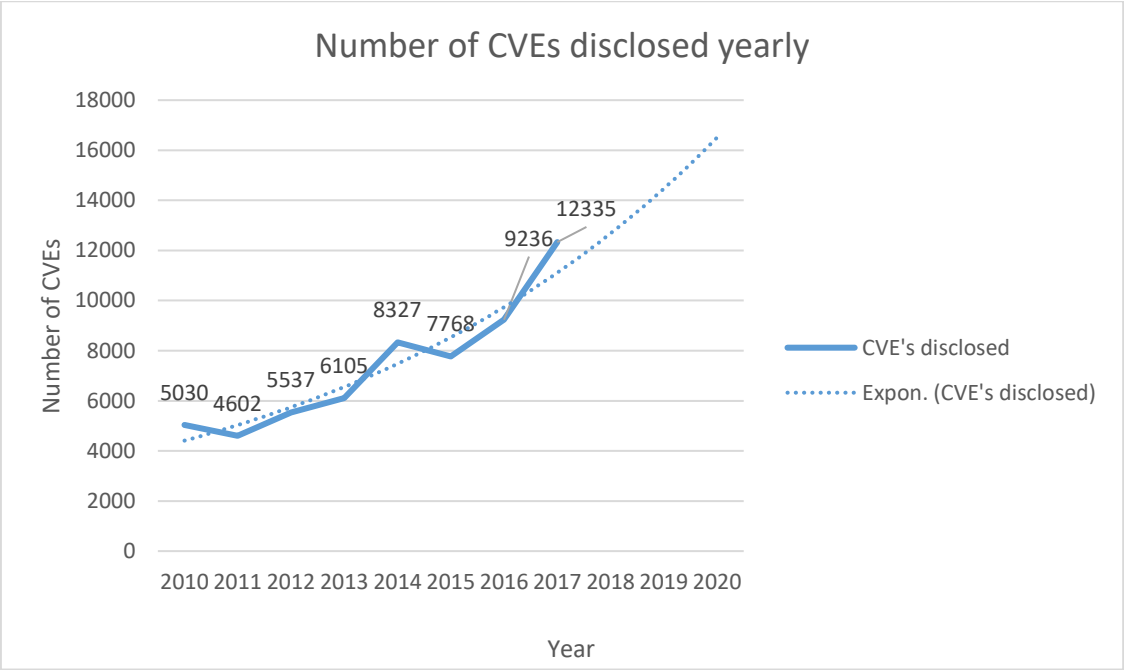


Figure 2. Number of CVE's disclosed yearly. Based on the data from MITRE [17]. The figure shows an exponential three-year forecast for the disclosed vulnerabilities.

By analysing the results, we can conclude that the vulnerabilities have been disclosed at an increasing rate for the past years. An exponential three-year forecast shows that the pace of vulnerability disclosure is most likely to increase. The ongoing and also the forecasted exponential increase in vulnerability disclosure cannot be answered with a single answer but the trend that support this is that technology is adopted at an increasing speed, which also enables us to investigate vulnerabilities more efficiently, but adopting new technology will also introduce new ones.

Statistics [18] show that the cyber security financing has been steadily increasing year to year with a slight drop in 2016 and in 2017 it is expected to hit the all-time record of $ 5 billion. Not all the investments were disclosed at the time when the statistics research was carried out. The amount of investments in 2017 is still a small portion when compared to the estimated losses caused by data breaches in 2015. Moreover, the current investments to new cyber security companies and technologies are expected to offer protection in cyber space with a certain amount of delay because of the research and development needed making the balance between losses and investments somewhat biased. Bug bounty program offered by HackerOne spent 16 % more money in 2016 in rewards for finding vulnerabilities and bugs in software and systems [19]. Therefore it is clear that new businesses and business models emerge that try to monetize the opportunity in many ways, which could also explain the steady increase in disclosed CVEs.

6.2 Internet users

ITU's Global And Regional ICT data from 2010 until 2017 [20] can be used to graph the number of individuals who have access to the internet.

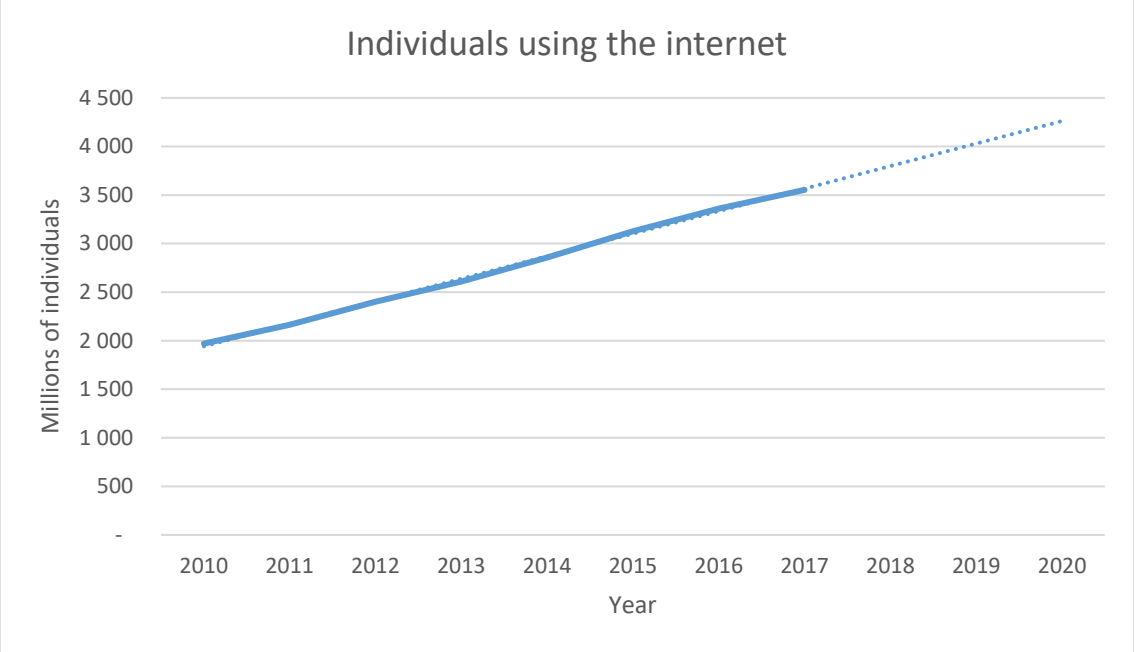


Figure 3. Individuals using the internet by year (solid line) with a linear three-year forecast (dotted line) [20].

As the amount of individuals using the internet is growing steadily, it is expected that it also increases the global attack surface.

According to another study [21], the cyber space is getting denser in the Southern and Eastern parts of our globe, meaning that the number of individuals using the Internet is increasingly getting higher in certain regions (see Table 1), a theory that the ITU data [20] also supports. We can calculate the increase per region based on that data. The results are shown in Table 1.

Table 1. Average increase (%) in individuals using the internet per region (2005 – 2017).

Region	Average increase (%) in individuals using the internet per region
Europe	5,1 %
Arab States	17,5 %
Asia & Pacific	15 %

CIS[1]	18,2 %
The Americas	6,3 %

What needs to be noted from this table, is the fact that the heavy increase in the number of individual Internet users is occurring in the regions where certain states may completely lack the policies and codes of conduct regarding the cyber space and cyber security, not to mention the possibility of lacking the basic fundamental (basic human rights, access to information, privacy, democracy, rule of law [11]) rights that have been more or less de facto for the Western countries including most countries in the Europe [21]. This also means that the corporate or state level cyber security strategies and policies enforced in the West are facing more and more threats from the "far ends" of more dense and uncontrolled cyber space where these national policies focusing on the interests of the nation itself do have little or no effect. Without proper cyber security policies and state level strategies the people in the developing countries with a heavy increase in the Internet use will pose a great threat to the whole cyber space – both from the victim's and attacker's perspective. It is, therefore, a vital precondition for a nation-state to have a cyber security strategy and necessary policies and laws in place in order for the organization operating from that nation to implement its own working cyber security strategy. Both entities have their own interests and therefore cannot share the same strategy. However, the actions taken by both the nation and organization support each other's safety and presence in cyber space.

6.3 Spam and websites

CBL's one of the larger email spam trap [22] recorded over 9000 emails per second in January 2018. Not all of them are spam, but the heavily fluctuating statistics can be used to correlate with active phishing and spam campaigns.

In May 2017, there were 1.8 billion websites alive according to Netcraft's Web Server Survey [23]. The number is up by approximately 800 % from May 2010 (0.2 billion) [24].

[1] CIS – Commonwealth of Independent States.

Numbers presented do not include the resources located in the dark web, which also introduces a serious threat to the cyber security.

In 2017, the top 5 prevalent threats included 4 different types of attacks all concerning with web servers, web applications and email abuse (spam and phishing) [16].

6.4 Net neutrality

Information available online enables many things, such as online learning. The fact that the cyber space is not heavily controlled has made it all possible. This has also provided certain side-effects, such as criminals using online services to facilitate their crimes. [11]

Recently, the neutrality of the Internet (net neutrality) has been under a heavy pressure, especially in the US [25]. More control over the information flowing through communications networks means more control over the people. With control over the information, an organization may face decreased interest in doing business over communication networks that cannot be fully trusted. It is an important part of a cyber security risk assessment process to evaluate how different nations fulfil the principle of net neutrality to properly protect the information important for the organization.

6.5 Data breaches

As new services emerge and are put available online, more personal and organizational information is exposed and left for the attackers to collect. These collections of data can be used to carry out further attacks to gain more information, which nowadays directly translates into money. Certain types of information are of greater interest to miscreants, such as virtual wallets used to store virtual currency such as Bitcoin. But this does not necessarily mean that attacking the target that is most interesting moneywise is the most profitable. We have seen attacks disclosing millions of records of personal data that have most likely resulted in a certain amount of privacy losses and other disturbing consequences [5].

Organizations capable of managing and protecting the business and personal data under their authority, with the organizations heavily violating the security principles, is making a colourful mixture which also affects the global attack surface. Some targets are easy

preys (the low-hanging fruits[1]), some are more protected and some in greater interests of attackers. The low-hanging fruit can be also located external to the target, such as a vendor providing products to the organization, and therefore introducing new attack vectors through supply-chains with less security. Targeted (attacker is motivated to attack a certain target) and untargeted (such as wildly spreading ransomware) attacks exploit those with a low level of security whereas more interesting targets with sufficient protection may be clear from the described data breaches. This makes the global attack surface somewhat unevenly distributed. It is also a goal of international standards [1] [2] to make the situation more even with proven methods, policies and processes which can be then adopted by the general public and organizations.

[1] https://en.oxforddictionaries.com/definition/us/low-hanging_fruit

7 How is cyber security different from information security?

7.1 Motivation

In order to reason the organizational transition, or ideology, from information security management towards cyber security management, it is necessary to understand the differences between these two. Obviously, information security and cyber security do not exclude each other – the meaning of transition from information security to cyber security is to rather complement each other and fortify the organization's security posture and to think information and cyber security management as one system [3]. From the standardization perspective, the ISO/IEC 27001:2013 can be considered to protect the organization owned information assets directly under the control of the organization [1]. However, as the cyber space is vast and spans across the whole globe, it presents threats and risks to assets that may not be directly controlled by the organization, but which can indirectly and negatively affect the organization as well. The traditional ISMS built and managed based on the ISO/IEC 27001:2013 may not be comprehensive enough to protect the assets in the cyber space.

7.2 Fundamentals

Threats that the cyber space uniquely introduces to the organization are researched in the following chapters. The following visualization (Figure 4) explains the fundamental difference between information security managed through the ISMS and the cyber space and cyber security. The scope of the ISMS has been set by the organization and may not consider all the relevant threats introduced by the evolving cyber space. The red arrows represent threats to the organization directly or indirectly affecting the assets controlled by, or in the interest of, the organization, eventually resulting in risks which may not be efficiently identified or managed by the ISMS.

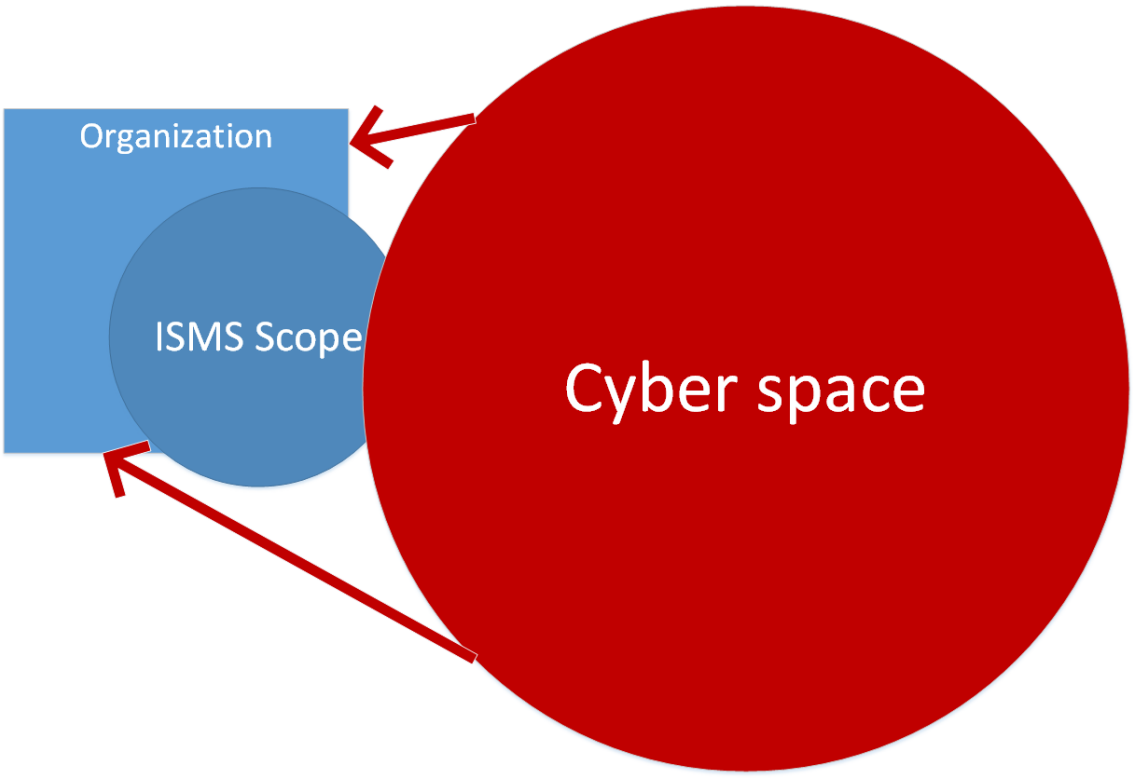


Figure 4. Information security vs. cyber security.

7.3 Common grounds

As a research shows, the common ground for the computer security is the security provided with the use of ICT. On top of ICT, there is information security, which is information or data transmitted either by the use of the ICT, on paper or when people are talking to each other. Information security relies on the security of the ICT whenever the information is transmitted or stored by the use of ICT. There can be other types of information as well that does not rely on the ICT. Similarly, with cyber security, there can be information or data that is either transmitted or stored by the use of ICT and secured both by ICT and information security. However, non-information-based assets (stakeholders and their interests [2]) are the things making the most difference to information security, although the information assets transmitted or stored by the ICT still needs to be considered as a fundamental part of cyber security. These non-information-based assets in cyber space benefit increasingly from the use and existence of ICT making them indirectly vulnerable via ICT to threats in cyber space. The following figure summarizes these three security domains and their common grounds. [3]

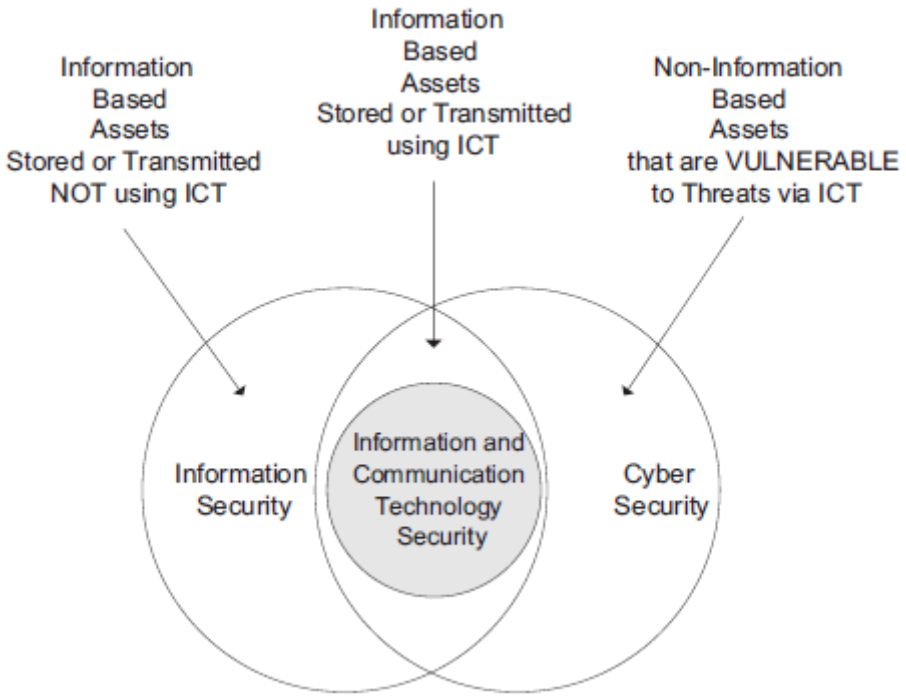


Figure 5. The relationship between information and communication technology security, information security, and cyber security [3].

7.4 Security domains explained

The following security domains have been summarized based on the research's [3] security domains (information, ICT and cyber security). In addition to the previously mentioned three security domains, the domains listed in the ISO/IEC 27032:2012 standard [2] are application, network, internet security and CIIP[1] domains. CIIP domain is considered to be an important part in terms of cyber security and has been therefore chosen to be introduced below in addition to the three domains presented in the research [3].

7.4.1 Cyber security

As a study argues [3], the primary goal of cyber security is not to secure the whole cyber space, but instead, to secure the interests (assets) of entities (person, society or nation) that are using the services provided by the cyber space. The study also argues [3] that the ICT and the information are the reason for the vulnerabilities that are exploited in the

[1] CIIP – Critical Information Infrastructure Protection [2].

cyber space, which on the other hand makes the cyber space less secure. This is evidently true if we consider the nature of the information and the ICT in the cyber space. The information and ICT itself make all the attacks feasible, and when organizations and individuals are exposing their information by the use of ICT to be able to better compete and receive services, they actually make new vulnerabilities to be exploited by the attackers.

Assets, vulnerabilities, and threats relevant to cyber security can be summarized as:

- Assets (stemming from the interests of stakeholders) are tangible or intangible, virtual or physical, personal or organizational and includes the societal values, people, their interests, and national infrastructure [2] [3].

- Information is a vulnerability that directly impacts assets, and use of ICT creates new vulnerabilities [3].

- Threats are malware infections, web-based attacks, web application attacks, phishing, spam, denial of service attacks, ransomware attacks, botnets, data breaches, identity theft [16].

7.4.2 Information security

In information security, the information is separated from the underlying ICT systems, and value is only regarded on that information [3]. Therefore, the assets to be protected can be either tangible (information on paper) or intangible (information presented in digital format) when compared to ICT security where the assets can be only physical [3]. If we consider a scenario where an information asset is being processed by an ICT system, and we suddenly take all the information (excluding the program designed to process information) out of that system for good, the existence of that system cannot be reasoned anymore. It has been initially designed to process information. Therefore, the information itself can be considered as an asset that is providing intelligence and operating instructions to ICT systems, and in light of the previous statement, also intelligence to modern businesses similarly.

Examples of assets, vulnerabilities, and threats are:

- Assets are considered to be information-based, transmitted using ICT, on paper and over speech [3].

- Vulnerabilities are for example related to weaknesses in access control [1], which usually relies heavily on ICT security.

- Example threat is an unauthorized disclosure of confidential information, which has been defined in the relevant standard by the characteristics of information to be protected (CIA paradigm) [1].

7.4.3 ICT Security

ICT security is the security of systems that produce, maintain, and aid transmitting information, such as computers (including their software), servers, routers and all hardware related to networks [26]. If we consider the attributes of confidentiality, integrity, and availability of ICT assets, it can be reasoned that the confidentiality of an ICT asset (for example a laptop) is not a rational value to protect. In this case, the asset is physical, so the confidentiality is only valid when the ICT asset contains, processes and presents an information asset. With integrity, however, it is possible to describe and appreciate the physical integrity of an ICT asset. Finally, the most important attribute for an ICT asset can be concluded to be availability. Unavailability of an ICT asset overshadows the availability of any other type of asset.

Examples of assets, vulnerabilities, and threats are:

- Assets are the technology (devices and systems) that are used to transmit and store information [3].

- Vulnerability in an ICT asset is for example related to a design weakness on the system.

- Example threat is an environmental threat where the operating temperature is either too low or high.

7.4.4 CIIP

Although the ISO/IEC 27032:2012 standard explicitly mentions that the CIIP is not addressed (2.2 Limitations [2]), it still pays attention to it from the dependencies to other

security domains point of view. This thesis will consider CIIP as an important part of cyber space security. Infrastructure that is enabling the connectivity to the cyber space is a valuable asset (and a business enabler) that is considered to be external to the organization and often out of control by the organization. It is of high importance for an organization to understand the connectivity to the cyber space from the Internet Service Provider's (ISP) point of view and what controls they have implemented to protect the availability of that connectivity.

Examples of assets, vulnerabilities, and threats are:

- CII assets are the infrastructure operated by critical infrastructure (CI) providers, such as energy and telecommunication providers [2], public administrative agencies and justice system [27].

- Vulnerabilities are stemming from the fact that especially the governments and military are consolidating their information infrastructures as part of a system operated and managed by commercial providers, connecting these information infrastructures directly to the common untrusted ground, the cyber space, by the use of ICT [27].

- These cyber related vulnerabilities are topped with the '*increased interdependency combined with greater operational complexity*' which introduces yet another threat dimension from the physical world – technical problems, human errors and natural hazards [27].

- Threats to CII assets are cyber crime, terrorism, warfare, natural hazards, human error and technical problems, or a combination of these [27].

7.5 Conclusion

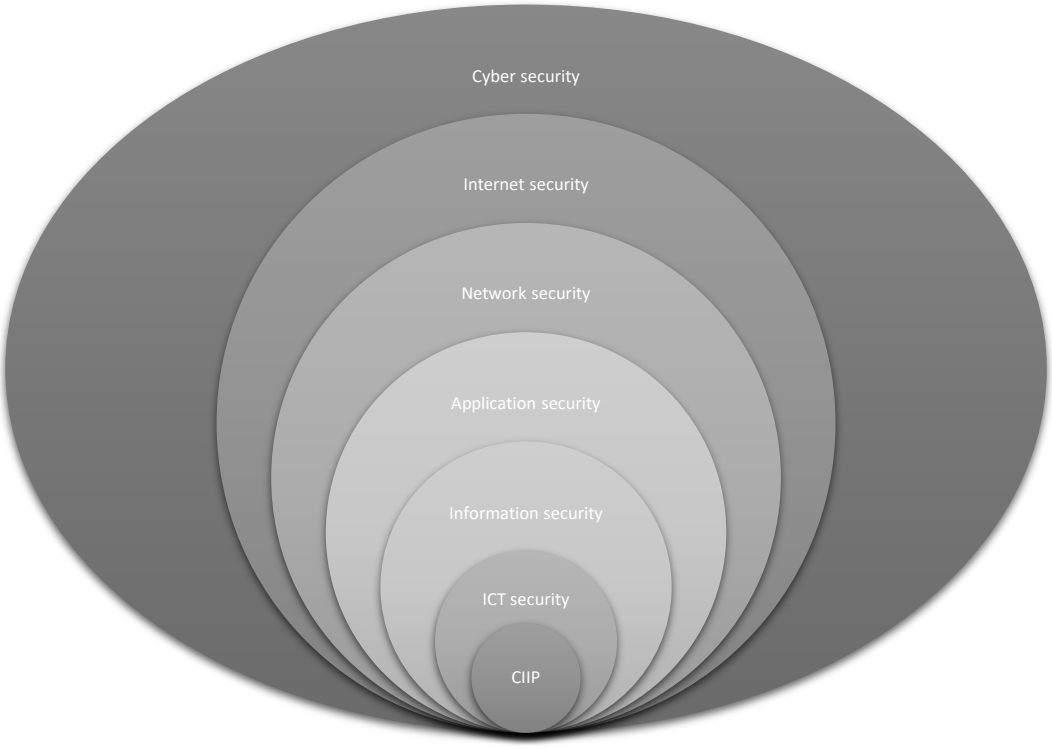


Figure 6. Seven overlapping domains of security. [2] [3]

Figure 6 visualizes these overlapping domains of security. Referring to the previously summarized security domains we can conclude that if the underlying domain is breached, it generally means that all the overlaying domains are compromised as well. If the information security is not capable of protecting the data from unauthorized disclosure, then the overlying domains are not most likely be able to cover this deficiency. The security is incrementally built from the bottom-most domain (CIIP) up to the top-most domain (cyber security).

Human has been considered as the weakest link in at least the ICT security domain for a long period [3]. The equipment used for communicating the information across networks operate through fixed instructions, and the behaviour and consequences of that communication are generally predictable and homogeneous. However, the nature of human makes the ICT equipment vulnerable to deviations in terms of secure and predictable operation, resulting in the human to be considered as a threat to the ICT security [3]. On the contrary, human operating in cyber space may take another role in addition to being a threat to the security. In cyber space, a human easily becomes an asset to protect, which is not the case in terms of ICT security [3]. When we consider the

bottom-most security domain (CIIP) the human is considered as a threat to the security, but when we move upwards, the human starts slowly adopting another role as well, which is an asset to be protected in at least information and cyber security domains. In information security, a human can be considered an asset from the knowledge and skills point of view – being a valuable asset to the organization that wants to protect the information and skills that the individual carries with him/her [3]. In cyber space, the situation is somewhat different. Human in cyber space will be moved away from the scope of information security and placed in a more broader scope where the human as an asset is protected both for his/her value in terms of information important for the organization, but also for his/her individual characteristics outside the organization, such as personal and online identity [3] [2]. Still, these previously introduced analyses do not exclude the human from being a threat to the security of information and cyber space as well [3].

8 Stakeholders

A stakeholder is a business term [28] and describes an entity that has an interest in an organization. The actions taken by the organization (both public or private) can have an effect on the stakeholder, and vice versa. From the ISO/IEC 27032:2012 standard's point of view, an organization is different from a government [2].

The ISO/IEC 27001:2013 standard sees stakeholders as parties that have an interest in an organization (clause 4.2 [1]). They are therefore called as "interested parties" in the context of the mentioned information security standard. Taking the previously mentioned statements into account, with a statement from a research [3] arguing that the interests of stakeholders in cyber space needs to be protected, we can come up with a deduction that identifying the stakeholders and their characteristics is a critical prerequisite in order to understand their interests. From interests, we can extract the concrete assets relevant to stakeholders.

From the business and project management perspective, the investigation of the organization's environment aims to provide information and knowledge how the identified stakeholders (with their characteristics, capabilities, and priorities set by their importance) may be taken advantage of in the strategic decision-making [29]. The business environment, especially when in connection with the cyber space, is likely changing constantly, resulting in a situation where the stakeholders' interests vary over time. Such an example is the advent of DPAs[1] in the wake of EU GDPR[2]. The DPA is an authoritative stakeholder in cyber space whose interests have strong influences in an organization in the near future in terms of administrative penalties due to possible personal data breaches [30]. Moreover, the same source [29] explains that the characteristics of stakeholders drive managers to come up with strategies (whereas strategies are driven by policies) to control the influence of stakeholders, whether they are neutralizing, mobilizing or defeating the organization's objectives. These statements

[1] DPA – Data Protection Authorities. [60]

[2] The EU GDPR – European Union General Data Protection Regulation. [30]

walk hand in hand with the ISO/IEC 27032:2012 standard as it also proposes the use of policies (12.5.2 Policies [2]) to manage risks that are introduced by the varying interests of stakeholders. The stakeholder analysis is also a common tool related to policy research in political sciences, making the topic helpful to cyber security practitioners as well [29].

Typical stakeholders for an organization are its employees, customers, and investors [28]. However, a government can be seen also as a stakeholder. The reasoning for this is that laws and regulations set by governments will likely have an effect on the organization's behaviour and could even open new business opportunities. Third party suppliers have an interest in distributing their products through the organization, which may rely its core business functions on these supplier relationships.

The ISO/IEC 27032:2012 standard divides the stakeholders into two main categories – consumers and providers [2]. The important thing to understand, that also originates from the complex characteristics of the cyber space itself, is that an organization providing products in the cyber space will not only adopt a single role of provider or consumer [2]. Instead, the organization providing a product to be used in the cyber space will very likely rely on the products provided by other organizations. This also means that the organization, as an initial provider, will also be a consumer of other products. This will make the connections in cyber space between consumers and providers rather complex, and they need to be properly addressed and investigated in order to be able to form a comprehensive risk assessment [2]. An organization may use products from other providers in the process of developing their own product, and this way become part of that ecosystem where all these provider and consumer connections may produce new hybrid risks that are then inherited by the organizations taking part in these product trades. The hierarchy of stakeholders has been visualized in a mind map in a relation to other functional areas of cyber space and can be found in the "Appendix 1 – Cyber space visualization".

It can be argued if the hacker can be considered a stakeholder in the cyber space. From the general definition of a stakeholder [24], a hacker would be a stakeholder in a cyber space, but from the ISO/IEC 27032:2012 standard's point of view [2], it does not fit into the provider or consumer role trouble-free and violates also the fact that the standard considers stakeholders as those who are safeguarding the assets of their interest. The hacker that is defending his or her assets from the threats posed by cyber space can be

naively considered as a stakeholder and will be therefore included in the stakeholder identification process. For the sake of clarity the hacker in the context of this thesis will be the one with only offensive or destructive intentions against assets owned by the others in the cyber space, thus not contributing to the overall security of the cyber space. In light of the previous analysis, we will include the hackers as a stakeholder only in an educational manner – to remind that certain special stakeholders' goals can be totally incoherent with the organization's goals where inherent risks must be treated through a risk management process.

8.1 Stakeholder analysis

8.1.1 Process

This thesis proposes a process to be used in analysing stakeholders and their interdependencies. The objective of the process is to come up with a list of stakeholders that can be quantitatively ranked, making it more suitable to analyse and value them in the risk assessment phase. This knowledge can be also used in the information sharing activities to determine the most efficient and influential communication channels. The process proposal is based on the fundamental steps presented in the previously analysed review paper regarding stakeholder analysis [29].

- Roles:
    - Determine if the stakeholder adopts a role of individual, group or organization [29], where the group is considered to consist of multiple individuals and an organization (private or public) is as specified in the standard [2].
    - Quantify the role (individual = 1, group = 3, organization = 5).
- Relationships:
    - Willingness to mobilize resources towards a particular goal (motivation) [29], where the common goal, in this case, is to make cyber space more secure.
        - Quantify the motivation (low = 1, medium = 3, high = 5).

    - Relationship to the desired outcome (influence) [29] is the stakeholder's capability to drive change towards the agreed goal.
        - Quantify the influence (defeating = -5, neutralizing = 0, mobilizing = 5).

- Interests [2]:
    - Describe in what way the stakeholder is interested in an organization.
- Interdependencies with other stakeholders:
    - List the primary and secondary stakeholder for each stakeholder and analyse the most critical interdependencies based on the count of all interdependencies.

The rank of the stakeholder can be calculated from the size of the group derived from the role with a certain level of motivation and capability to influence in the security of cyber space. Attributes' weights are set so that role is set to 20 %, motivation 30 % and influence 50 %. The tool that is used to visualize these attributes with a basic summary function with mentioned weightings is called LineUp. The tool can be used to visualize and rank homogenous multi-attribute data sets [31]. An example Excel sheet that is available in the "Appendix 3 – Stakeholder analysis" contains the data (role, motivation, influence) for each stakeholder. The tool uses the data in the Excel file (exported to the tool as a CSV file). All these values are estimates and they must be derived from actual entities operating from and within the nation, and their willingness to participate building better cyber security. Indicators are for example a national cyber security strategy and regulations, and if authorities have set comprehensive rules and responsibilities for the actors under their influence. For example, European Commission has established a cyber security strategy [11], directive (NIS [32]) on the security of network and information systems, and a regulation for personal data protection (EU GDPR [30]) making them highly motivated and influential in terms of enhancing security in cyber space.

The following non-exhaustive list sourced from the standard (7 Stakeholders in the Cyberspace [2]) and enriched with an example stakeholder analysis based on the previously described process (including the data in Appendix 3 – Stakeholder analysis)

presents a set of stakeholders that should be considered in an organization when planning and developing cyber security:

- Investors and shareholders,
- Organization's employees,
- Internet Service Providers (ISPs) [2],
- Application Service Providers (ASPs) [2],
- Customers,
- Government and regulatory authorities,
- Suppliers,
- Critical Information Infrastructure (CII) providers,
- Hackers.

8.1.2 An example case of stakeholder relations

Methods of attacking various supply chains [25] have come to a light recently. Although supply chain attacks have been carried out successfully by exploiting a compromised software or network of a supplier [33], many opportunities are available for carrying out the same in the physical products' supply and mass-manufacturing chains, such as injecting keylogger software to physical products at the time of manufacturing [34].

Supply chains can be considered introducing risks to business through external parties (also known as stakeholders). Therefore the CERT Program by Carnegie Mellon University is also talking about the external dependencies management instead of supply chains. The main concern of a supply chain from an organisational point of view is an integrity of the provider's hardware, software, and staff [35]. This is the situation when the organization is outsourcing its ICT functions to third parties. The risks related to external dependencies, or supply chains, has to be managed the same way as risks relevant to any other security domain. The reason why supply chain risks management falls back to the cyber security is simply that the assets relevant to the supply chain are outside the scope of the other security domains.

The figure (Figure 7) depicts an example of the previously described supply chain attack with some of the stakeholders operating in the cyber space. Organization A may not assess and manage the risks inherited from the relationships with the suppliers. The vulnerable product is published and delivered to a customer who is then exploited by the hacker. This situation may arise when proper security controls and policies are missing from the Organization A. Although the ISO/IEC 27001:2013 standard has a suitable control (A.15.1.3 Information and communication technology supply chain [1]) for mitigating the risks introduced by supply chains, it may not consider the complex relationships regarding the stakeholders and their assets in the cyber space, not to mention any collaterals caused by such attacks.

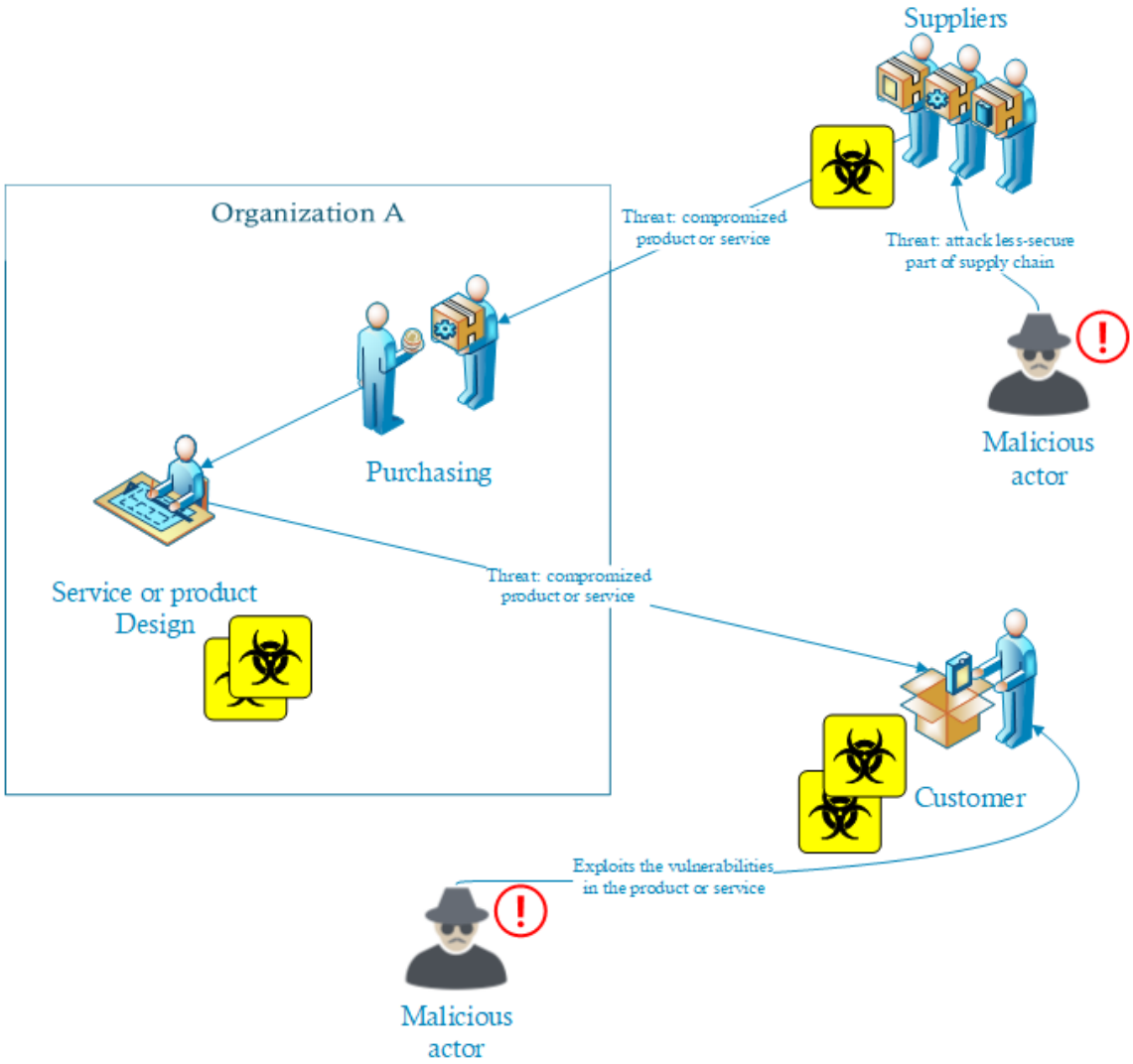


Figure 7. Stakeholders, malicious actors and a supply chain attack.

Similar situation, but in a different direction, may occur when the Organization A decides to serve their product on a shared cloud platform where the inherent risks arise from the fact that the platform itself may have vulnerabilities (or even intentionally built functions that allow the platform owner to eavesdrop traffic or transactions) and the organization may not have capabilities or power to mitigate them. According to ENISA, additional emerging supply chain attacks in 2017 involved tampered browser extensions and plugins [16]. A noteworthy thing to consider is also that the customer in the figure (Figure 6) can be also a private or public organization who has its own customer base. The supply chain can be and usually is more complex as is presented in the figure for clarity.

8.2 Analysing the results

By analysing the stakeholder ranks presented in the figure below, a conclusion can be drawn regarding a generalized organization (Organization A). The most important stakeholders to co-operate with are Internet Service Providers, government and the regulatory authorities, investors and shareholders and the CII providers. Also, two of these previously mentioned stakeholders share the densest dependencies among other stakeholders – Internet Service Providers and CII providers (Appendix 3 – Stakeholder analysis). These can be considered the two stakeholders that introduce most of the threats to the continuity of the business and its processes and the risks corresponding to these threats must be controlled through a risk management process.

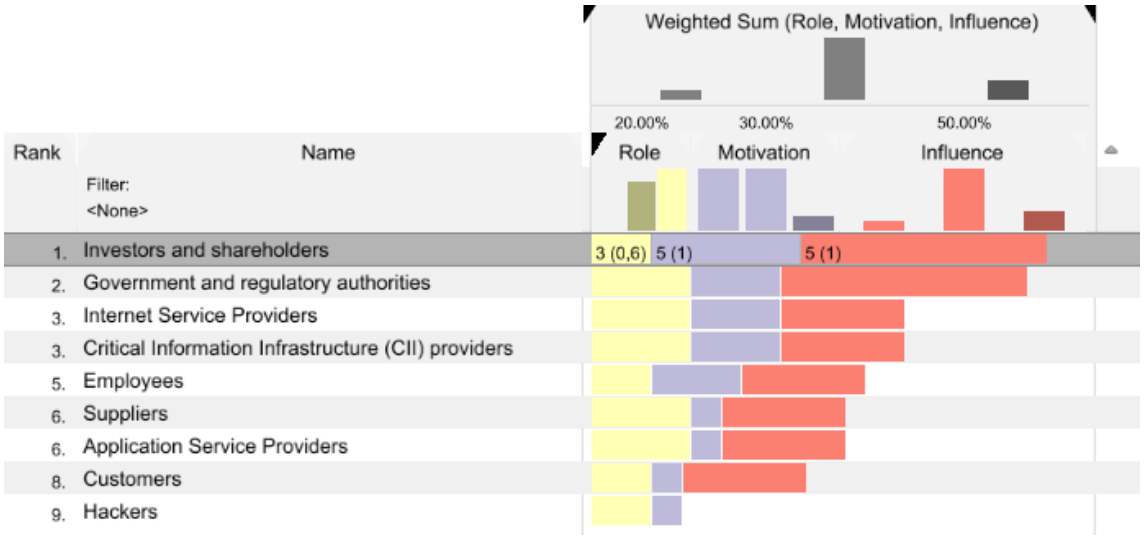


Figure 8. Stakeholder ranks calculated with the LineUp tool from the data presented in the Excel file (Appendix 3 – Stakeholder analysis).

In the figure (Figure 8) the stakeholders with highest ranks (1-3) are strongly aligned with the common goal of improving the security of cyber space. In contrast, the stakeholders with low ranks (5-8) are not primarily interested in the security of cyber space, and can be said as a light argument to introduce most of the vulnerabilities and threats to the security of cyber space. The hacker is ranked with the lowest rank and must be understood as a pure threat to cyber security without practical capability or willingness to contribute to the security of the cyber space directly. A hacker, in this case, can be considered an umbrella term for all miscreants in cyber space. In this example situation, cyber security policies to manage stakeholders in cyber space would be most beneficial and efficient when enforced against the low-to-mid (5-8) ranked stakeholders, where the motivation and capability to influence towards common goal, is rather low. If the stakeholders cannot influence positively towards a common goal, they must be controlled. The high-end ranked stakeholders are therefore more difficult to be managed through cyber security policies as they would already have a strong motivation and influence capabilities to drive change in cyber space (for their own interests coherent with the given organization), making management of these stakeholders inefficient. However, these stakeholders participate in critical roles in public-private partnerships regarding information sharing and incident coordination.

8.3 Transferring the results to ISMS

Integrating the cyber security management into the Information Security Management System (ISMS) makes sense in terms of manageability. One solid system to manage both information and cyber security risks will most likely be beneficial not only in terms of resource use but also from the assets manageability and risk assessment point of view. Most of the assets protected under the cyber security domain are genuinely based on information, which is also proved later in this thesis. Rest of the assets, such as interests of stakeholders and non-information-based assets can be easily integrated as part of the risk management process by these guidelines (9.5 Transferring the results to ISMS) when the place of stakeholders in the ISMS has been fully understood and documented in relation to the interested parties that have been already identified as a requirement originating from the information security standard [1].

8.3.1 Understanding the roles and responsibilities of stakeholders

In the context of the information security standard, interested parties receive confidence in how well the organization manages their information security risks [1]. An interested party should only care about the organization's risks management process' performance if the interested party has a genuine interest in that organization. Examples are a shareholder or an employee who both are interested in the financial wellbeing of an organization – one to receive value for his/her shares and one to receive steady income as salary. These interested parties can be said to set indirect requirements to protect the valuable information assets of an organization in order to safeguard their own interests.

Likewise, the stakeholders share lots of similarities with interested parties. Stakeholders consist of organisations and individuals and should be considered to be consolidated together with the ISMS' interested parties as they both have aligned interests (or stakes) in an organization and they both set similar requirements in terms of enhancing security (excluding Hackers whose interests are colliding with the rest). Therefore, we define interested parties analogous to stakeholders. However, important differentiator to consider and remember is that interested parties have interests in the context of an ISMS' scope, whereas the stakeholders have complex stakes in the context of the whole cyber space due to the characteristics of the Internet. This will also result in a situation where the assets of interest will be somewhat different, and those differences are analysed more in detail in the later sections.

Still, there are certain exceptions and additions introduced by cyber security standard that should be documented under an ISMS, in more detail as part of an ISMS scope documentation [1]. The reason for this is that the interests, or stakes, of the identified entities, may not be all equal, as was analysed before, and specific needs and characteristics should be documented for clarity. Roles of stakeholders in cyber space can be roughly divided into two categories – consumers and providers [2]. A stakeholder who is a consumer can be either an individual or an organization. They consume the services provided within the cyber space. Stakeholders adopting a role of the provider are usually organizations who are offering online services in cyber space (Application Service Providers), and services to connect to the cyber space, such as Internet Service Providers [2]. The area of focus in this work is an organization, whether it be a consumer or a provider of services.

An organization who is consuming services in cyber space has limited capabilities in influencing to the actual state of security in cyber space and the services they consume, limiting the role to more or less to an information coordinator and manager of cyber security risks relevant to the assets it has defined critically valuable [2]. It must be reminded that an organization can be a consumer and a provider at the same time. It depends on the service whether the organization is consuming or providing it. An organization is consuming a service in cyber space when it allows its employees (a stakeholder) to access and use externally provided and managed service in the cyber space, such as a social media platform. In this particular case, the provider (Application Service Provider which is also a stakeholder) is responsible for the security of the platform, and consumers (employees of the organization) must be made aware of the risks inherent in the use of that particular platform by both the provider and the organization as a consumer. Still, the primary responsibility for managing cyber security risks in this scenario falls back to the organization, and eventually to the employee him/herself.

An organization who is providing services in cyber space is either facilitating the users' access to the cyber space by providing services and equipment for that purpose, such as Internet Service Providers [2]. Also, Application Service Providers are considered as providers of services in cyber space [2]. These providers enable organizations and individual consumers to access and interact with the services hosted in cyber space. The providers have more control over the security of their products and services and therefore are entitled to deliver secure products and services, guidance to consumers and sharing information with other providers and consumers [2]. A provider most likely will adopt a role of the organizational consumer as well adopting the same expectations as set to consumers [2]. A provider may also have responsibilities set by the government and regulatory authorities, which are important to analyse in order to understand the expected level of security in their products and services. The following chapters analyse the ranked stakeholders (8.2 Analysing the results) from the role point of view.

Investors and shareholders are mainly individual consumers. Their stakes consider the financials of an organization making them indirectly capable and motivated to steer the organization's strategy towards better cyber security posture.

Government and regulatory authorities are mainly organizational consumers, but they will also set certain assurance on the level of security by legislations and regulations. In

addition to the government, the regulatory authorities can be DPAs or instances such as national CERTs. Their stakes concern the national security, including the security of cyber space, related networks, infrastructures, and citizens. A CERT function is not generally understood as a regulatory authority, but it is usually operating under the governance of a certain regulatory authority, such as the CERT-FI (Computer Emergency Response Team Finland) is governed by the FICORA[1] (Finnish Communications Regulatory Authority). It would be therefore reasonable to describe CERT functions as both consumers and providers of services in cyber space, where the providing role is considered more important in this context in terms of resolving a major cyber attack. Also, authorities (such as police) responsible for solving criminal activities in cyber space against an organization should be considered as both consumers and providers, where the providing role is considered more important in this context in terms of criminalizing a cyber attack.

Internet Service Providers (ISPs) are both consumers and providers serving as information carriers and connectivity-enablers while also consuming external services located in cyber space. They may, or may not, be under a governance of a regulatory authority. In Europe, ISPs are for example regulated by the "net neutrality" regulation that prevents ISPs from filtering and throttling the Internet traffic [36]. Internet Service Providers' stakes concern the subscriptions (customers) to Internet-related services. It is therefore important for them to maintain a certain level of trust through implementing security controls either integrated to the service directly or giving out knowledge and tools to the users to mitigate the risks [37].

Critical Infrastructure (CI) providers ensure the essential services for a nation, such as water, healthcare, energy and transport [27]. CI providers also provide the Critical Information Infrastructures (CIIs) that are the infrastructures and telecommunications networks to operate the CI using ICT-based control systems [38]. The CIs are of high importance to the national security, also meaning that the stakes of these providers are usually supported strongly by the national security strategies and policies to maintain the continuity of these essential services. Depending on a geographical location, CIIs may

[1] https://www.viestintavirasto.fi/en/ficora/presentationandduties.html

also rely heavily on the private-owned infrastructure (telecommunications networks) making their dependency on Internet Service Providers critical [27].

Employees of an organization are consumers of services in cyber space. Their stakes are mostly in protecting their identity from the threat of theft or misuse [2]. Employees are also considered to be the weakest link in the security chain and are therefore exploited first by criminals in order to gain access to the actual point of interest. Their capacity to influence in the security of cyber space is rather low, so protective measures, such as information security awareness program must be implemented. This section also includes customers as a stakeholder, which has same characteristics as employees.

Suppliers are both providers and consumers of services in cyber space. As was described earlier (8.1.2 Example case of stakeholder relations), the suppliers are proliferating as targets of supply-chain attacks. Suppliers may be threatened as a consumer of services in cyber space. Those threats are then rippled to their operations as providers. Their stakes are in selling services and products to manufacturers and therefore not directly related to security. Suppliers also include vendors of ICT equipment, software, and facility maintenance services – any services or products whether digital, non-digital, IT or non-IT that are needed to carry out day-to-day business activities, also including external services such as cloud computing and data hosting.

Application Service Providers (ASPs) are both providers and consumers of services in cyber space. Their stakes are similar to stakes regarding the supplier. They are also positioned in a similar situation making ASPs as targets of supply-chain attacks. It is also notable that the ASPs (social media platforms) may process and store large amounts of personal data.

8.3.2 Stakeholders as part of communication and information sharing process

Information presented in the previous section is used here to form a proposal and set up a communication and information sharing process that also supports the ISO/IEC 27001:2013 standard's requirement for internal and external communication relevant to the ISMS (requirement 7.4 Communication [1]). This proposal here injects the stakeholders and their primary roles as part of the communication process based on the previously mentioned requirement. A table (Appendix 4 – Communication and information sharing process (RASCI table) (RASCI – Responsible, Accountable,

Support, Consulted, Informed [39]) contains a proposal for both internal and external communication and information sharing. The communication tasks (left-most column) have been derived from the ISO/IEC 27032:2012 standard, particularly from the risk assessment and treatment chapter (11.2 Risk assessment and treatment) where the standard sets responsibilities towards stakeholders participating in cyber space. Security incident management has been added to these tasks because it is part of a control set available in the Annex A of ISO/IEC 27001:2013 standard (A.16.1.2 Reporting information security events [1]). The stakeholders (top-most row) have been derived from the stakeholder analysis presented in this thesis, in addition to the information security responsibilities and corresponding roles that are defined in the ISMS according to the requirement (5.3 Organizational roles, responsibilities and authorities [1]). IPO (Information Providing Organization) and IRO (Information Receiving Organization) describes the direction of communication and also reveals the type of organization regarding the potential opportunity to receive support (S) and consultancy (C) [2]. Rest of the principles regarding the framework for information sharing and coordination are presented in the standard (13 Framework of information sharing and coordination [2]).

The tasks listed on the left-most column are clarified in the list below:

- Acknowledgement – a task of understanding and communicating a scenario where a stakeholders' actions in cyber space may introduce risks to other stakeholders and their assets (11.2 Risk assessment and treatment [2]).

- Reporting – a task where certain external stakeholders must be included in the reporting of threats, incidents, and risks (11.2 Risk assessment and treatment [2]).

- Information sharing – a task where organization is actively sharing information regarding information security and cyber security (11.2 Risk assessment and treatment [2]).

- Security incident management – a task described in the previous paragraph [1].

- Risk assessment – a task that involves the analysis of risks introduced to the organization by the participation and actions of stakeholders in cyber space (11.2 Risk assessment and treatment [2]).

- Regulatory/Legislative – a task that considers the regulatory and legislative requirements regarding cyber space and involves the stakeholders in this process at least at an informational level (11.2 Risk assessment and treatment [2]).

8.4 Conclusion

It is unclear from the stakeholders' point of view how the roles and responsibilities for securing cyber space are accounted for. The reason for this is the lack of common rules, segregated interests and missing codes of conduct in cyber space. This section came into a conclusion that each stakeholder has a unique interest in operating cyber space, and therefore must be uniquely identified and analysed to understand their interests and to derive the relevant cyber security assets to be protected from the results. A process for quantifying attributes used in policymaking was introduced and applied. The results of this process were ranked with a tool to come up an ordered list based on the weighted values of the attributes. From that information, it is evident that certain stakeholders are more important than others, also taking account the interdependencies among all participants. High-end ranked stakeholders are strongly aligned with the common goal of making cyber space more secure, and therefore managing those stakeholders may be inefficient, but which are still crucial in terms of communication and information sharing. Mid-to-low-end ranked stakeholders were noticed to have less motivation and capability to influence in the state of cyber security, making these stakeholders to be ideally controlled by enforcing policies against them and increasing awareness in the area of information and cyber security. The mid-to-low-end stakeholders were also concluded to introduce most of the threats to the security of cyber space because of their lack of motivation towards a common goal.

Finally, and based on the results of stakeholder analysis, stakeholders were described in more detail from the role and responsibilities perspective – whether they adopt a role of consumer, provider or both. Integrating the acquired information into an existing ISMS is close to seamless as the stakeholders can be simply included with the existing interested parties as a documented information while contributing at the same time to the information security incident management process in terms of a proposed customized communication and information sharing process. A RASCI table was produced from all

the data acquired in this section to support strategic decision-making, information sharing, and risk assessment activities.

9 Assets

This chapter introduces the assets unique to the cyber space (derived from interests of stakeholders) and a process how to analyse the assets' criticalities through dependencies. From information security point of view, an asset is generally only considering a value of information under the control and scope of the information security management system (ISMS) [40]. More general view covering additional types of assets when compared to information assets only, and more applicable to the current understanding of cyber security, is that anything that has a value for an organization is an asset and needs to be protected, whether it be personal, organizational, virtual or physical asset [2]. Risk IT framework defines an asset as '*Something of either tangible or intangible value worth protecting, including people, information, infrastructure, finances and reputation*' [41]. Software Engineering Institute's work on this area at the Carnegie Mellon University summarises assets as '*basic units of value in the organization*' [42]. This should also support the strategy in the organization's risk assessment phase where measuring the change in security plays a major role in order to determine if the applied control is efficient and mature enough. If an asset has an estimated value, it can be measured, which makes the use of any qualitative risk assessment methodologies unreasonable (Chapter 2 – A measurement primer for cybersecurity [13]).

This chapter is aligned with the CERT Program's (by the Software Engineering Institute at the Carnegie Mellon University) Resilience Management Model (RMM) Process Area (version 1.2) and in more detail with its Asset Definition and Management (ADM) part [43]. However, the purpose of this thesis is not to elaborate the contents of the mentioned resource, but instead, find the useful linking with the cyber security standard and take high-level influence (implementation-wise) from the CERT Program to be used as a practical example in this thesis. The content and goals of the ADM that are covered in this chapter can be summarized as shown in the following list.

- Methodology and process to establish the organizational assets [43].
- Establish the relationship between assets and services [43].

9.1 Understanding the business

From the risk assessment perspective, it is a fundamental thing to understand the valuables (assets) (and the interconnections among them) that need protection from the threats originating from cyber space. According to the ISO/IEC 27001:2013, a process that is continuously assessing risks must be documented and implemented making it reasonable to include the assets that are concerned of cyber security as part of that existing documented process [1].

There are many methods to model core processes for an organization. This is also a recommended practical step in order to understand the interested parties and their interconnections in the context of the ISO/IEC 27001:2013 standard, which was also introduced earlier in the Stakeholders chapter. The analysis of the interested parties is also a requirement set by the information security standard (clause 4.2 [1]). This thesis will rely on a simple classical swimlane approach [44] with basic Microsoft Visio flowchart objects to identify the participating processes in an example organization where the business mission is being fulfilled by a service (as is called by the Software Engineering Institute [45]) that sells products to customers. The mission of the business is to generate revenue and value for shareholders. The input that is needed for the business process analysis is practically acquired (through workshops) from the staff of the organization at different levels (senior managers, operational area managers, general staff and information technology staff), as is proposed in electronic resource regarding the OCTAVE method (5.1 Overview of Processes 1 to 3 [46]).

Breaking down the organization's service (there can be many services) into logical departments divided by the swimlanes (horizontally) and different stages of the service delivery (vertically), we can analyse the importance of each logical department. A logical department is analogous to a business process in this context. By removing a certain horizontal swimlane (a business process) from the diagram (see the example diagram in "Appendix 2 – Business processes of Organization A") we will soon notice which processes are vital in terms of achieving the particular service. If we take away the external business process of supplying resources in order to produce new product, then the whole business mission is at risk. But if we take the internal support away then it may not greatly weaken the whole service but may undermine the mission of the organization

if other services in the same organization rely on this process more heavily. This way we can prioritize the processes and put more resources in protecting the more critical ones.

The modelling of the business processes do not reveal all the information that is needed to understand all the threats that the organization's assets may be facing in cyber space but it greatly helps in understanding the critical processes and their interconnections, revealing the underlying assets.

9.2 Categorization of assets

The service that was modelled using swimlanes (service is to sell products or services to the customer in order to achieve the business mission, which is to generate revenue and value for shareholders) is the top tier on the hierarchy of business. The service tier binds the underlying business processes and assets together with relationships, as is illustrated in the following figure [45]. The assets make the service possible through business processes. Every tier of this hierarchy should be considered as an asset itself where the bottom-most tier contains a variety of assets feeding the business process assets. It is therefore vital to start from the high-level analysis of the assets – hence the importance of understanding the mission, the services, modelling the business processes (service enablers) and finally going further from there to find the underlying assets. The following figure has been adjusted from the Software Engineering Institute's diagram in a way that the version in this thesis will consider all the objects and tiers of the diagram as assets where the bottom-most tier are the concrete assets especially of great interest to cyber security [45].

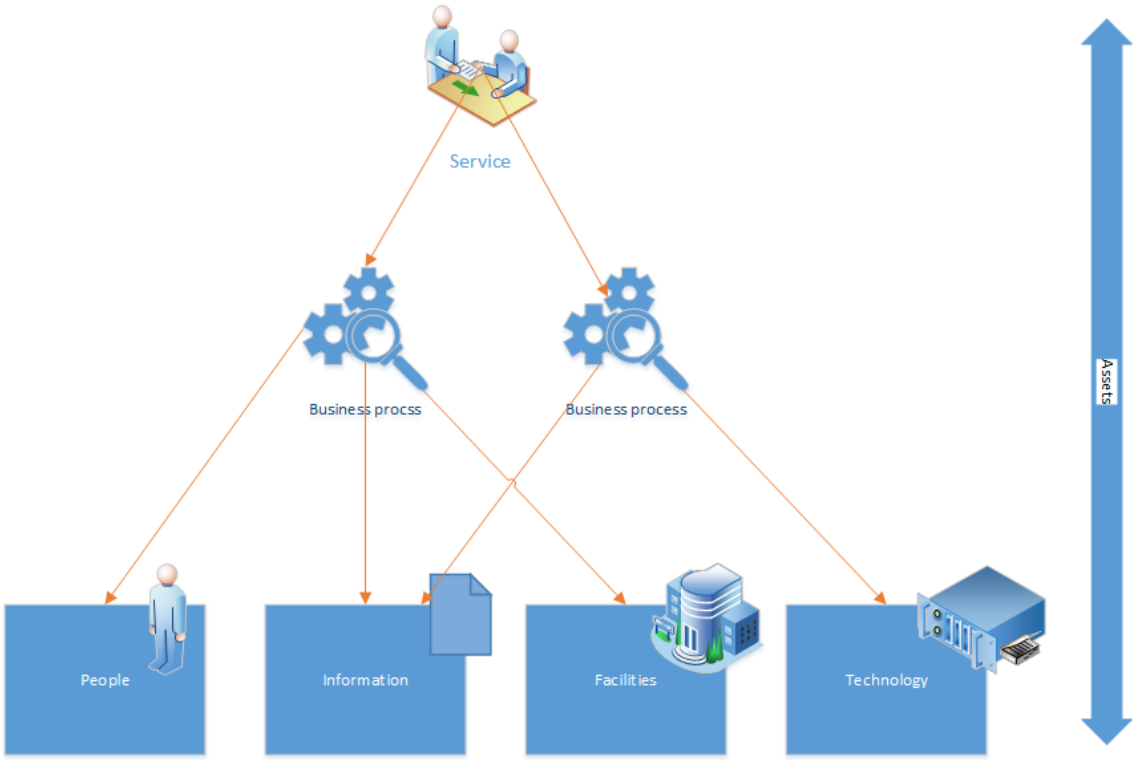


Figure 9. Asset hierarchy in an organization. The highest tier is called the Service tier. [45]

The Software Engineering Institute (SEI) separates the assets at the bottom-most tier into four different categories as shown in the figure (Figure 9). Not all the overlaying business processes depend on all of the underlying assets, similar to a service may not depend on all of the business processes. These categories are a rough division of assets [45]. These same categorizations can be more or less found from the ISO/IEC 27032:2012 standard as well (8 Assets in the Cyberspace [2]), still making the Software Engineering Institution's presentation more useful and comprehensive to be used in the context of cyber space because its direct contribution to OCTAVE and its threat profiles [47], which are helpful in modelling risk scenarios with actors and threats to assets.

Below non-exhaustive figure showcases some examples of assets in the cyber space based on the examples presented both in the ISO/IEC 27032:2012 [2] and the SEI's research [42] and enriches the contents with generalized organizational assets introduced to the cyber space after the publication of the standard, or if there has been a noticeable lack of examples in the standard's presentation of assets. The list does not include traditional assets relevant only to classical information security under a control of an ISMS, however, certain overlapping (domain-wise) assets such as business processes are presented here as they are an important part of identifying both cyber and information security assets.

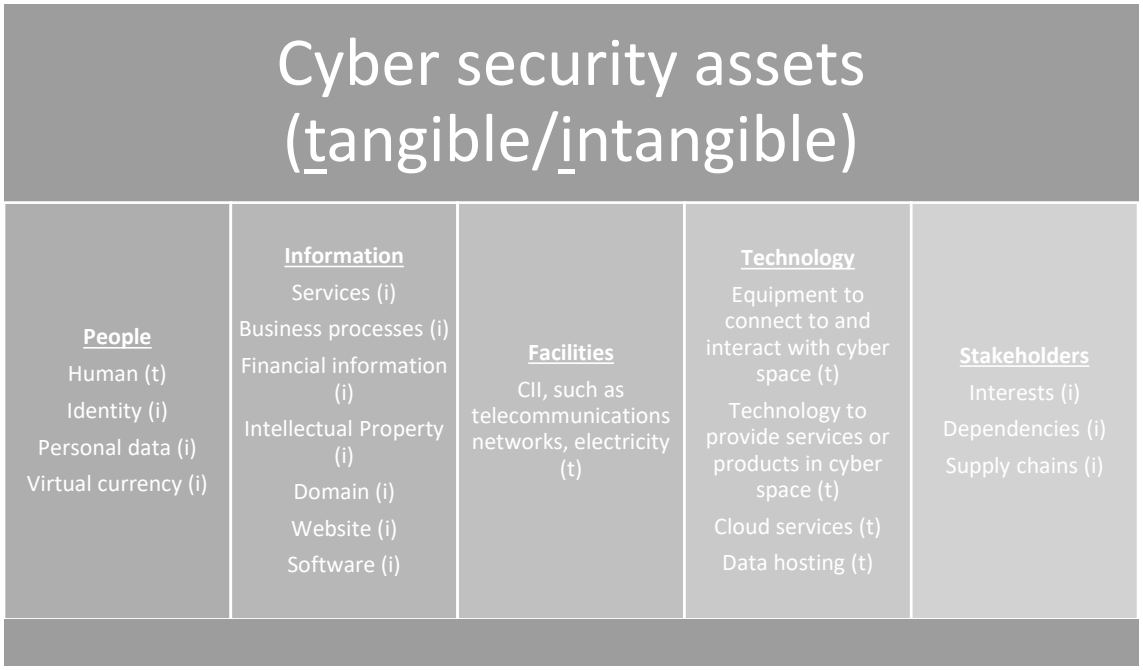


Figure 10. Example organizational cyber security assets based on the categorization presented by SEI [42] with an addition of "Stakeholders" category.

This thesis will focus on the organizational assets but will include the personal assets as well whenever they have a connection point to the organization, such as when an employee is allowed to bring his/her mobile phone to a workplace and accesses organization's resources with it [48]. Hence the "People" category in the above figure (Figure 10). People will be assets both from the organization's internal and external point of view because their certain assets, such as personal data and identity, are a shared responsibility with the individual himself, organization processing the personal data and the organization employing the individual.

The reason for adding a fifth category (Stakeholders) into the categorization of assets is because the SEI's framework is based on information assets only [42], and is now being adjusted to cyber security assets by this work. Even the U.S. Department of Homeland Security (DHS) with the collaboration of U.S. CERT Program has identified the growing appetite for assessing and mitigating complex supply chain related risks that are stemming from the external dependencies, also known as stakeholders [35].

9.3 Defining a high-level process

We shall come up with a formal process proposal from the previous analysis of assets relevant to cyber security. The process consists of the following phases and details are introduced after the list:

- Write down the organization's mission and consider it as an asset (each service fulfilling the organization's mission may be considered as an asset).
- Analyse how the organization is fulfilling that mission within the departments and functions to come up with the list of business processes – see "Appendix 2 – Business processes of Organization A".
- Analyse which underlying assets are being consumed by the business processes that make it possible to achieve the organization's mission.
- Draw up a model of the interdependencies between a service, its underlying business processes, and assets, which are introduced in detail in the following chapters:
    - Step 1 – analysing the assets of the Research & Development process.
    - Step 2 – differentiating the information security assets from cyber security assets.
    - Step 3 – consider the dependencies with stakeholders as assets.
- Prioritize the business processes, assets and stakeholder dependencies based on their criticality – if a certain process fails, does the whole mission or service fail? If a certain process fails, does it cause another process to fail? If a sub-asset fails, does it cause a business process to fail? If a stakeholder dependency is removed, does it cause a business process to fail?

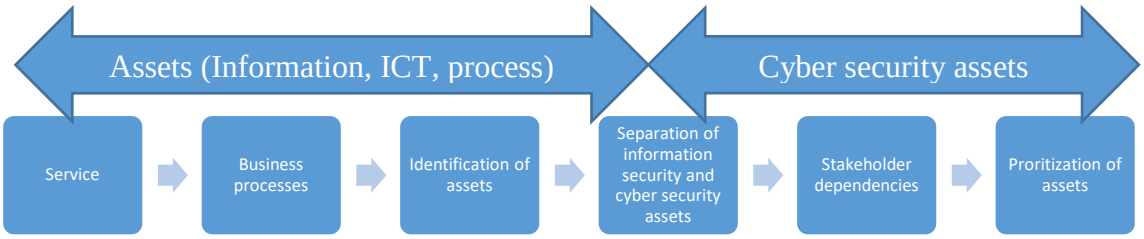


Figure 11. Asset evaluation flow.

The ISO/IEC 27001:2013 standard's control in Annex A (A.8.1.2 Ownership of assets [1]) requires that every asset protected has an owner. This may get complicated with complex relationships with assets owned externally (which is also one of the current key problems in cyber security [2]), but which still may have indirect impact or value to the organization. It is, therefore, a common sense, in certain cases, to set the owner based on the business process, rather than assigning an owner to each asset. Still, identifying and documenting the concrete assets consumed by the business processes is an important task and a prerequisite to fully accomplish the asset evaluation flow (Figure 8). The asset evaluation flow (Figure 8) is a summary of the asset identification and analysis process.

9.4 From business processes to underlying assets

After modelling the involved business processes in the "Understanding the business" chapter for the organization's service to sell products or services to the customer, the intent is to start breaking those processes apart to find the assets that make those processes functional. This topic is linked with the CERT-RMM ADM:SG2.SP1, which is also known as the "Associate assets with services" phase [43].

The internal research and development process for organization A will be used as an example.

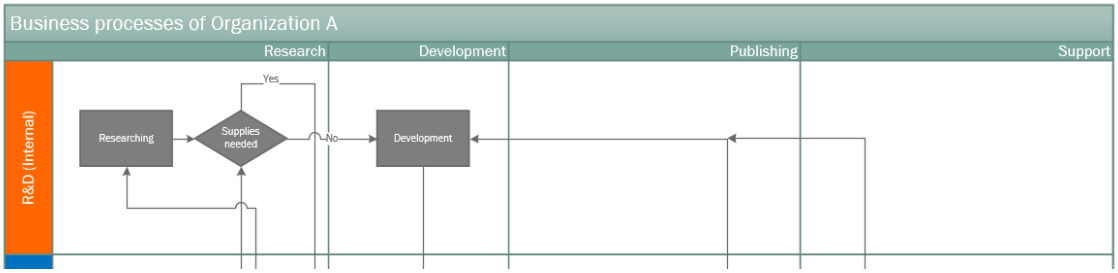


Figure 12. Internal research & development process of a service or product.

The lifecycle of the organization's service has been divided into four phases as vertical lanes – research, development, publishing, and support. Research and development process is involved only with the first two phases. Now we must start looking what are the assets necessary for the research and development department to actually come up with a new service or product. First, they will need input from the sales team to specify what kind of service or product has demand. They will also need to purchase services and products externally to be used to support the research and development phase. They also have existing assets that they are using, including computing systems and software, employees and information. We can conclude that the research and development process is relying on two other processes, which are the internal sales and the external supply process. However, the external process of customers buying the products or services cannot be excluded at this point as it is the power that sets everything in motion and makes it initially possible for the organization to achieve its mission and goals. In the context of cyber security, these three processes must be analysed from the point of view where the traditional information security has no effect. The chapter below introduces the process to analyse these dependencies between processes and assets according to the asset evaluation flow presented earlier.

9.4.1 Step 1 – analysing the assets of the Research & Development process

The following figure (Figure 13) has been formed to introduce the high-level assets involved in the research and development business process. The figure also shows the dependencies with other stakeholders including the critical internal and external business processes according to the business processes model in "Appendix 2 – Business processes of Organization A". The purpose of this step is to understand all of the assets that make these business processes work. At this point, there is no need to separate assets between information and cyber security assets. However, at this point, it is necessary to document if certain assets are being shared among multiple business processes or even services. Shared assets introduce more complex operational risks and must be therefore properly evaluated in order to understand their criticality and value from the multiple business processes or services perspective [43].

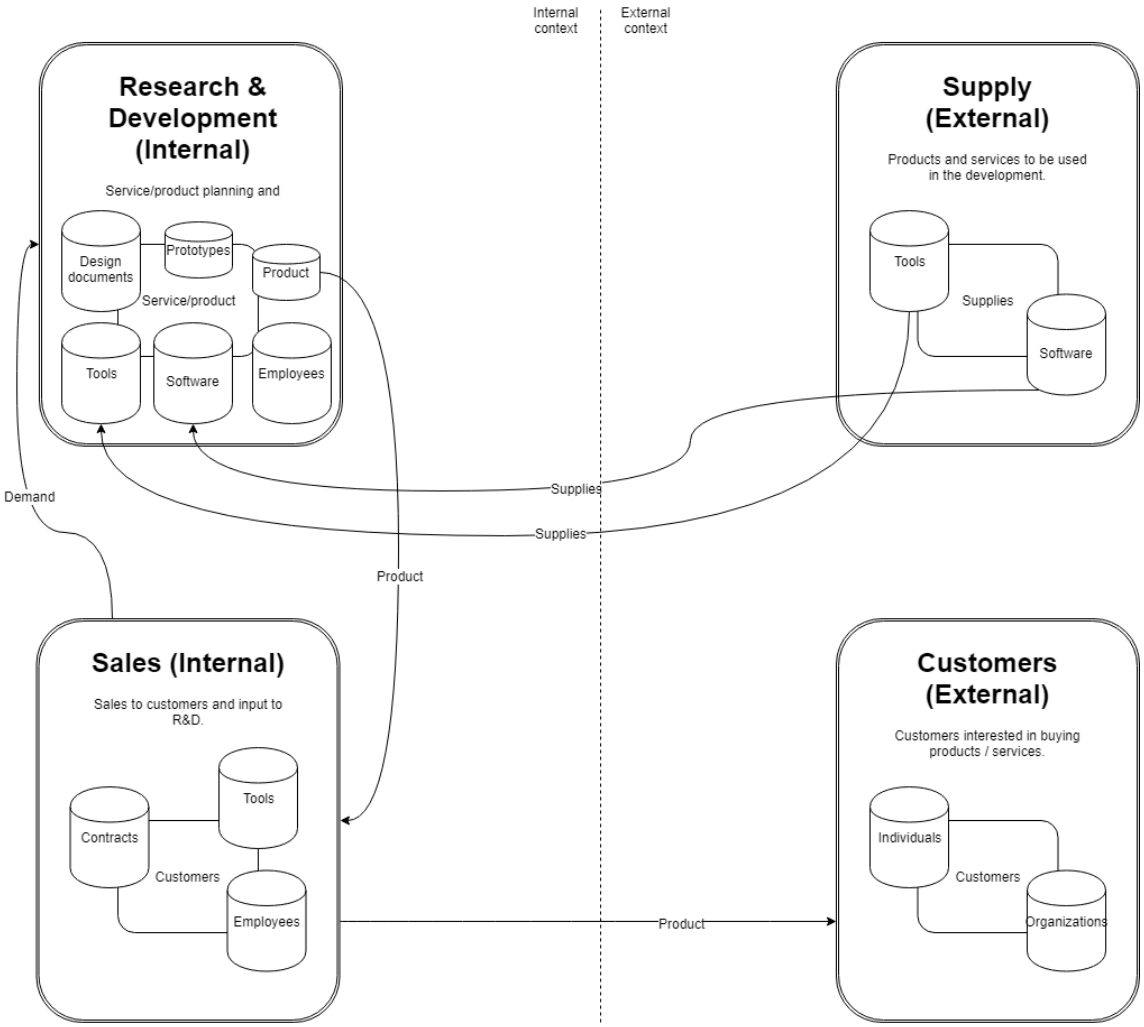


Figure 13. Critical internal and external business processes with high-level assets.

9.4.2 Step 2 – differentiating the information security assets from cyber security assets

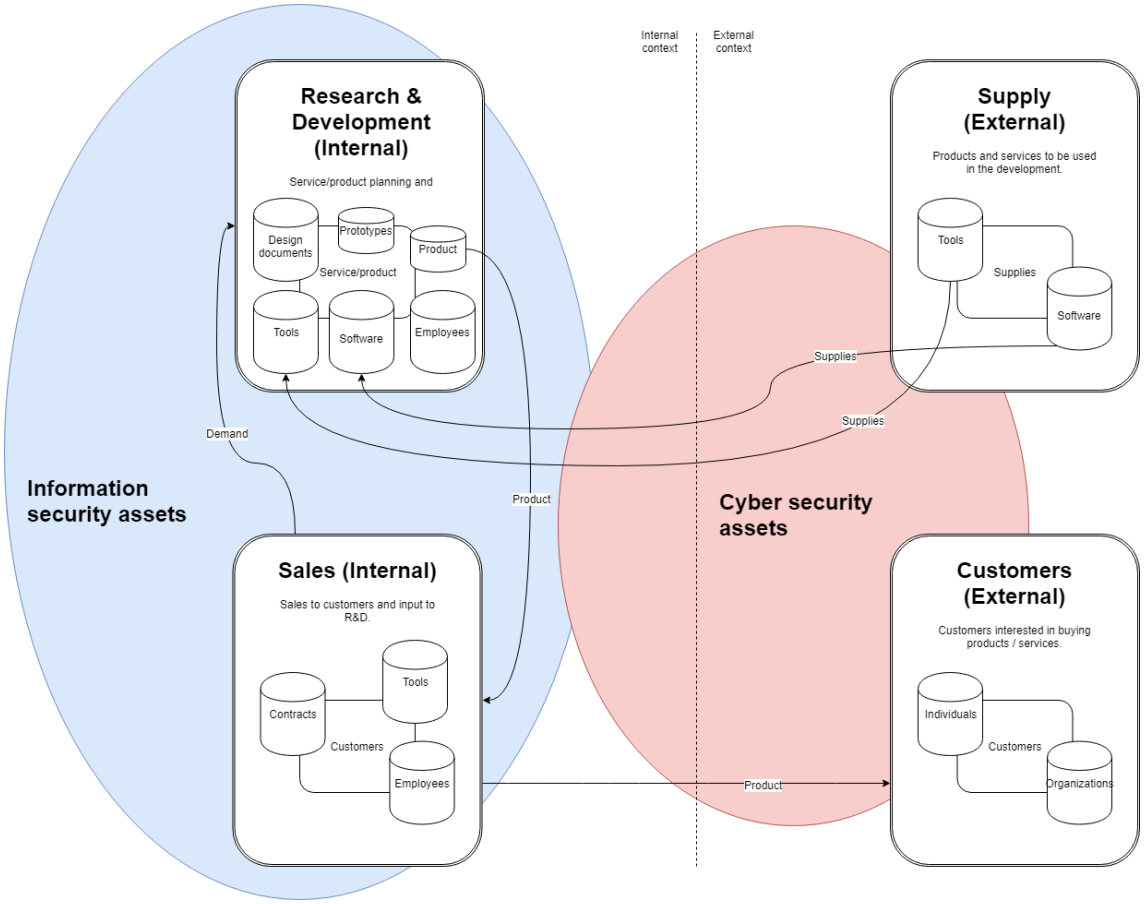


Figure 14. Critical internal and external business processes with high-level assets including information and cyber security domains.

The most relevant parts in understanding the cyber security assets in the context of the figure shown above are the processes of delivering the supplies from the external supplier to the organization A (an example organization) and selling a published product or service to the customer by the organization's sales process. The reason for this compartmentalization is that these business processes (supply, customers) will fail if the stakeholders (suppliers, customers) are taken out of the equation, which will have a direct negative impact on the organization's mission. Their stakes and underlying assets in cyber space that facilitate these processes are the cyber security assets of high interest in this particular study.

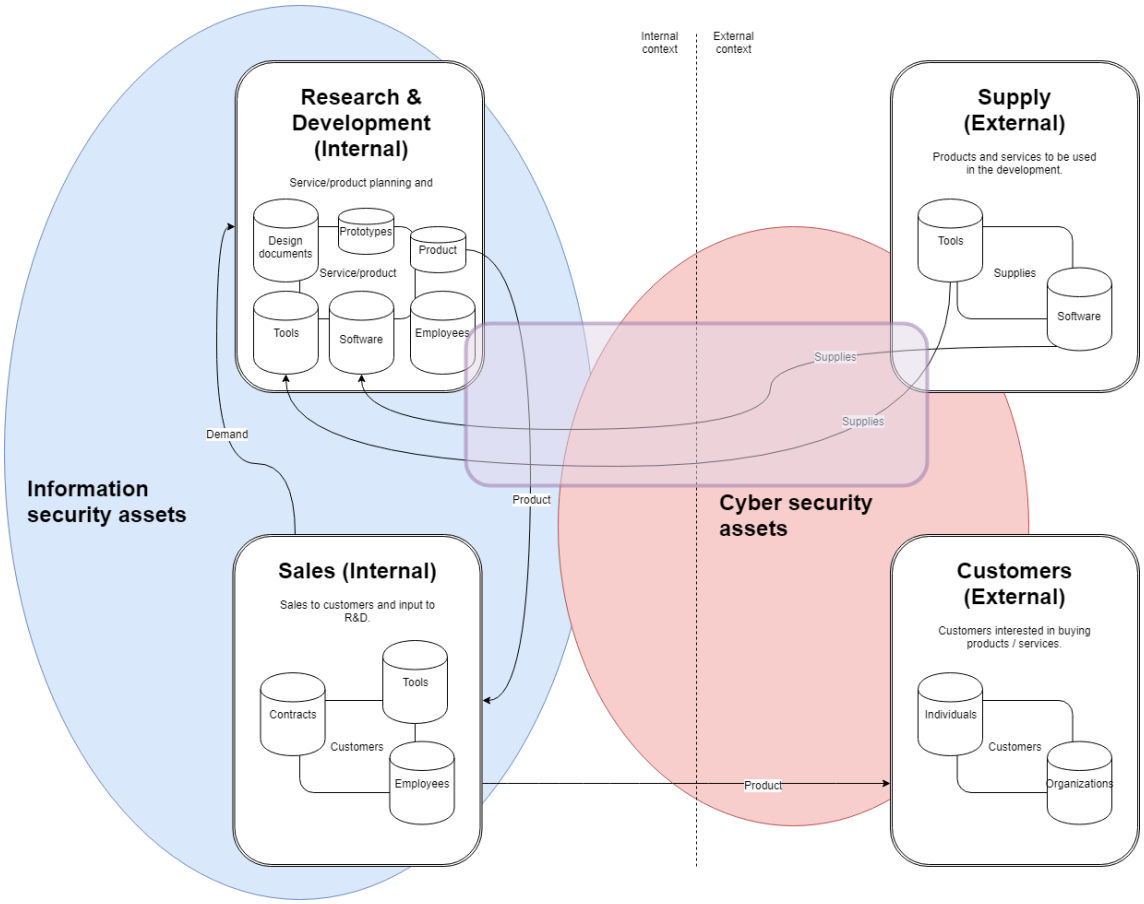


Figure 15. Critical internal and external business processes with high-level assets including information and cyber security domains. The focus on this figure is set as shown in the transparent rectangle connecting the R&D department and the supplier.

The points of interest depicted in the figure above are the assets that make R&D process, which is dependent on the external supplies, functional. The general concept that applies to this scenario is that there are multiple external stakeholders that the organization is depending on, and on the other hand, the external stakeholders may depend on multiple organizations meaning that their interests are shared among multiple stakes (multiple organizations interested in supplies) making the interests somewhat biased from the organization's point of view. Therefore it falls back to the organization A to match their security controls against their own interests instead of relying only on the security controls provided by for example the interconnecting infrastructure (CII, such as telecommunications network) or the external stakeholder.

When the organization purchases resources from the external supplier, the entities share information either by digitally over the Internet, through phone or by postal services. The contents of this communication are information that may be of high interest from the attacker's perspective, and harmful to the organization if accidentally disclosed to

unauthorized parties. The information is transmitted, processed and stored by the use of ICT [3]. Organization mitigates the threats against information security assets through the controls (or countermeasures) available in the ISO/IEC 27001:2013 standard, such as classifying the information into classes and encrypting any classified information leaving the security perimeter towards untrusted environments [1]. However, the organization has less control over that information when it has been sent out to the Internet (or anywhere in cyber space). Still, the organization might be able to influence how its stakeholders' processing, transmitting, and storing that information manage their information security risks. Security policies or service level agreements can be used as example tools to manage the external risks [35]. It can be concluded that the information security management system (ISMS) is sufficient in terms of coverage until the point when the information has left the security perimeter defined and protected by the ISMS. This is the area until where the vulnerabilities in ICT systems processing and storing information are controlled. After that point, the information and the ICT systems used are those that cascade the vulnerabilities in these assets to an environment (cyber space) with inconsistent controls and users who are generally unaware of these vulnerabilities [3]. It is therefore important to understand the vulnerabilities that are caused by the collaboration of using ICT and information together and consider the users of these vulnerable systems and services as assets to be protected under cyber security domain.

In this particular scenario, the infrastructure, whether it be CII (Critical Information Infrastructure) or CI (Critical Infrastructure), transmitting the information between the organization and the supplier will likely take advantage of the use of ICT. ICT systems may have vulnerabilities in configurations or hardware because they are usually configured and designed by humans. A human can be considered a threat to ICT security [3]. Networks that connect separate ICT systems together may pose additional vulnerabilities through weaknesses in network protocols. The application that is running on the ICT system may have vulnerabilities due to the weaknesses in programming standards and security testing. The ICT system, and its application, offering interaction with the processed information may be connected to the Internet which exposes the already vulnerable system to the users on the Internet. The user on the Internet, or through any other media available, uses that system and immediately is exposed to a risk that he or she may be completely unaware or incapable to mitigate. This is a definition of a cyber security asset in this context – users of information-based assets in cyber space that

receive their vulnerabilities from the use of ICT. The user, in this case, is the cyber security asset – a human, organization or another ICT system. That asset can either belong to an individual or organization, be virtual or physical [2]. In the example depicted in the figure (Figure 15) the cyber security assets can be defined by finding the underlying ICT systems and investigating their vulnerabilities and users. The following example scenarios all apply.

- The organization has an ICT system that automatically orders resources for the R&D department from the supplier using a secured communications channel over the Internet. The assets, in this case, are the actual order transaction and the secured communications channel that is exposed to threats via vulnerabilities introduced by the use of ICT.

- The supplier delivers the resources (such as software) to the organization electronically over the Internet. From the organization's point of view, the cyber security assets are in this case the purchased software and the secured communications channel used for delivery. These two assets are being threatened via the vulnerabilities in the underlying ICT.

- The organization is paying the resources it has bought from the supplier using online banking service. In this scenario, the employee interacting with the online banking service is using virtual currency to pay the bill. The cyber security assets are therefore the employee and the virtual payment transaction. Both these assets are being threatened via the vulnerabilities in the underlying ICT systems that are external to the organization.

    - In more detail, the external underlying ICT systems are the online banking service, Internet Service Providers' networks, Critical Information Infrastructure and the equipment the employee uses to connect to the cyber space.

    - To be able to countermeasure the vulnerabilities in the ICT systems that are threatening the cyber security assets, the organization has to focus on protecting the cyber security assets by understanding all the critical vulnerabilities in the underlying infrastructure without an actual capability to influence to those vulnerabilities directly. This might sound like an

absurdly impossible task to achieve at first. To generalize, the countermeasures must be implemented within the identified cyber security assets by securing the human factor and the actual virtual payment transaction.

The following figure (Figure 16) explains the before mentioned scenarios by visualizing the transition of an information asset to the cyber space environment. The underlying ICT will be different, which also means that the vulnerabilities are different and cannot be directly controlled with the countermeasures available in the internal context of an ISMS.

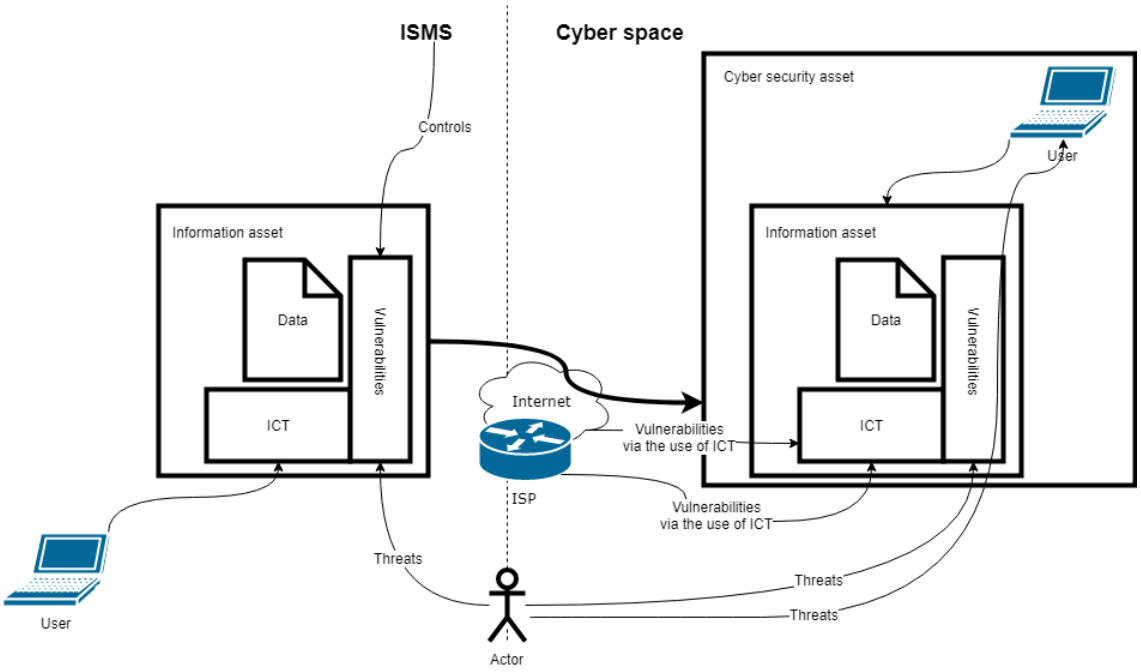


Figure 16. Information asset versus the cyber security asset. The ISMS is considered as an internal context and the cyber space as an external context. The underlying ICT is different when comparing the contexts, making the vulnerabilities also different.

It is also worth mentioning that in this particular type of scenario the organization transmitting information outside the context of the ISMS is adopting a role of consumer of services in cyber space, not a provider. In order to receive services provided by cyber space, the organization has to first expose their information assets and protect them as cyber security assets. An example scenario is an online banking service, where the organization or a user needs to be authenticated first in order to use the banking service.

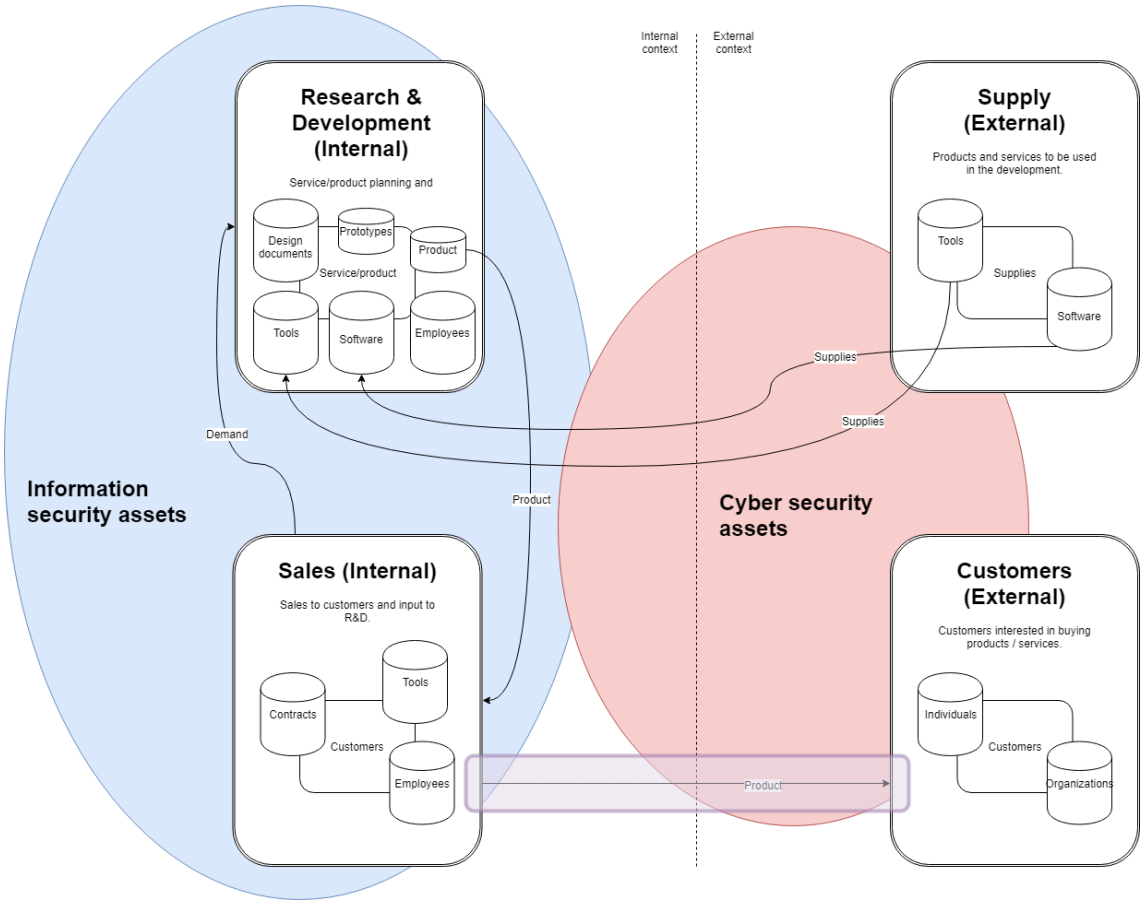


Figure 17. Critical internal and external business processes with high-level assets including information and cyber security domains. The focus on this figure is set as shown in the transparent rectangle connecting the Sales department and the customers.

The second key issue depicted in the figure above is the cyber security assets that facilitate the selling of products or services by the sales team to customers. The same assets that are responsible for transmitting the transactions through the Internet are important here, but there is also another angle that is introduced by the actual selling process. When the product has been sold to the customer, whether it be individual or organization, it is the responsibility of the provider (according to the cyber security standard) to ensure the security of their product in the cyber space [2]. In contrary to the previous scenario (Figure 15), the organization, in this case, adopts a role of provider of services in cyber space.

There are few different angles in this issue. First, the product or service that has been developed by the R&D department may contain vulnerabilities. Secondly, and depending on the characteristics of the product, the use of the product in cyber space may introduce new vulnerabilities that are originating from the use of ICT. Vulnerabilities in the product or service may allow an attacker to steal confidential (such as personal) information about

the customer by exploiting the vulnerabilities introduced by the R&D process and the use of ICT in the cyber space. In this case, the cyber security assets are the customers, and a service or a product that is being sold, in addition to protecting information assets as cyber security assets that are being threatened via vulnerabilities in ICT systems. These assets can be for example the reputation of the organization, a domain name and a web server for selling the services and products to customers – almost anything that is a user of an information-based asset that inherits the vulnerabilities from underlying ICT. The following examples explain these particular scenarios in more detail.

- A reputation of an organization is an intangible information security asset, that will become a cyber security asset when that information is processed, stored and transmitted in the cyber space by a user (a human, organization or an ICT system). The vulnerabilities that are introduced by the use of ICT can indirectly harm the reputation of the organization for example in a scenario where confidential information is processed and leaked to unauthorized entities through a vulnerability in an ICT system. The cyber security asset is, therefore, a reputation of an organization, including the underlying information and ICT-based assets.

- The product or service may be considered as (at least partly) an intellectual property (IP) [48] (such as patents [2]) to the organization A, and selling it to customer may expose it to additional risks in cyber space, where the controls available under the ISO/IEC 27001:2013 standard [1] have no effect. The intellectual property (IP) is a cyber security asset in this case.

- The product may allow the criminals in cyber space to exploit the vulnerabilities in the product in order to gain benefit (information, money) from the customer, or use the product as a tool to facilitate another attack, which may also harm the organization itself:

    - For example, products that are connected to the Internet and manageable over the Internet (IoT) pose a great risk of ending up as part of a botnet [49].

    - Known vulnerabilities in the product or service may allow an attacker to steal confidential (such as personal) information about the customer.

- The provider of the product or service may be indirectly impacted as well, where a damage to reputation (for example facilitated by a data breach), is threatening a cyber security asset.

Based on this analysis, the product may introduce new vulnerabilities in the cyber space, and act as a threat to others, including the organization itself. The result of attackers exploiting the before mentioned cyber security assets may have negative consequences on the organization's reputation, which may indirectly affect the other stakeholders (such as investors) as well.

Consider an example of an organization's domain name as a cyber security asset to protect from criminals. The organization values the domain name because it represents the company in the cyber space and they can communicate their vision and values through a uniquely identifiable online name. The Internet, in this case, is just another channel to build a stronger brand for the organization in order to achieve the goals set by the shareholders of that organization. Usually, the organization also relies on the Internet for directly selling services and goods to customers for profit. The domain name itself, in this case, is the cyber security asset that needs to be protected from the threat of website defacement (caused by the vulnerabilities in ICT) for example. Another angle to this scenario is provided by users of the domain name while browsing the Internet. They must be considered as users of this information-based domain name, which receives vulnerabilities from the use of underlying ICT (vulnerability in a web server's software allowing a hacker to redirect users to a malicious website), making the users of that domain name also assets in terms of cyber security.

A domain name "example.com" has value for its owner, but it may be controlled and configured external to the owner. Website of the organization may be hosted externally, and a global Domain Name System (DNS) takes care of translating the IP address into a domain name and vice versa. Basically, this is again a kind of a supply chain to deliver the benefits of having a domain name through external suppliers, that need to be also considered as stakeholders, as is analysed in the Stakeholders chapter. Present organizations rely on external suppliers usually more than is understood from the business perspective making the analysis of external dependencies extremely crucial in terms of cyber security [35]. If the web server and DNS service is hosted and configured in full control of the organization (without any reliance to external suppliers, which would be a

very rare occasion) then the situation would be less complex, and relevant risks could be covered mostly by the applicable information security controls, but as the organizations are more and more cutting down the operational costs they are outsourcing the management of these critical information infrastructure services to external organizations, which will be directly translated into additional cyber security risks [27].

We can conclude from the previous analysis that if the domain name is a valuable asset to the organization, then a certain value must be set for the external organizations (in this case the DNS system and web server hosting which are considered as stakeholders as well) who are serving the underlying infrastructure in order for the domain name to provide its full benefits. The figure below clarifies this example.

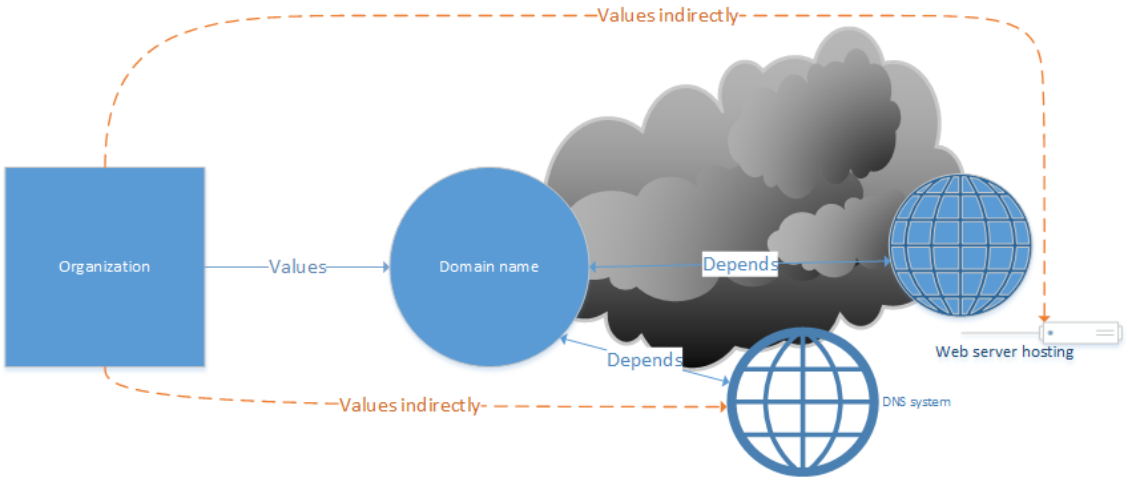


Figure 19. Direct and indirect asset valuation. Providers of DNS and web server hosting services must be considered as stakeholders.

A rough demarcation point between a purely traditional information asset and asset in the context of cyber space is where the asset in cyber space has at least one vital dependency external to the organization, such as the value of a domain name relying on the DNS and web server hosting services. In other words, what this also means is that an information asset is taken out of the internal context of the ISMS and moved to the external context of cyber space, and letting an external stakeholder (dependency is formed) take care of the countermeasures against the vulnerabilities stemming from the underlying ICT systems owned or controlled by the stakeholder. The linking between the stakeholders and assets is therefore crucial in understanding the requirements to protect an information asset in cyber space.

To summarize the difference between information and cyber security assets, we shall describe the cyber security asset as the overall target (incl. users of the asset) of countermeasures to mitigate the risks to the organization's information caused by the actors in cyber space threating to exploit the vulnerabilities in the underlying external ICT systems.

9.4.3 Step 3 – consider the dependencies with stakeholders as assets

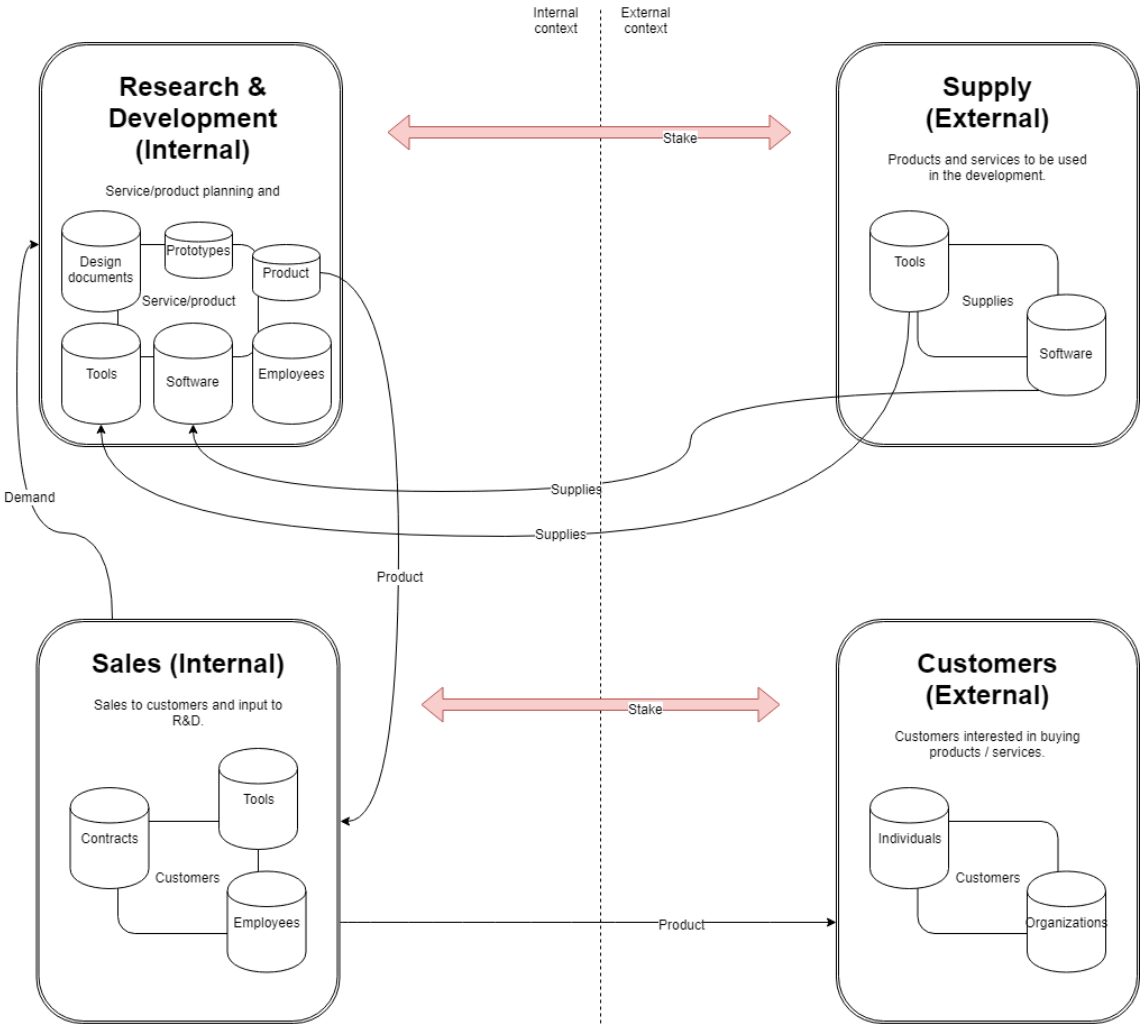


Figure 18. Critical internal and external business processes with high-level assets and dependencies between stakeholders.

When considering the dependencies between the stakeholders, it is of high importance to analyse how the actions and behaviour of stakeholders have an effect on the organization operating in cyber space. The figure above summarizes the dependencies between the processes. The sales process is relying on the customers buying the product or service. The R&D process is relying on the services and goods provided by the supply process. Customers are relying on the sales department to sell a product fulfilling their needs. Both

entities may affect negatively on each other under the circumstances presented in the following chapters.

The supplier may not be able to deliver the supplies due to the problem in the communications (for example a major Internet Service Provider fault). In this case, a vulnerability in the underlying ICT system has been exploited by an external threat to the system, affecting directly to the state of cyber security as well. The risk of not receiving supplies and losing money because of the delayed R&D process must be mitigated via cyber security risk management process where the cyber security asset of interest is the availability of the communication channel. Taking into account all of the stakeholders in this scenario, both the organization and supplier are depending on the communications network provided by the Internet Service Provider. The availability of the communications channel is depending on the Internet Service Provider, making the Internet Service Provider a critical stakeholder for both the organization and the supplier. A single dependency with an Internet Service Provider leads to a problem when moving in the asset hierarchy towards the business processes. When the availability of the communications channel is considered as a valuable asset to the organization, then unavailability of this asset will have a direct negative impact on the overlying business process of research and development, which will cascade directly into the service level threating the entire business mission. This kind of simple risk scenario can be mitigated with redundant communication technologies and service level agreements (SLAs) with the service providers. According to the cyber security standard, the organization is also responsible for communicating information regarding prevalent cyber security risks to other stakeholders [2].

9.5 Transferring the results to ISMS

A traditional ISMS will likely (not a requirement, but a countermeasure) contain a documented asset register with their corresponding owners (A.8 Asset management [1]). Moreover, an organization may already mitigate risks relevant to external supply chains through the ISMS using the controls available in the Annex A (A.15 Supplier relationships [1]). However, the area that needs attention from the cyber security management point of view are stakeholder relationships to assets. When a communications channel is considered to be a critical cyber security asset from the

availability and confidentiality point of view to protect organization's information-based assets in cyber space, it is necessary for an organization to consider the vulnerabilities the stakeholder (the infrastructure providing the communications channel, for example, an ISP) introduces by their use of ICT systems. Certain trust (such as proof of countermeasures, whether organizational or technical, implemented by the ISP) must be assured in order for the organization the be able to accept the level of risk of transmitting confidential information in cyber space. Similarly, an ISP will likely build their own business based on a trust they have formed with the Critical Infrastructure providers. Building trust can be difficult as the cyber space provides virtual anonymity to a great extent [2]. Building trust should be a groundwork for a cyber security strategy – to choose who to trust and based on what conditions, including the internal employees of an organization [50].

9.5.1 Including cyber security assets as part of an asset register

A proposal for a method to include cyber security assets as part of an existing information asset register is presented in the following paragraph. When considering the general attributes of information security assets (the CIA paradigm), same attributes apply to cyber security assets as well. If an asset's availability and confidentiality are assured in the context of an ISMS, then these attributes will arguably remain same when moved out of that context to cyber space. In the light of the above, removing an attribute of availability may seem attractive at first, as it could seem less important attribute in a hostile environment such as cyber space. But how can one assure confidentiality without availability? As is stated in the standard, there may be additional attributes as well, such as authenticity, accountability, non-repudiation or reliability [2]. Additional attributes may be necessary to add for an asset in order to fulfil the assurance needs in cyber space.

For the purpose of inventorying cyber security assets as part of an information asset register, and for this knowledge to be available in the risk management process, a proposed method is presented below.

- Information-based cyber security asset is inventoried with a corresponding information security asset, meaning that the information security asset is marked uniquely for the risk management process to become aware of its special characteristics and requirements in terms of cyber security.

- These characteristics and requirements contain information about relevant stakeholders, and dependencies, in addition to the dependencies with the business processes or services.

- Vulnerabilities and threat scenarios are sourced, formed and analysed based on the underlying infrastructures (ICT systems, organizations, individual users) that are processing, storing or transmitting (using) the asset in cyber space external to the context of traditional ISMS.

- Non-information-based cyber security assets are mostly found to be attached to scenarios where the information is not at a direct risk [3]. Such a scenario could be an attack on Critical Infrastructure (CI) that directly negatively affects to wellbeing of a society or nation [3]. In this case, information is just a collateral. An attack can be also targeted to an individual person directly (cyber bullying), without any interest set forth in the individually owned information-based property, such as Bitcoins [3].

    - These special scenarios and their corresponding assets (societal values, individuals) should be included in the asset register, dissociating them from traditional information-based assets, as controls to reduce risks to societal and individual values and wellbeing are typically out of scope of a private organization, unless the risks are explicitly introduced by the organization's service, product or presence in cyber space.

9.6 Summary of assets

The tables in "Appendix 4 – Summary of assets" summarize and categorize the assets that have been introduced in the chapter "9 Assets" with their dependencies. The assets have been categorized based on their type (service, process, stakeholder, tangible or intangible and information or non-information-based asset).

To analyse the summary of assets presented in the appendix "Appendix 4 – Summary of assets" the following conclusion shall be made.

- The organization's mission is depending on the service, where the service is depending on the four critical core processes:

- Research & Development (R&D) as an internal core process,
- Sales as an internal core process,
- Supply as an external core process and
- Customers as an external core process.

- These four core processes have internal dependencies where the R&D process is depending on the Sales an Supply processes, whereas the Sales process is depending on the R&D and Customers processes.
- The core processes also have complex dependencies with stakeholders, where Employees, Internet Service Providers, and Critical Infrastructure Providers play the most important roles.
- The core processes lean heavily on the following assets: secure communications channels, the organization's employees and the equipment used to connect to the cyber space, and the equipment and systems used to provide services in cyber space including the Critical Information Infrastructure (CII).

To combine the information gathered from analysis of (inter)dependencies it is possible to summarize, that in this particular case, protecting the human factor from the employees' perspective, and securing the both information and non-information-based cyber security assets through managing the risks related to Internet Service Providers and Critical Information Infrastructure are the key areas of focus.

9.7 Conclusion

Taking into account the previous analysis of assets and their dependencies with stakeholders, business processes, and services, we can summarize the assets to belong either in one of these two categories:

- Information-based cyber security assets are those that are intangible. Users of information-based assets in cyber space that receive their vulnerabilities from the use of ICT formulate the eventual cyber security assets. The user, in this case, is the cyber security asset to protect as well – a human, organization or another ICT

system. That asset can either belong to an individual or organization, be virtual or physical [2]. These assets are mainly located in the categories of People and Information as is presented in the figure (Figure 10). A demarcation point between an asset managed by a traditional ISMS and a cyber security asset is in the external dependencies with other stakeholders, such as Internet Service Providers. Therefore, it can be said that most of the information security assets will become cyber security assets at the point when they are moved outside the defined scope of an ISMS. In the light of the above, the external dependencies, also known as stakeholder dependencies or supply chains, must be managed to be able to mitigate the risks impacting these information-based cyber security assets.

- Non-information-based cyber security assets can be tangible or intangible. They consist of nations, stakeholders, humans, and their societal values and interests, plus facilities, technology, and equipment that are needed to store, process and transmit information [3]. These assets are mainly located in the categories of People, Facilities, Technology and Stakeholders as is presented in the figure (Figure 10).

This chapter provided means to transfer the asset evaluation analysis to an existing ISMS. Important factors were noted to be related to the stakeholder relations and building trust among these stakeholders and the supply chains they form. Therefore the scope of asset analysis can be concluded the be somewhat larger than a scope of a traditional information-based asset because the analysis contain all the stakeholders who are using that information asset in cyber space, and thus introducing unique vulnerabilities by the use of their ICT systems.

A proposal for moving identified cyber security assets as part of an information asset register (or inventory) was presented. The cornerstone of these new assets to be included is mostly concerned of the big brothers of information assets – the information-based cyber security assets that receive their special needs from the dependencies with stakeholders, such as ISPs and other vendors. A general approach is that an information security asset will become a cyber security asset whenever it is moved outside the influence of the countermeasures implemented under the ISMS. This is where the cyber security controls are introduced as part of cyber security management system, a functional part of an ISMS.

10 Summary

This thesis argues that the cyber security as a security domain differs from the other security domains, such as information security domain which is the base domain for this work, and these terms cannot be used interchangeably within the international standards to efficiently identify and manage risks. The fundamental understanding of each security domain, especially the information and cyber security domain, is a prerequisite to a successful implementation of the standardized cyber security guidelines. The cyber security standard do not specify the requirements enough in order to efficiently identify the relevant stakeholders and assets relevant to cyber security. This will make the mentioned cyber security standard seemingly obsolete mostly because of the quality and amount of security controls available already in the ISO/IEC 27001:2013 standard. This will undermine the effects and slow down the adoption of the cyber security standard to practically make cyber space more secure.

This thesis proves that there are certain fundamental differences between these two security domains, and understanding those are vital to moving on with analysis of stakeholders and assets in order to move to a risk assessment phase. Tools and knowledge to understand the stakeholders and their complex dependencies with business processes, other stakeholders and assets are provided and tested on a generalized conceptional organization to maintain the international applicability of these guidelines and the guidelines presented in the cyber security standard. Assets are analysed based on their characteristics and explained what it actually means if an asset is a cyber security asset, comparing analyses to traditional information assets and concepts.

The final result is a set of knowledge and tools to drive the change towards cyber security management. The proposed method is including the cyber security aspect as part of an ISMS where the cyber security assets are being evaluated based on their unique requirements introduced by cyber space, and the stakeholders involved. The transition is not problem-free but it makes sense from the resource and state of mind point of view. To be able to assess all risks (in addition to traditional information-based risks) stemming

from stakeholders' interests and dependencies will add value and rigor to the whole management system.

Future research in this field should focus on a truly experimental validation and testing of stakeholder analysis in a more controlled environment using real data acquired from a real organization based on the proposed analysis process. After that, carrying out a fully practical asset evaluation, analysis and experiment on top of the verified stakeholder analysis data, rather than relying on data and knowledge derived from the hypothetical environment, should be a logical step before moving into actual risk assessment and treatment activities.

References

[1] Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques, "ISO/IEC 27001:2013 "Information technology. Security techniques. Information security management systems. Requirements."," ISO/IEC, Geneva, 2013.

[2] Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques, "ISO/IEC 27032:2012 "Information technology. Security techniques. Guidelines for cybersecurity."," ISO/IEC, Geneva, 2012.

[3] R. von Solms and J. van Niekerk, "From information security to cyber security," *Computers & Security,* vol. 38, no. Cybercrime in the Digital Economy, pp. 97-102, 2013.

[4] ENISA, "Definition of Cybersecurity - Gaps and overlaps in standardisation," 01 July 2016. [Online]. Available: https://www.enisa.europa.eu/publications/definition-of-cybersecurity. [Accessed 19 March 2018].

[5] E. Dezenhall, "A Look Back at the Target Breach," Huffington Post, 6 June 2015. [Online]. Available: https://www.huffingtonpost.com/eric-dezenhall/a-look-back-at-the-target_b_7000816.html. [Accessed 9 March 2018].

[6] J. Robertson, ”The Branding of a Bug: How Heartbleed Became a Household Name,” Bloomberg, 28 April 2014. [Online]. Available: https://www.bloomberg.com/news/2014-04-28/the-branding-of-a-bug-how-heartbleed-became-a-household-name.html. [Haettu 18 February 2018].

[7] International Organization for Standardization, "Executive Summary of The ISO Survey of Management System Standard Certifications 2016," International Organization for Standardization, Geneva, 2017.

[8] NIST, "Cybersecurity framework," NIST, [Online]. Available: https://www.nist.gov/cyberframework. [Accessed 12 March 2018].

[9] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," 12 February 2014. [Online]. Available: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf. [Accessed 20 March 2018].

[10] High Representative of the European Union for foreign affairs and security policy, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace," European Commission, Brussels, 2013.

[11] A. Mitra and R. L. Schwartz, "From Cyber Space to Cybernetic Space: Rethinking the Relationship between Real and Virtual Spaces," *Journal of computer-mediated communication,* vol. 7, no. 1, 2001.

[12] D. E. G. Jr., D. W. Hubbard, S. McClure and R. Seiersen, "How to Measure Anything in Cybersecurity Risk," John Wiley & Sons, 2016.

[13] B. Filkins, ”IT Security Spending Trends - A SANS survey,” SANS Institute, 2016.

[14] S. Gandel, "Lloyd's CEO: Cyber attacks cost companies $400 billion every year," Fortune, 23 January 2015. [Online]. Available: http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/. [Accessed 18 February 2018].

[15] ENISA, "ENISA Threat Landscape Report 2017," 15 January 2018. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017. [Accessed 19 March 2018].

[16] MITRE, "Download CVE List," 11 February 2018. [Online]. Available: https://cve.mitre.org/data/downloads/index.html. [Accessed 17 February 2018].

[17] CBInsights, "Cybersecurity Funding On Pace For A Record-Breaking Year," 23 August 2017. [Online]. Available: https://www.cbinsights.com/research/cybersecurity-deals-funding-acquisitions/. [Accessed 28 February 2018].

[18] Z. Kacy, "Bug bounty report," Cybersecurity Ventures, 17 August 2017. [Online]. Available: https://cybersecurityventures.com/bug-bounty-report-2017/. [Accessed 28 February 2018].

[19] ITU, "Statistics," [Online]. Available: https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2017/ITU_Key_2005-2017_ICT_data.xls. [Accessed 18 February 2018].

[20] D. Ron, "Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace," Canadian defence & foreign affairs institute, 2012.

[21] CBL, "Spam trap flow statistics," [Online]. Available: https://www.abuseat.org/public/totalflow.html. [Accessed 28 February 2018].

[22] Netcraft, "May 2017 Web Server Survey," 25 May 2017. [Online]. Available: https://news.netcraft.com/archives/2017/05/25/may-2017-web-server-survey.html. [Accessed 28 February 2018].

[23] Netcraft, "May 2010 Web Server Survey," 14 May 2010. [Online]. Available: https://news.netcraft.com/archives/2010/05/14/may_2010_web_server_survey.html. [Accessed 28 February 2018].

[24] F. Cheng and C. Yeh, "Paradigm Shift of Net Neutrality in the United States, 14th International Telecommunications Society (ITS) Asia-Pacific Regional Conference: "Mapping ICT into Transformation for the Next Information Society"," International Telecommunications Society (ITS), Kyoto, 2017.

[25] Eurostat, "Glossary:Information and communication technology (ICT)," 20 September 2016. [Online]. Available: http://ec.europa.eu/eurostat/statistics-explained/index.php/Glossary:Information_and_communication_technology_(ICT). [Accessed 4 April 2018].

[26] E. Nickolov, "Critical information infrastructure protection: analysis, evaluation and expectations," *Information & Security. An International journal.*, vol. 17, pp. 105-119, 2005.

[27] Investopedia, "Stakeholder," [Online]. Available: https://www.investopedia.com/terms/s/stakeholder.asp. [Accessed 4 March 2018].

[28] B. Ruairi and V. Zsuzsa, "Stakeholder analysis: a review," *Health and policy planning,* vol. III, no. 15, pp. 239-246, 2000.

[29] THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT

AND OF THE COUNCIL," 27 April 2016. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679. [Accessed 13 March 2018].

[30] S. Gratzl, A. Lex, N. Gehlenborg, H. Pfister and M. Streit, "LineUp: Visual Analysis of Multi-Attribute Rankings," 2013. [Online]. Available: http://dx.doi.org/10.1109/TVCG.2013.173. [Accessed 31 March 2018].

[31] European Commission, "The Directive on security of network and information systems (NIS Directive)," European Commission, 5 July 2016. [Online]. Available: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive. [Accessed 22 March 2018].

[32] B. Krebs, "Target Hackers Broke in Via HVAC Company," 5 February 2014. [Online]. Available: https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/. [Accessed 24 March 2018].

[33] BBC, "HP laptops found to have hidden keylogger," BBC, 11 December 2017. [Online]. Available: http://www.bbc.com/news/technology-42309371. [Accessed 24 March 2018].

[34] J. Allen, M. Butkovic and J. Haller, "Supply Chain Risk Management: Managing Third Party and External Dependency Risk," March 2015. [Online]. Available: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=435490. [Accessed 26 March 2018].

[35] European Commission, "Open Internet," 2 March 2018. [Online]. Available: https://ec.europa.eu/digital-single-market/en/open-internet-net-neutrality. [Accessed 2 April 2018].

[36] B. Rowe, D. Wood, D. Reeves and F. Braun, "The Role of Internet Service Providers in Cyber Security," Institute for Homeland Security Solutions, 2011.

[37] M. Dunn, "The socio-political dimensions of critical information infrastructure protection (CIIP)," *Int. J. Critical Infrastructures,* vol. 1, pp. 258-268, 2005.

[38] Management Mania, "RASCI Responsibility Matrix," 17 March 2016. [Online]. Available: https://managementmania.com/en/rasci-responsibility-matrix. [Accessed 2 April 2018].

[39] Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques, ”ISO/IEC 27000:2018 "Information technology - Security techniques - Information security management systems - Overview and vocabulary",” ISO/IEC, Geneva, 2018.

[40] ISACA, "THE RISK IT FRAMEWORK," ISACA, Illinois, 2009.

[41] J. J. Cebula and L. R. Young, "A Taxonomy of Operational Cyber Security Risks," Carnegie Mellon University, Software Engineering Institute, Pittsburg, 2010.

[42] R. A. Caralli, J. H. Allen, D. W. White, L. R. Young, N. Mehravari and P. D. Curtis, "CERT®-RMM - SEI Digital Library - Carnegie Mellon University," February 2016. [Online]. Available: https://resources.sei.cmu.edu/asset_files/BookChapter/2016_009_001_514739.pdf. [Accessed 26 March 2018].

[43] Lucidchart, "What is a Swimlane Diagram," [Online]. Available: https://www.lucidchart.com/pages/swimlane-diagram. [Accessed 5 March 2018].

[44] R. A. Caralli, J. H. Allen, P. D. Curtis, D. W. White ja L. R. Young, ”CERT Resilience Management Model, v1.0 (CMU/SEI-2010-TR-012),” Carnegie Mellon University, Software Engineering Institute, Pittsburgh, 2010.

[45] C. Alberts ja A. Dorofee, ”Managing Information Security Risks: The OCTAVE(SM) Approach,” Addison Wesley, 2002.

[46] C. Alberts and A. Dorofee, "OCTAVE Threat Profiles," Carnegie Mellon University, Software Engineering Institute, Pittsburgh, 2001.

[47] T. I. o. I. Auditors, "Cybersecurity: keeping IP under lock and key," The Institute of Internal Auditors, Florida, 2014.

[48] A. Haritha and A. Lavanya, "Internet of Things: Security Issues," *International Journal of Engineering Science Invention,* vol. 6, no. 11, pp. 45-52, 2017.

[49] R. Hayes, "Cybersecurity: a question of trust," Microsoft, 20 October 2016. [Online]. Available: https://cloudblogs.microsoft.com/microsoftsecure/2016/10/20/cybersecurity-a-question-of-trust/. [Accessed 3 April 2018].

[50] ENISA, "Supply chain attacks," 29 August 2017. [Online]. Available: https://www.enisa.europa.eu/publications/info-notes/supply-chain-attacks. [Accessed 4 March 2018].

[51] Lucidchart, ”What is Business Process Modeling Notation,” [Online]. Available: https://www.lucidchart.com/pages/bpmn#section-3. [Haettu 5 March 2018].

[52] S. Bistarelli, F. Fioravanti and P. Peretti, "Defense trees for economic evaluation of security investments," Dipartimento di Scienze Universita degli Studi “G. d’Annunzio”, Pescara, 2006.

[53] J. Moteff and P. Parfomak, "Critical Infrastructure and Key Assets: Definition and Identification," Congressional Research Service, Washington, 2004.

[54] C. O. T. E. COMMUNITIES, "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on Critical Information Infrastructure Protection," COMMISSION OF THE EUROPEAN COMMUNITIES, Brussels, 2009.

[55] G. C. Wilshusen and D. A. Powner, "Statement for the Record To the Subcommittee on Terrorism and Homeland Security, Committee on the Judiciary, U.S. Senate, CYBERSECURITY, Continued Efforts Are Needed to Protect Information Systems from Evolving Threats," United States Government Accountability Office, Washington DC, 2009.

[56] A. Calder and S. Watkins, "IT Governance," in *An International Guide to Data Security and ISO27001/ISO27002,* London, KoganPage, 2015, p. 85.

[57] N. Virvilis and D. Gritzalis, "The Big Four - What we did wrong in Advanced Persistent Threat detection?," 2013 International Conference on Availability, Reliability and Security, Greece, 2013.

[58] J. A. Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," Center for Strategic and International Studies, Washington DC, 2002.

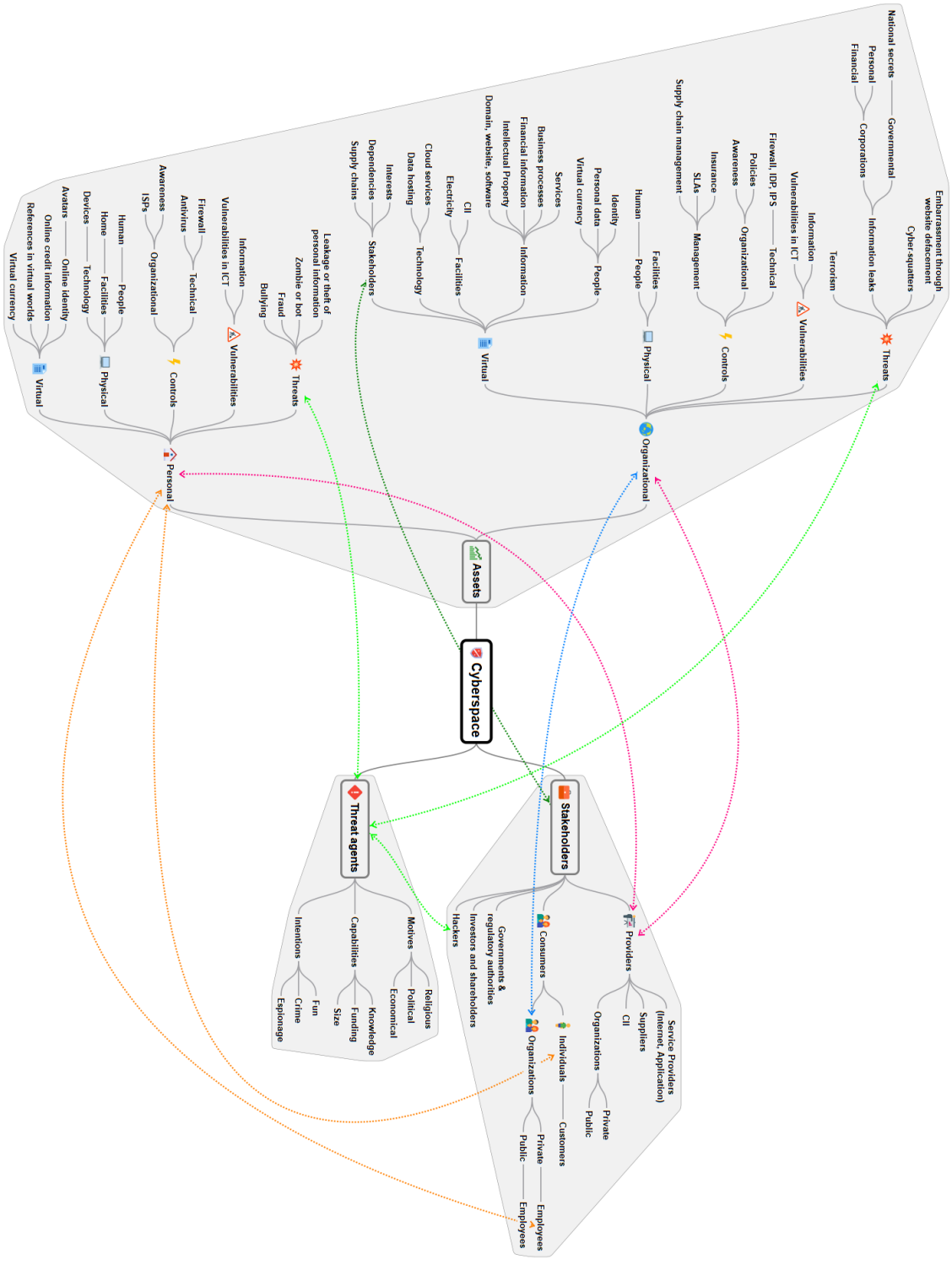
[59] European Commission, "What are Data Protection Authorities (DPAs)?," European Commission.

[60] WIPO, "What is Intellectual Property?," [Online]. Available: http://www.wipo.int/edocs/pubdocs/en/intproperty/450/wipo_pub_450.pdf. [Accessed 25 March 2018].

[61] T. W. Edgar and D. O. Manz, "Research Methods for Cyber Security," Syngress, Cambridge, 2017.

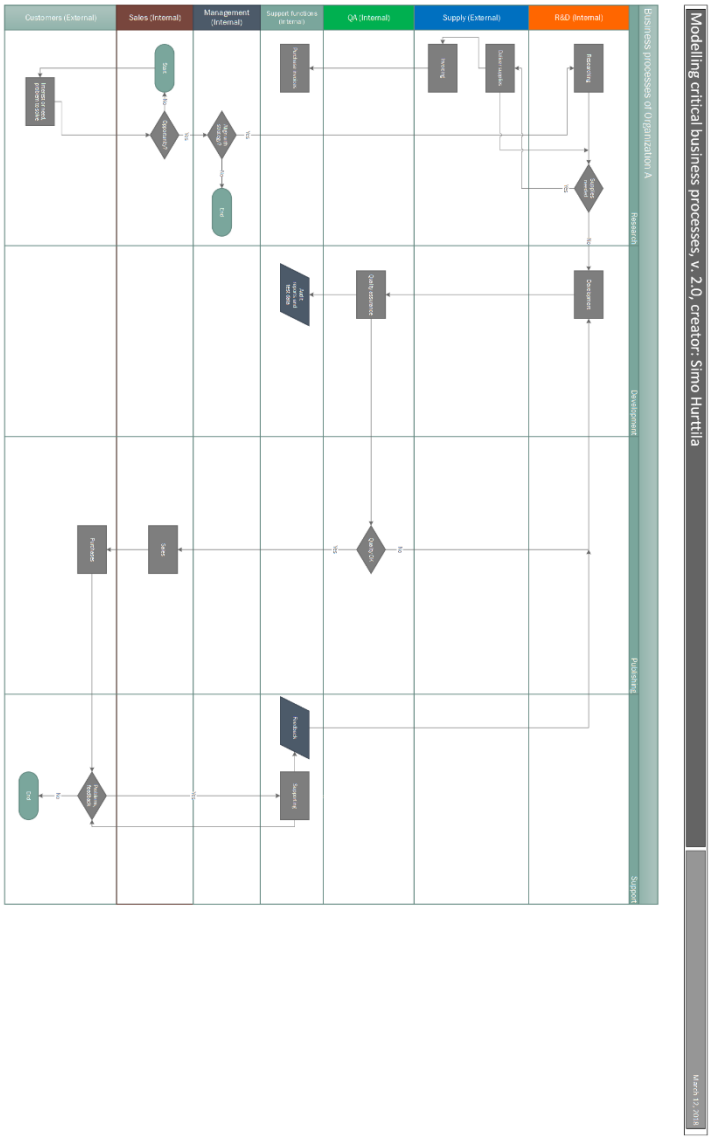
Appendix 1 – Cyber space visualization

Download URL (PDF)



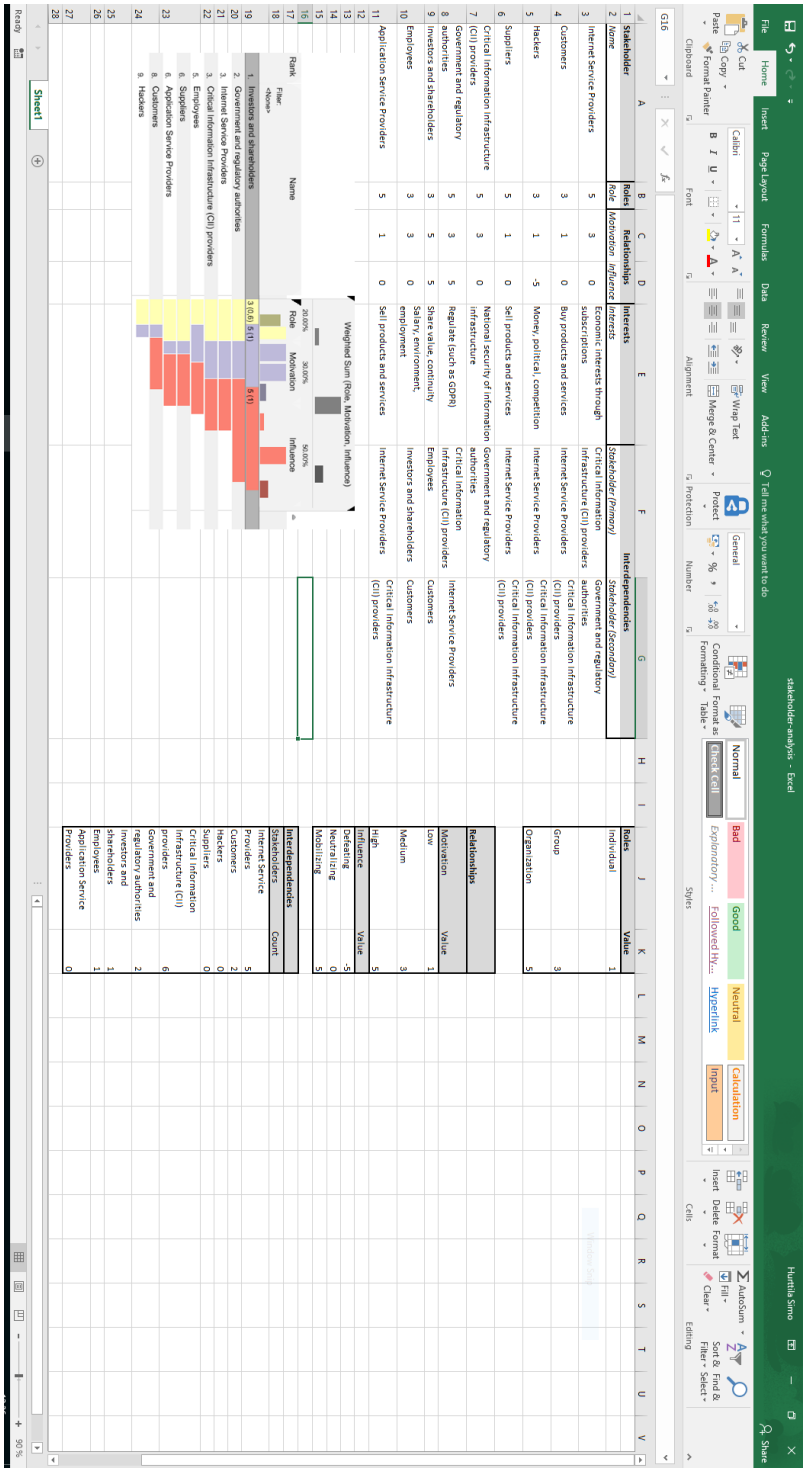
Appendix 2 – Business processes of Organization A

Download URL (Visio)



Appendix 3 – Stakeholder analysis

Download URL (Excel)



Appendix 4 – Communication and information sharing process (RASCI table)

Table 2. Communication and information sharing process (RASCI table).

	Roles and responsibilities in ISMS	Investors and shareholders	Government and regulatory authorities	Internet Service Providers	CII providers	Employees	Suppliers	Application Service Providers	Customers
Type of organization (IPO or IRO)	IPO & IRO	IRO	IPO & IRO	IPO & IRO	IPO	IRO	IPO & IRO	IPO & IRO	IRO
Acknowledgement	R/A	I				I			I
Reporting	R/A	I	S/C	S		I	I		I
Information sharing	R/A	I	C	C		I	I		I
Security incident management	R/A	I	S/C	S/C		I	I		I
Risk assessment	R/A	I	C	C	C	C	C	C	I

Regulatory/ Legislative	R/A	I	C	C					I

Appendix 5 – Summary of assets

Table 3. Missions and their dependencies.

ID	Type of asset	Asset	Note	Critical dependencies
	Missions			
MI1	Mission	Mission 1	Mission to generate value to shareholders	SE1
Summary: Only one critical service dependency exists in this scenario, but there can be many.				

Table 4. Services and their dependencies.

ID	Type of asset	Asset	Note	Critical dependencies
	Services			
SE1	Service	Service 1	Service to sell products customers	P1, P2, P3, P4
Summary: The most critical process dependencies were analysed in the "From business processes to underlying assets" chapter.				

Table 5. Processes and their dependencies.

ID	Type of asset	Asset	Note	Critical dependencies
	Processes			

P1	Process	R&D (Internal)	Research & Development process	P2, P3 S1, S2, S3, S4 A1, A2, A3, A4, A5, A6, A7, A11
P2	Process	Sales (Internal)	Selling products to customers	P1, P4 S1, S3, S4, S5 A2, A4, A5, A6, A7, A8, A9, A10, A11, A12
P3	Process	Supply (External)	Supplying goods	- S2, S3, S4 -
P4	Process	Customers (External)	Buying a product to fulfil a need	- S3, S4, S5 -
P5	Process	QA (Internal)	Quality Assurance process	P1 S1, S3, S4 A2, A4, A5, A6, A7, A12
P6	Process	Support (Internal)	Support functions	P1, P4 S1, S3, S4 A2, A4, A5, A6, A7, A12

P7	Process	Management (Internal)	Top management to steer the organization according to the strategy	- S1, S6, S7 A11
Summary: R&D process relies on Sales and Supply processes. Sales process relies on R&D and Customers processes. The processes also rely heavily on the following stakeholders: Employees, Internet Service Providers and Critical Infrastructure providers. The processes rely heavily on the following assets: Secure Communications Channel, Employees, Equipment owned by organization to connect to cyber space, Equipment and services provided by service providers and CII.				

Table 6. Stakeholders and their interdependencies.

ID	Type of asset	Asset	Note	Critical dependencies
	Stakeholders			
S1	Stakeholder	Employees (Internal)	Staff developing, supporting and selling products	S7, S5
S2	Stakeholder	Suppliers	Making product development possible	S3, S4
S3	Stakeholder	Internet Service Providers	Providing online services and connectivity to cyber space	S4, S6
S4	Stakeholder	Critical Information Infrastructure providers	Communications infrastructure	S6

S5	Stakeholder	Customers	Buying and using the product	S3, S4
S6	Stakeholder	Government and regulatory authorities	Regulating markets and cyber space	S3, S4
S7	Stakeholder	Investors and shareholders		S1, S5
S8	Stakeholder	Hacker		S3, S4
Summary: Internet connectivity through Critical Information Infrastructure providers and Internet Service Providers are the key stakeholder dependencies, as was also analysed in the "Stakeholders" section.				

Table 7. Tangible and intangible assets and their interdependencies used under the R&D process.

ID	Type of asset		Category	Asset	Note	Critical dependencies
	Tangible or intangible	Information or non-information-based	Category from the figure (Figure 10)			
A1	Intangible	Information-based	Information	Order transaction (data)	Order transaction from R&D department to supplier	A2, A4, A5, A6, A7

A2	Tangible	Non-information-based	Technology	Secure communications channel	Maintaining the confidentiality of the transactions between stakeholders	A5, A6, A7
A3	Intangible	Information-based	Information	Software	Software purchased from the supplier	A1, A2, A5, A6, A7
A4	Tangible	Non-information-based	People	Employees	Employees operating the systems and making virtual transactions	A2, A5, A6, A7
A5	Both	Both	Technology, Information	Equipment	Organization's equipment to connect to the cyber space	A6, A7
A6	Both	Both	Technology, Information	Equipment and services	ISP's equipment to provide services in cyber space	A7
A7	Tangible	Non-information-based	Facilities	CII	Telecommunications networks, DNS root servers	-
A8	Tangible	Non-informa	Technology	Web server	Organization's web server	A6, A7, A9

		tion-based				
A9	Intangible	Information-based	Information	Domain name	Organization's domain name	A6, A7, A8
A10	Intangible	Information-based	Information	Reputation	Organization's online reputation and brand	A8, A9
A11	Intangible	Non-information-based	Stakeholders	Interests of stakeholders	Interests of stakeholders	-
A12	Intangible/tangible	Non-information or information-based	Information or Technology	Product or service	Product or service sold to customers	A2, A4, A5, A6, A7, A8, A9, A10, A11
Summary: Similarly with the stakeholders, the equipment, facilities and providers of Internet connectivity services form the most critical dependencies among assets.						